La blockchain au regard du droit et de l'identité

Thibault Langlois-Berthelot

École des Hautes Études en Sciences Sociales

Ecole doctorale de l'EHESS

Centre Georg Simmel

Doctorat en

DROIT ET SCIENCES SOCIALES

THIBAULT LANGLOIS-BERTHELOT

LA BLOCKCHAIN AU REGARD DU DROIT ET DE L'IDENTITÉ

Thèse dirigée par : M. RAINER MARIA KIESOW

Date de soutenance : le 15 juin 2023

Rapporteurs
1 MME CAROLINE LEQUESNE-ROTH
2 M. GRÉGOIRE LOISEAU

Jury

1 MME VALÉRIE CHAROLLES, CHERCHEURE STATUTAIRE, HDR, LABORATOIRE D'ANTHROPOLOGIE POLITIQUE CNRS/EHESS

2 M. RAINER MARIA KIESOW, DIRECTEUR D'ÉTUDES, EHESS

3 M. JEAN LASSÈGUE, DIRECTEUR DE RECHERCHE, CNRS

4 MME CAROLINE LEQUESNE-ROTH, MAÎTRESSE DE CONFÉRENCES, HDR, UNIVERSITÉ CÔTE D'AZUR

5 M. GRÉGOIRE LOISEAU, PROFESSEUR À L'UNIVERSITÉ PARIS 1 PANTHÉON-SORBONNE

À toute ma famille, à tous mes amis, d'hier et d'aujourd'hui.

REMERCIEMENTS

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont rendu la réalisation de cette thèse possible. Je remercie mon directeur de thèse pour son soutien constant et pour sa confiance. Je remercie également mes collègues de la société IN Groupe qui m'ont accompagné et mes amis qui m'ont apporté un réconfort moral et une aide précieuse tout au long de ce parcours académique. Cette thèse a été enrichie par de nombreuses interventions et auditions, notamment lors de réunions publiques, de discussions privées, de colloques et divers autres évènements. Que les nombreux participants universitaires et/ou professionnels en soient vivement remerciés. Enfin, je remercie ma famille pour son soutien indéfectible tout au long de mes recherches.

RESUMÉ ET MOTS CLÉS

Depuis plus d'une décennie, les technologies blockchains redéfinissent progressivement et en profondeur les frontières politiques, juridiques et économiques de notre contrat social. Certaines de ses caractéristiques libèrent autant qu'elles défient l'ordre établi, c'est-à-dire les modèles de gouvernance existants. En collaboration avec la société IN Groupe, il est étudié à travers un prisme interdisciplinaire comment le positionnement et les perspectives de ces nouvelles technologies s'articulent, s'opposent ou s'inscrivent dans les cadres juridiques et sociaux actuels. Le concept d'identité numérique ne cesse depuis plusieurs décennies d'évoluer et d'être interrogé par les sciences pour faire face à l'expansion fulgurante des interactions et des besoins d'identification en ligne des personnes. Cette insatiable numérisation de nos vies implique de nouvelles considérations philosophiques, sociales et juridiques à la lumière des nombreuses facettes de nos identités, d'ores et déjà 'phygitales'. Avec ces tentatives de définitions et de réappropriations scientifiques de l'identité sont également évoquées des pistes de réflexion concrètes et actualisées au regard de l'émergence d'une nouvelle identité numérique 3.0. Supposées décentralisées, émancipatrices et au service de droits numériques, nous identifions en quoi l'identité numérique décentralisée et les technologies blockchains représentent une révolution à la recherche de nouvelles règles de droit. Par une photographie des (éco)systèmes socio-numériques cette étude interroge les conséquences de ces nouvelles technologies de décentralisation du Web 3.0, permettant aux individus de détenir une preuve d'existence numérique universelle en adéquation avec leurs droits fondamentaux, désormais cryptographiques et programmables. Une voie de réflexion privilégiée suggère également qu'il ne faudrait pas interdire ni discréditer certaines blockchains ouvertes et décentralisées, afin de satisfaire les besoins continus de confiance et de propriété cryptographique des internautes et des citoyens. Ces infrastructures peuvent effectivement servir d'alternative et de contre-pouvoir numérique, tout particulièrement dans les pays en voie de développement.

Mots clés

Sciences juridiques, sciences informatiques, décentralisation, Bitcoin, blockchain, crypto-actifs, identité numérique décentralisée, Web 3.0

ABSTRACT AND KEY WORDS

For more than a decade, blockchain technologies have been gradually and deeply redefining the political, legal, and economic boundaries of our social contract. Some of their characteristics both liberate and challenge the established order, i.e. existing governance models. In collaboration with the IN Groupe company and through an interdisciplinary lens, this paper examines how the positioning and perspectives of these new technologies are articulated, opposed, or integrated into current legal and social frameworks. In parallel with societal upheavals analyzed in the context of computer decentralization, the concept of digital identity has been evolving and questioned for several decades to cope with the explosive expansion of online interactions and identification needs of individuals. This insatiable digitization of our lives implies new philosophical, social, and legal considerations considering the many facets of our already 'phygital' identities. These attempts at defining and scientifically reclaiming identity also evoke new concrete lines of reflection regarding the emergence of a new digital identity 3.0. Supposedly decentralized, emancipatory, and serving digital rights, we identify how decentralized digital identity and blockchain technologies represent a revolution in search of new legal rules. By examining socio-digital (eco)systems, this study questions the consequences of these new Web 3.0 decentralization technologies, allowing individuals to hold universal proof of digital existence in line with their fundamental cryptographic and programmable rights. A privileged line of reflection suggests that it is crucial not to prohibit or discredit certain open and decentralized blockchains, to satisfy the continuous needs of trust and cryptographic ownership of Internet users and citizens. These infrastructures can indeed serve as an alternative and digital counterbalance, particularly in developing countries.

Keywords

Legal sciences, computer sciences, decentralisation, Bitcoin, blockchain, crypto-assets, decentralized digital identity, Web 3.0

Avertissement

L'École des Hautes Études en Sciences Sociales ainsi que la société IN Groupe n'entendent donner aucune approbation ni improbation aux opinions émises dans cette thèse.
Ces opinions doivent être considérées comme propres à son auteur.

Sommaire

Table des matières

Introduction

Toute construction sociale nécessite la mise en place de mécanismes d'identification afin que chaque personne puisse efficacement se reconnaître, c'est-à-dire s'identifier. Ce besoin d'identification s'explique par l'attribution individuelle et collective de droits et de devoirs pour faire société. Depuis ses formes les plus primitives comme l'attribution d'un nom d'usage fondé sur l'apparence physique, jusqu'à des formes d'identification aujourd'hui unique et aboutie comme la biométrie couplée à l'utilisation de documents d'identité aux capacités digitales, les formes d'expression de l'identité se multiplient et se croisent à l'ère numérique. L'identité est aujourd'hui plus que jamais un concept polysémique qui peut être défini sous l'angle philosophique, social et juridique afin de cerner l'identité vécue des personnes, c'est-à-dire à la fois les contextes et les besoins d'identification auxquels elles sont confrontées quotidiennement. L'identité se composerait de plusieurs contextes, un contexte temporel, un contexte social, un contexte de territoire. Qu'elle soit hors ligne ou en ligne, l'identité est ainsi une mise en abîme dont nous ne maîtrisons que certaines composantes, tout en ayant l'impression et l'intuition d'en posséder une compréhension parfaite. Par exemple, une carte d'identité porte et fixe certaines caractéristiques juridiques d'une personne, tout en considérant qu'elles demeurent relatives dans un temps long, en raison de leurs changements au gré du parcours social de chaque personne. L'un des objectifs de cette étude est de prendre conscience de l'identité numérique en général pour que chaque individu soit sensibilisé à l'émergence d'une quintessence numérique, c'est-à-dire d'un Internet de troisième génération plus ouvert, transparent et décentralisé, le Web 3.0.

Toutes interconnectées et dématérialisées, les interactions sociales sont sans cesse optimisées pour répondre aux besoins des individus, le numérique représentant une troisième révolution industrielle[1]. Toujours plus globales, rapides et personnalisées, les communications actuelles caractérisent un changement civilisationnel, depuis l'*homo sapiens* vers l'*homo numericus*[2]. En moins d'un demi-siècle, cette profonde (r)évolution est devenue la source d'un progrès sociétal planétaire. Notre capacité à échanger tous types d'informations, menant à tous types d'interactions, a été démultipliée grâce aux réseaux sociaux et aux plateformes numériques (Uber, Google Maps, réunions à distance) dont l'infrastructure pionnière demeure Internet. En 2021, presque 5 milliards de personnes disposant d'une connexion Internet peuvent profiter des avantages d'être connectés au reste du monde[3]. Aujourd'hui, de nombreuses interactions en ligne requièrent une identité numérique pour rejoindre des communautés, accéder à des services et recueillir des informations, publier des idées ou encore pour gérer ses finances en ligne. À ses débuts, Internet n'a pas été structurellement conçu pour fournir à tous ses utilisateurs une identité numérique, ce qui explique les multiples solutions d'identification et d'authentification actuelles

[1] ROUTLEY Nick, « The multi-billion dollar industry that makes its living from your data », 10 mars 2019, disponible en ligne
[2] COMPIEGNE Isabelle, « La société numérique en question(s) », chap. V, Qui est l'homo numericus ? pp.59-70, Éd. Sciences Humaines, 2010.
[3] PETROSYAN Ani, « Number of internet and social media users worldwide as of January 2023 », in *Statista Inc*, en ligne

que chaque individu tente de s'approprier. En réponse à ce besoin d'identification des internautes, chaque service en ligne propose une identification numérique plus ou moins fiable à l'usage et gourmande en données. Cette délégation aujourd'hui massive des identités numériques a engendré un déficit de confiance numérique, notamment en raison d'une dépendance informatique structurelle des utilisateurs envers ces services en ligne. Par exemple, il est aujourd'hui facile de numériser une information, il est plus complexe de lui faire confiance une fois en circulation dans l'univers numérique, par exemple au regard de son intégrité, de sa validité ou de son origine. Face à l'ampleur croissante de ces phénomènes, régulièrement faits générateurs d'atteintes aux droits des personnes, le législateur tente avec plus ou moins d'harmonisation et de succès un encadrement de cette sphère numérique. Si Internet est virtuel, ses conséquences sont bien réelles pour les internautes. L'univers informatique n'étant ni séparé, ni accessoire au monde physique, il est désormais complémentaire et graduellement devenu essentiel au pacte social.

Formidable outil de prospérité et de liberté économique et social pour certains, lente dérive vers une technocratie[4] par des détournements de finalités pour d'autres, Internet représente sans doute une révolution sociotechnique aussi inédite qu'en demi-teinte[5]. En effet, la croissance et l'utilisation exponentielle[6] de l'univers numérique atteint un paroxysme avec l'enfermement virtuel des internautes auprès de leurs services en ligne, dont la conception participe trop souvent à introduire une forme de dépendance psychosociale. Ainsi, la part de l'identité subjective construite et revendiquée en ligne tend à croître en importance de telle façon que l'univers numérique n'ait jamais aussi bien porté son nom. Pourtant, ce formidable progrès des communications numériques doit être mis en perspective d'une dépossession informatique et juridique qu'il entraîne pour l'identité *phygitale*[7] des personnes, qui se retrouvent sur-personnalisées, voire lésées, de certains droits et éléments de leur identité (manipulation de l'opinion publique, rumeurs, harcèlement). En 2022, il a été constaté que plus d'un milliard de clients ou de citoyens ont subis des vols d'enregistrements de données[8]. Selon une étude publiée la même année, la majorité des Américains ont le sentiment d'avoir peu de contrôle sur les données collectées par les entreprises et le gouvernement à leur sujet[9]. Ces constats sont partagés à travers le monde et démontrent les premières limites de cette sphère numérique parfois plus idyllique qu'elle ne l'est en réalité. Le constat de cette dystopie du Web 2.0 ne doit néanmoins pas éclipser le potentiel d'autres technologies

[4] Wikipédia, l'encyclopédie libre, *Technocratie*, 30 mars 2022, disponible à l'adresse suivante
[5] « Le numérique se présente ainsi tout à la fois comme témoin, catalyseur et source des bouleversements du droit », in *Annales des mines* n°18 et in *Propriété et gouvernance du numérique*, Institut Mines-Télécom, juin 2022, p.9.
[6] REINSEL D., RYDNING J., GANTZ JF., « The world keeps creating more data - now, what do we do with it all ». V. également, traduction libre de l'anglais : « la quantité de données numériques créées au cours des cinq prochaines années sera plus de deux fois supérieure à la quantité de données créées depuis l'avènement du stockage numérique », in *Worldwide global data sphere forecast 2021-2025*, consulté le 20 mars 2021 à l'adresse suivante
[7] Wikipédia l'encyclopédie libre, *Phygital*, il s'agit de la contraction des mots '*physique*' et '*digital*'.
[8] Forrester reveals lessons learned from Top 2022 data breaches. In *Forester Media*, Traduction libre de l'anglais, 24 février 2023, disponible à l'adresse suivante
[9] AUXIER Brooke et al., « Americans and privacy: concerned, confused and feeling lack of control over their personal information », in *Pew Research Center*, 15 novembre 2019, disponible à l'adresse suivante

du Web 3.0 au service de l'identité psychosociale et juridique des personnes, c'est-à-dire au service d'un Internet plus sûr.

L'évolution *phygitale* de nos interactions sociales est concrètement possible en raison de multiples révolutions technologiques successives et imbriquées. Depuis Internet et l'informatique conventionnelle 1.0 en passant par l'identité numérique 2.0, jusqu'aux récentes normes informatiques vérifiables ou infrastructures blockchains[10] décentralisées et 3.0, notre recherche étudie les impacts transversaux de chacune de ces technologies sur l'identité ainsi que les droits des personnes, des notions fondatrices de tout contrat social. D'autres technologies plus disruptives, mais encore incertaines, comme l'identité numérique génétique 4.0 et les ordinateurs quantiques 5.0 sont également analysées pour tenter de projeter cette étude dans un temps long. Depuis plus d'une décennie, une nouvelle technologie bouleverse notre rapport aux interactions et transactions monétaires en ligne : la blockchain Bitcoin. Cette récente technologie blockchain d'abord sous-jacente au bitcoin (avec un petit b tout au long de notre recherche), est ainsi devenue la source de nombreuses caricatures de tous ordres, c'est-à-dire d'autant de fantasmes que de peurs à l'égard de son fonctionnement, de ses impacts juridiques et sociétaux ou encore de ses cas d'usage métiers. Plus tard, elle a donné naissance à de multiples autres formes technologiques de blockchains, plus ou moins informatiquement décentralisées. En 2021, le marché mondial des technologies blockchains a été évalué à 4,7 milliards de dollars et pourrait représenter 164 milliards de dollars d'ici 2029[11]. Le secteur des crypto-actifs utilisant une technologie blockchain pourrait atteindre un milliard d'utilisateurs en 2030 selon un rapport publié en 2022 par la société Boston Consulting Group (BCG)[12]. L'année 1998 correspondait pour mémoire à une période analogue pendant laquelle des sociétés commerciales comme Google, PayPal ou encore Netflix ont été créées. En parallèle de ces technologies blockchains, l'identité numérique décentralisée (IND) consacre l'idée d'une identité en ligne indépendante d'une autorité centrale ou d'un tiers pour être informatiquement établie et valide. Elle peut être liée à une technologie blockchain pour stocker et gérer des données d'identité de manière décentralisée, c'est-à-dire sans avoir besoin d'une autorité centrale comme des institutions publiques ou des sociétés pour les administrer et les contrôler. Ce changement de paradigme conceptuel et technologique pour l'identité numérique propose une nouvelle transparence, accessibilité et ouverture sociale et numérique pour les internautes et les fournisseurs d'identité et de services en ligne. Lorsqu'une identité décentralisée utilise une blockchain ouverte, cette association

[10] Le terme est utilisé au pluriel tout au long de cette étude pour insister sur les multiples aspects et variantes informatiques de cette technologie.
[11] « Blockchain market size, share and Covid-19 impact analysis, forecast 2022-2029 », in *Fortune business insights*, mars 2022 disponible à l'adresse suivante
[12] « What does the future hold for crypto exchanges? » in *Boston Consulting Group*, juillet 2022, accessible à l'adresse suivante, p.10.

inédite entre un registre électronique décentralisé et des données d'identité vérifiables qu'il héberge, offre pour la première fois une identité numérique universelle[13].

Pour l'auteure et la docteure en mathématiques Aurélie Jean, les nouvelles technologies numériques sont bien souvent incomprises du grand public « *alors que nous devrions tous être des habitants éclairés et intégrés dans le pays des algorithmes, nous n'en sommes que des touristes mal renseignés, sans véritable accès ou carte pour en comprendre les reliefs et les secrets* »[14]. Tous condamnés à s'accommoder en continu à ces nouvelles technologies pour ne pas faire l'objet d'une obsolescence programmée, les technologies blockchains représentent une mutation numérique complexe face à laquelle le droit doit s'adapter, car il existe autant de blockchains et de briques technologiques sous-jacentes, que de multiples variantes organisationnelles possibles. Parce que leur gouvernance, leur force et leur encadrement juridique sont aujourd'hui inégaux. Nous évoquerons la manière dont les contrats intelligents et d'autres applications des technologies blockchains vont modifier la nature des interactions numériques entre les individus. Par exemple, depuis environ 2015, une personne disposant d'une connexion internet peut utiliser sans permission des crypto-actifs aux finalités et au fonctionnement multiples et variés. La blockchain Bitcoin (ici avec un grand B pour désigner cette technologie) a initié un mouvement d'ouverture et d'émission de (crypto)monnaies privées, c'est-à-dire légalement non reconnues par des États, ce qui a progressivement fait naître de multiples applications sous-jacentes comme des organisations autonomes et des réseaux sociaux décentralisés dont la majorité s'exécute à ce jour en toute méconnaissance des cadres légaux. Ces applications et programmes ont déjà produit des effets sociaux et juridiques nouveaux, exprimés par une « *lex cryptographia* » dès 2015[15], à l'instar d'une *lex mercatoria* ou *lex electronica*.

En parallèle, l'identité semble aujourd'hui aussi complexe à définir[16] qu'à protéger et à mettre en œuvre au sein de l'espace numérique. Le droit limite sa définition à certains de ses éléments matériels, alors que l'identité semble désormais être un concept multidimensionnel pour la sphère numérique, c'est-à-dire une identité légale statique dans l'état civil versus une identité numérique fluide en ligne. Les contextes géopolitiques incertains pourraient avoir pour effet d'accentuer le recours à ces technologies 3.0 en matière de sécurisation et de traçabilité de données impliquant toujours l'identité numérique d'une personne et d'une machine. Cette étude traite de l'identité juridique et numérique des personnes, c'est-à-dire limitée aux transactions et interactions qui la rendent strictement nécessaire. Elle est analysée en

[13] PERSON Pierre, juriste et ancien député, « L'universalité et l'ouverture, fondements même de la blockchain : vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et Monétaire », in *Rapport de l'Assemblée Nationale, quinzième législature, 2022*, p.182.
[14] JEAN Aurélie, « Les algorithmes font-ils la loi ? », version en ligne in *decitre.fr*, Humensis, 2021, position de lecture dans le livre : 22%.
[15] WRIGHT Aaron, De FILIPPI Primavera, « Decentralized blockchain technology and the rise of Lex Cryptographia », 25 mars 2015, en ligne à l'adresse suivante ; MIRANDA Maxime, « vers le développement d'une Lex Cryptographia », 13 novembre 2017, in *Droitdu.net*.
[16] MAALOUF Amin, « Une vie d'écriture m'a appris à me méfier des mots. Ceux qui paraissent les plus limpides sont souvent les plus traîtres. L'un de ces faux amis est justement 'identité' », in *Les identités meurtrières*, 2021, p.15.

d'autres termes à travers le prisme de ses finalités et de ses contextes d'utilisation et cas d'usage. Par principe, les juristes retiennent le droit pour appréhender une nouvelle technologie en recherchant les différentes façons dont il pourrait s'en emparer, mais parfois en s'éloignant de la qualification informatique des technologies, c'est-à-dire de leur compréhension informatique. Il est proposé de faire une lecture inversée, c'est-à-dire d'étudier certaines nouvelles technologies puis leurs règles applicables afin de mener une analyse juridique au plus proche de l'existant numérique. Il est également proposé au travers de la littérature scientifique portant sur ces nouvelles technologies 3.0 de porter un regard transversal sur plusieurs années d'évènements au sein de cet écosystème de l'Internet 3.0.

L'analyse de la littérature scientifique portant sur l'identité numérique démontre des recherches croissantes sur Internet liés à ces termes, depuis 2004 jusqu'à aujourd'hui[17] et une importante hausse de l'intérêt pour le concept d'identité des années 1800 jusqu'en 2014[18], avec un constat similaire pour les technologies blockchains de 2010 jusqu'à 2019[19]. Début 2023, la jurisprudence française sur l'identité compte 122 822 décisions des tribunaux et des Cours, presque exclusivement fondées sur la notion de contrôle d'identité[20]. À cette même période, 338 entreprises ont été enregistrées aux Registres des Commerces et des Sociétés (RCS) des tribunaux de commerce avec le terme blockchain dans leur objet social[21]. Ce chiffre est relativement important au regard des présumées 716 sociétés opérant sur le marché des technologies blockchains et officiellement recensées au sein de l'UE en 2022[22]. A l'échelle mondiale, 1286 projets sont recensés, la majorité se situant en Europe et aux États-Unis[23]. L'analyse graphique des cas d'usage et d'application sectoriel de ce panel montre que 20% de ces projets sont relatifs au domaine monétaire et financier, tandis que 10% au domaine de la propriété et de l'identité numérique. Pour ce qui concerne l'incontournable infrastructure blockchain de Bitcoin, il ressort de la littérature académique qu'il existe en France approximativement 22 thèses de doctorat en droit accessibles en ligne et mentionnant cette technologie[24]. Parmi elles, plus de 50% évoquent le protocole Bitcoin (retenu avec une majuscule) ou son jeton natif bitcoin (retenu avec une minuscule) sous un angle négatif ou tout au mieux relativement neutre (seulement 3 thèses sur 22 adoptent une perception neutre). Ce discernement négatif se matérialise par des références à son usage supposé intrinsèquement dédié au blanchiment de capitaux, au financement du terrorisme ou encore à la corruption des élites. À l'inverse,

[17] Concernant les recherches sur Internet liées au terme « identité numérique » voir la courbe sur *Google Trend* à l'adresse suivante ; *Id.*, pour le terme « blockchain » voir la courbe suivante
[18] « Google Books Ngram Viewer », graphique présentant le terme « identité » mentionné dans les œuvres littéraires de 1800 jusqu'à 2019, en ligne à l'adresse suivante
[19] « Google Books Ngram Viewer », graphique présentant le terme « blockchain » mentionné dans les œuvres littéraires de 2010 jusqu'à 2019, en ligne à l'adresse suivante
[20] V. Justice.pappers.fr, recherche de décisions de justice, disponible en ligne
[21] *Ibid.,* Recherche d'entreprises, disponible à l'adresse suivante
[22] Directory of European Blockchain Startups, 23 août 2022, *ChainEurope*, disponible à l'adresse suivante
[23] Analyse des données et graphiques de l'observatoire des blockchains et du développement durable, « Blockchains and Sustainable Development Observatory », 23 février 2023, disponible à l'adresse suivante Association Blockchain for Good
[24] Consulté sur Theses.fr en ligne le 04 avril 2023. Si 42 thèses sont répertoriées sur ce sujet, seules 22 thèses sont accessibles en ligne, permettant une brève analyse de leur contenu relatif à la blockchain Bitcoin

seule une minorité (32% soit 7 thèses sur 22) adopte une perception positive, celle d'une infrastructure numérique ouverte proposant une monnaie alternative relativement viable.

En Europe, la France fait figure de pionnière derrière la Suisse en matière d'encadrement juridique des crypto-actifs, avec des conséquences économiques et sociales pourtant nuancées. À l'échelle communautaire, un cadre juridique transfrontalier applicable au sein de l'UE est en cours d'adoption (étudié plus loin) et influencera de nombreuses juridictions dans les années à venir. Certaines d'entre elles envisagent d'encadrer ces nouvelles technologies pendant qu'une harmonisation juridique internationale demeure balbutiante[25]. Si cet encadrement juridique des crypto-actifs apparaît plus avancé en Europe, il semble cependant qu'il existe une motivation politique à freiner l'adoption des technologies blockchains ouvertes et publiques sur lesquelles ils reposent. Cela s'explique par la volonté de mettre en avant des versions technologiques plus fermées et contrôlables, autrement dit de favoriser le déploiement des technologies blockchains dites privées ou hybrides (qui n'intègrent pas de crypto-actifs). Les pouvoirs politiques oscillent variablement entre des discours visant à attirer les acteurs de la crypto-économie, tandis que les règlements s'intensifient au point parfois de mettre en péril les acteurs les plus fragiles de ces écosystèmes 3.0. À titre d'illustration, un rapport publié en 2022 par la Direction générale des entreprises (DGE)[26] insiste sur les prétendus avantages des technologies blockchains fermées face aux technologies blockchains publiques qui consommeraient trop d'énergie ou seraient informatiquement inefficientes.

À ce jour, les recherches académiques ont davantage porté sur la notion de crypto-actifs ou de gouvernance de systèmes décentralisés. Il s'agit de définir pourquoi et dans quelles mesures les modes de gouvernance des systèmes d'identité numérique décentralisée diffèrent des alternatives centralisées toujours utilisées. Une absence de prise de conscience politique semble persister tant pour certaines technologies blockchains que pour le concept d'identité numérique décentralisée (IND), une notion assez méconnue en raison de peu de recherches en France à son sujet[27]. Selon une étude publiée en octobre 2021[28], la France serait le 6e pays sur 33 pays à avoir publié au moins une publication scientifique sur le sujet d'identité numérique décentralisée ce qui représente seulement 6,7% du total des publications. L'intérêt pour ce nouveau terrain de recherche semble toutefois croître « *si l'on considère la croissance globale, de 2017 à 2021, le nombre d'articles* [sur l'IND] *a augmenté de 96,7 %* »[29]. Comme précédemment mentionné, certaines institutions publiques délivrent l'identité civile et

[25] PERSON Pierre, « La réglementation des cryptoactifs vit ses balbutiements. […] les prémices de cette future réglementation sont extrêmement disparates », *op. cit.* p.12.
[26] V. Guide de sensibilisation à la blockchain | entreprises.gouv.fr., 13 avril 2022, www.entreprises.gouv.fr
[27] Seulement 3 332 documents en français contenant les termes « identité décentralisée » sont référencés sur le site Academia.edu, comparé aux 152 015 trouvés en anglais, in Academia.edu | Search | identité décentralisée, recherches effectuées en ligne le 18 novembre 2021.
[28] CUCKO Spela, TURKANOVIC Muhamed, "Decentralized and self-sovereign identity: systematic mapping study", 15 octobre 2021, *Faculty of Electrical Engineering and Computer Science*, University of Maribor, Slovenia, p.10, disponible en ligne
[29] *Ibid.* p.9.

racine des citoyens et sont en même temps confrontées au défi de la numérisation des interactions sociales. Se pose ainsi la question de savoir comment continuer à assurer l'exercice et la protection de l'identité des personnes et de leurs droits à l'ère numérique, depuis l'État vers un « *Big Data* »[30]. Pour illustration, certaines institutions comme la société IN Groupe (ex-Imprimerie Nationale)[31] propose depuis plus de 500 ans de matérialiser l'identité civile des personnes sur des supports physiques de confiance (CNIe, passeports). Toutefois, l'essor des comportements et des technologies du numérique a entraîné une redéfinition du positionnement de cette institution depuis le marché de l'identité physique et régalienne vers le marché *phygital* et parfois exclusivement numérique. Cette transition stratégique et technologique entamée avec succès par cette institution amènerait d'ici plusieurs décennies le numérique à se substituer aux besoins de titres d'identité physiques. Une telle éventualité entraînerait des conséquences irréversibles à mettre en perspective face à des risques de dérives technologiques, comme la suppression numérique d'identités en ligne. Envisager les technologies 3.0 comme une garantie pour l'identité numérique d'une personne, apparaît par conséquent comme essentiel. Il devient d'autant plus nécessaire de recréer la confiance à l'heure du partage généralisé des données et de la multiplication des services en ligne. Par exemple, chaque citoyen en acceptant les conditions générales d'utilisation peut créer en quelques clics de nombreux comptes dont la suppression effective et définitive des données peut prendre plusieurs mois. S'il est légitime de considérer que de grandes entreprises technologiques poursuivent leurs finalités commerciales, celles-ci doivent plus que jamais respecter le cadre légal et règlementaire de leurs activités aux fins d'éviter des dérives comme en témoignent les célèbres affaires Snowden en 2013[32] et Cambridge Analytica en 2018[33]. Les applications et les grandes entreprises étant devenues de facto des contrôleurs d'identité, les utilisateurs ont progressivement perdu le contrôle sur leurs données et identités numériques et ainsi augmenté leur dépendance informatique et sociale. Par conséquent, l'identité décentralisée pourrait représenter un contre-pouvoir à la centralisation des données d'identité et à ses dérives. La société numérique qui rencontre aujourd'hui une révolution d'envergure avec l'adoption des nouvelles technologies blockchains et l'émergence de l'identité numérique décentralisée semble soulever à tout le moins trois questions majeures :

(i) La décentralisation informatique et sociale est-elle nécessaire, utopique ou bénéfique pour une nouvelle confiance numérique ? Les technologies 3.0 sont-elles incompatibles avec les règles de droit ?

---

[30] 'Métadonnées' ou 'données massives', constituant d'importants renseignements sur nos habitudes, comportements, tâches

[31] Devenue la société anonyme 'Imprimerie nationale SA' en application de la loi n° 93-1419 du 31 décembre 1993, modifiée par le décret d'application n°2006-1436 du 24 novembre 2006, disponible à l'adresse suivante

[32] Wikipédia, l'encyclopédie libre. « Snowden » (film), consultation le 26 juin 2022 à l'adresse suivante

[33] Cambridge Analytica filiale de Facebook (aujourd'hui *Meta*) a contribué en 2016 à la campagne électorale du Président des Etats-Unis Donald Trump - ainsi que celle de Boris Johnson en Angleterre - en raison de la récolte, l'analyse puis l'influence des données d'utilisateurs des réseaux sociaux Facebook et Instagram. Pour illustration, cette société avait plus de 5000 points de données concernant chaque électeur américain. Le psychologue et docteur Michal Kosinski a prouvé qu'à partir d'un minimum de 68 « likes » sur Facebook, il est possible de prédire la couleur de peau (efficace à 95%), l'orientation sexuelle (88%) et les convictions politiques (85%) d'une personne. Wikipedia contributors, l'encyclopédie libre, 17 mars 2023, disponible en ligne

(ii) Les technologies blockchains et l'identité décentralisée caractérisent-elles une révolution 3.0 pour l'identité psychosociale et juridique des personnes ?

(iii) Les internautes préféreront-ils une infrastructure informatique décentralisée, résiliente, mais monofonctionnelle et peu conforme aux règles de droit, ou bien une infrastructure centralisée dotée de multiples fonctionnalités et conforme aux règles de droit, mais peu résiliente ?

Il est autorisé de penser que les technologies 3.0 permettront de s'orienter depuis une forme d'identité numérique sauvage vers une identité numérique graduellement contrôlée par les internautes. Toutefois, pour nuancer ce degré de contrôle, en réalité variable selon les contextes en ligne, il faut rappeler que derrière toute machine ou protocole informatique il reste la main de l'Homme. Il convient ainsi de se demander s'il est pertinent de créer un droit spécifique aux phénomènes de décentralisation informatique. Depuis déjà plus d'une décennie, les internautes peuvent créer et partager de la valeur en pair à pair sur Internet grâce aux technologies blockchains sans faire confiance à des tiers (banque, serveurs informatiques). Le législateur doit-il encourager ou réduire cette libéralisation de l'identité en ligne, désormais exacerbée par la possibilité d'un pseudo-anonymat (développé plus loin) et d'une désintermédiation des échanges ? L'avènement d'un nouveau droit cryptographique 3.0 est-il nécessaire et viable ? L'hypothèse retenue est que les technologies blockchains et d'identités numériques permettraient au mieux de rendre plus démocratiques les droits des personnes en ligne en renforçant leurs libertés. Ainsi, les présentes recherches nous mèneront à comprendre l'urgence de la mise en place de solutions informatiques plus décentralisées pour permettre l'avènement d'un véritable droit cryptographique. Cette recherche étudie dans quelles mesures une décentralisation partielle de l'identité numérique primaire est nécessaire, et si une décentralisation totale de l'identité numérique secondaire est souhaitable. Il est également proposé de ne pas opposer les deux schémas d'identité numérique, l'un centralisé et l'autre décentralisé, mais de les concevoir de façon complémentaire et hybride[34]. L'identité décentralisée est une opportunité d'intérêt général qui permettra de fournir une identité unique pour tous les écosystèmes numériques et les services en ligne (abolition des multiples noms d'utilisateur et mots de passe), des paiements plus fluides et personnalisés (éventuellement couplés aux crypto-actifs), des messageries et communications plus sécurisées et respectueuses de la vie privée (réseaux sociaux décentralisés), c'est-à-dire un Internet plus sûr, neutre et respectueux des personnes.

Nous déterminerons le potentiel des technologies blockchains existantes relancées au fur et à mesure de l'adoption de nouvelles technologies, la Commission européenne s'étant prononcée en faveur d'une identité numérique européenne harmonisée et partiellement décentralisée « *une identité électronique*

[34] Une identité numérique hybride fait référence à une identité numérique à la fois issue du Web 2.0 et du Web 3.0. Elle est issue du premier, car elle est souvent dérivée d'une identité physique matérialisée par un titre d'identité. Elle est également issue du second grâce aux standards de l'identité décentralisée que consacre cette thèse. En d'autres termes, sur le plan informatique, une *identité numérique hybride* est partiellement décentralisée, c'est-à-dire *semi-décentralisée* ou inversement *semi-centralisée.* V. Glossaire.

publique (eID) universellement acceptée est nécessaire pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils souhaitent sans avoir à utiliser des plateformes non apparentées pour ce faire et à partager inutilement des données personnelles avec celles-ci »[35]. Nous déterminerons également comment ces technologies 3.0 permettront de fournir une preuve d'existence universelle en conformité avec les droits et l'identité des personnes. Nous partirons de l'hypothèse qu'un encadrement juridique devrait être nécessaire pour certaines solutions 3.0, notamment dans le domaine financier et monétaire, mais qu'une intervention juridique entendue sur mesure et proportionnée devrait toutefois tolérer l'expérimentation monétaire décentralisée que représente la technologie blockchain la plus ancienne, Bitcoin. Si la règlementation doit assurer la diffusion de certaines garanties légales pour ses utilisateurs, la blockchain Bitcoin leur assure d'ores et déjà une confiance informatique. Les décideurs et législateurs doivent prêter attention à concevoir des règles de droit cohérentes et au plus proche du vécu et des besoins socio-technologiques de la société « *l'Europe doit désormais prendre la tête du processus d'adoption et de normalisation de la nouvelle génération de technologies : blockchain, supercalculateurs, technologies quantiques, algorithmes et outils permettant le partage et l'utilisation des données* »[36]. Chaque nouvelle technologie ne représente qu'un nouvel outil et support au service de l'Homme et de ses valeurs, le Web 3.0 ne serait ainsi qu'un nouveau support et vecteur de communication[37], comme est le papier depuis des siècles. Le philosophe français Bernard Stiegler rappelle que « *tout objet technique est pharmacologique : il est à la fois poison et remède. Le pharmakon est à la fois ce qui permet de prendre soin et ce dont il faut prendre soin, au sens où il faut y faire attention : c'est une puissance curative dans la mesure et la démesure où c'est une puissance destructrice* »[38]. Par analogisme, toute nouvelle technologie informatique, quels que soient son support et son contenu, peut faire l'objet de manipulations, de désinformations ou être source d'inégalités[39]. Si les nouvelles technologies 3.0 n'échappent pas à cette réalité, elles peuvent toutefois s'en écarter en fournissant des preuves de fiabilité et de confiance. Une certitude est possible, toute nouvelle technologie prend souvent plus de temps qu'il n'y paraît pour mûrir et atteindre une adoption sociale satisfaisante.

À la lumière de ces propos introductifs qui seront adossés aux expériences de terrain menées au sein de la société IN Groupe (antérieurement l'Imprimerie Nationale), et de l'écosystème français du Web 3.0 depuis 2020, nous proposons dans une première partie d'étudier l'épistémologie de l'identité et des

[35] Traduction libre de l'anglais. « Communication Shaping Europes Digital Future », consulté en ligne le 6 décembre 2021, p.6.
[36] *Ibid*, p.7.
[37] JEAN Aurélie, « Les algorithmes font-ils la loi ? », « l'algorithme n'est pas coupable pour la simple et bonne raison qu'il n'est ni une personne physique ni une personne morale, et que ce sont bien des hommes et des femmes qui décident de l'usage, de l'implémentation et des effets qui en résultent, et qui sont donc les seuls responsables », *op. cit*., in *Humensis*, 2021, position de lecture dans le livre : 19%.
[38] STIEGLER Bernard, « Questions de pharmacologie générale. Il n'y a pas de simple pharmakon » in *Psychotropes*, 2007/3-4, Vol. 13, pp.27-54, disponible à l'adresse suivante
[39] MAZEREEUW Faustine, « Le numérique est une gigantesque machine à renforcer les inégalités », in *Les Echos Start*, publié le 17 février 2023, interview par Mathilde Saliou, journaliste spécialiste du numérique chez Next Inpact.

technologies blockchains à travers le prisme de la philosophie, des sciences sociales et de l'informatique (**Partie I**, **Titre 1**, chap. 1 et 2). Nous examinerons l'équilibre qui existe entre la recherche de stabilité du droit et les constantes mutations technologiques et sociales auxquelles il se confronte, à l'appui de promesses et défis de la société numérique 2.0 et d'une transition vers des technologies 3.0 de décentralisation et d'émancipation (**Titre 2**, chap. 1 et 2). Dans une seconde partie, nous introduirons le concept avec ses enjeux sociétaux d'une identité numérique décentralisée au service de l'universalité des droits des personnes (**Partie II**, **Titre 1**, chap. 1 et 2) avant d'analyser plusieurs cas d'usage et projets transversaux et spécifiques, parfois déjà déployés en faveur de l'adoption d'une identité numérique 3.0 (**Titre 2**, chap. 1 et 2).

I/ Epistémologie de l'identité juridique et de la technologie blockchain

Titre 1 : Le périmètre complexe et ductile de l'identité

Chapitre 1 : L'identité comme objet philosophique, social et juridique implexe

1.1 Définir les champs de l'identité et de ses mécanismes

Cette première partie a pour ambition d'appréhender les différents sens que peut recouvrir la notion d'identité. Il s'agit d'évaluer les différentes définitions possibles qui ont pu lui être attribuées au fil de l'évolution de la société désormais sujette à une numérisation progressive. Une analyse transversale de l'identité s'impose depuis son appréhension philosophique et sociale, jusqu'à sa définition numérique et juridique. Ces dernières décennies, le concept d'identité est évoqué de façon grandissante à travers diverses disciplines, informatiques, politiques, sociales ou encore juridiques. Ces disciplines sont unanimes quant à la difficulté d'appréhension et de définition du concept d'identité. Autrement dit, aucune vérité ne peut être admise pour une définition générale qui pourrait satisfaire toutes les sciences. Il existe autant de définitions de la notion d'identité que d'auteurs écrivant sur le sujet en raison de multiples situations différentes, avec des sens aussi différents que contradictoires. Au même titre qu'une technologie, l'identité ne pourrait être qu'un outil social au service d'une perception et d'une attribution sociale individuelle et collective. Pour étudier les contours et différents sens de cette définition qui peut paraître insaisissable, cette partie traite du terme d'identité à travers ses multiples facettes qui sont présentées de façon non limitative dans le tableau ci-après selon nos recherches et notre compréhension :

Nombre total d'équivalences trouvées dans la littérature	**Type de vocabulaire rattaché au terme « identité » issu de la littérature scientifique**	**Catégorie 1 : *Identité philosophique***	**Catégorie 2 : *Identité sociale***	**Catégorie 3 : *Identité juridique***
1	*Identité vécue*	X	X	
2	*Identité morale*	X	X	
3	*Identité subjective*	X	X	
4	*Identité psychologique*	X	X	
5	*Identité perçue*	X	X	
6	*Identité revendiquée*	X	X	
7	*Identité élémentaire*		X	X
8	*Identité juridique*			X
9	*Identité civile, légale*			X

10	*Identité étendue*	X	X	X
11	*Identité racine*			X
12	*Identité biologique*	X	X	
13	*Identité génétique*	X	X	X
14	*Identité plurielle*	X	X	
15	*Identité singulière*	X	X	X
16	*Identité relative*	X	X	
17	*Identité contextuelle*	X	X	
18	*Identité sociale*		X	X
19	*Identité collective*		X	X
20	*Identité temporelle*	X		
21	*Identité corporelle*		X	X
22	*Identité culturelle*	X	X	X
23	*Identité étymologique*	X	X	
24	*Identité anthropologique*	X	X	X
25	*Identité de genre*	X	X	X
26	*Identité en silo*	X	X	
27	*Identité en contexte*	X	X	
28	*Identité solidaire*	X	X	X
29	*Identité(s) meurtrière(s)*	X		
30	*Identité négociée*	X	X	
31	*Identité narrative*	X	X	
32	*Identité générique*		X	X
33	*Identité spécifique*	X	X	X
34	*Identité choisie*	X	X	
35	*Identité administrative*			X
36	*Identité dérivée*	X	X	
37	*Identité pivot*			X
38	*Identité régalienne*			X
39	*Identité primaire*			X
40	*Identité secondaire*	X	X	

Total	**~ 40 occurrences régulièrement citées dans la littérature scientifique**	**28**	**31**	**20**

L'analyse de ce tableau prospectif permet d'émettre l'hypothèse selon laquelle l'identité est majoritairement reconnue dans la littérature scientifique par une acceptation philosophique, sociale et juridique. Cette rapide comparaison permet aussi de regrouper les adjectifs et les termes qui renvoient à des concepts d'identité proches ou similaires. Il est généralement admis que l'identité d'une personne, d'une organisation ou d'une chose fait référence à tout ce qui est susceptible de les caractériser. Dans une acceptation générale et pour les individus, l'identité englobe aussi bien ses caractéristiques physiques (biométriques)[40] que d'autres caractéristiques telles que ses interactions sociales, ses expériences, ses titres ou biens. Dès lors, il existe une infinité d'attributs qui composent nos identités en tant qu'êtres humains, la plupart d'entre eux étant en constante évolution, ce qui explique le caractère ductile de l'identité. Étant donné l'importante quantité d'attributs et de facteurs qui contribuent à l'identité des personnes, il devient complexe de les organiser, c'est-à-dire de les collecter, les stocker et de les répertorier au sein d'un unique espace physique ou numérique. Pour cela, le recours à des acteurs de confiance - désignés en tant que tiers de confiance (entreprises, institutions étatiques) - est historiquement nécessaire pour fournir aux personnes une identité stable et de confiance, ces derniers assurant ainsi une gestion et une distribution centralisée des attributs de leur identité. Les définitions académiques et littéraires de la notion d'identité rendent compte de son aspect multidimensionnel. Selon le dictionnaire en ligne de l'Académie Française, le terme « identité » possède quatre sens possibles. Le premier se réfère à une « *exacte ressemblance entre des êtres* (...) *qui ont une existence distincte* », il est ainsi fait référence à une identité au sens physique du terme. Le deuxième fait référence à une identité plus abstraite et relative, une identité de nature « *caractère de ce qui ne fait qu'un ou ne constitue qu'une seule et même réalité* (...) ». Le troisième fait référence à une identité psychosociale, c'est-à-dire sur ce qui « *fonde l'individualité* ». Enfin, la dernière définition renvoie à une identité juridique, c'est-à-dire à la « *personnalité civile d'un individu, légalement reconnue ou constatée établie par différents éléments d'état civil* (...) ». L'encyclopédie définit plus généralement l'identité comme le « *caractère permanent et fondamental de quelqu'un, d'un groupe qui fait son individualité, sa singularité.* »[41], ce terme étant issu du latin « *idem* » signifiant « *le même, la même, la même chose* » lorsqu'il est employé comme adjectif ou pronom. Cette traduction latine et littérale du terme identité a été attribuée au travail de réflexion et de traduction mené par le philosophe français Paul Ricœur dans son ouvrage « *soi-même comme un autre* »[42]. Il apparaît qu'aucune discipline scientifique n'affronte à elle seule cette question

[40] V. Titre II, chap. 1, 1.3
[41] Larousse Éditions, « Identité » (bas latin identitas, -atis, du latin classique idem, le même), consulté en ligne le 18 août 2021.
[42] RICOEUR Paul, « soi-même comme un autre », consulté le 18 août 2021, ISBN 2-02-011458-5, disponible à l'adresse suivante

historique et rhétorique qu'est l'identité, en essayant d'y apporter une définition précise et universelle. Pour définir l'identité, il faut adopter plusieurs regards en raison des différentes disciplines parfois complémentaires, parfois incompatibles. Bien que présente dans de nombreux corpus et réflexions en sciences sociales, la notion d'identité reste fortement plurivoque et énigmatique. L'identité est le bon moyen pour proposer une analyse pluridisciplinaire, non pas d'une réalité dont elle rend compte, mais de ses multiples réalités et contextes d'utilisation. Plusieurs questions peuvent être soulevées, par exemple est-il illusoire d'essayer de définir l'identité ? Existe-t-il une ou plusieurs identités ? Dans quelles mesures les cas d'usages de l'identité permettent-ils de définir ses contours ? Quelle assimilation ou confusion existe-t-il entre l'identité physique, l'identité sociale et l'identité juridique ? La dématérialisation d'une identité physique affecte-t-elle son intégrité ou seulement sa substance ?

Il est possible de percevoir l'identité comme une notion multifacette dans laquelle chaque science vient puiser ses conclusions[43], ce qui permet de l'appréhender à la fois avec globalité et pluridisciplinarité. Le rôle des sciences est de proposer une identification des personnes assez générale et impersonnelle à l'échelle individuelle des personnes. Ainsi, selon les sciences abordées, la notion d'identité n'aura pas la même signification ni la même portée. Par exemple, la psychologie évoque l'identité personnelle, la sociologie l'identité de groupes et le droit l'identité juridique. Cette essence polysémique du terme identité fait appel à une multitude de contextes et de situations qu'il convient d'étudier avec précaution pour ne pas recourir à une généralisation systématique du concept d'identité. Il semble toutefois qu'un degré de généralité soit nécessaire pour que toute personne puisse comprendre de quoi il s'agit au regard des deux approches généralement admises au sein de l'univers physique et numérique :

(i) une première approche tend à ce que chaque personne possède une identité unique. Toutes les données générées par une personne lui sont attribuables de façon directe ou indirecte. Selon cette approche, chaque donnée est unique puisqu'elle représente un ou plusieurs aspects de l'unicité de l'identité de son propriétaire. Une telle définition suppose un caractère inaltérable de l'identité à travers le temps, ce qui ne peut être le cas en raison de l'évolution de l'identité d'une personne dans le temps.

(ii) Une seconde approche envisage qu'il existe une identité en contexte, c'est-à-dire autant d'identités que de besoins d'identification au sein d'une société avec par exemple une naissance inscrite dans un registre d'état civil, un accès à un compte en ligne via un identifiant numérique ou un emploi avec la preuve nécessaire d'une qualification professionnelle par un diplôme.

Ces deux approches et tentatives de délimitation de l'identité peuvent s'entendre par les notions d'identité racine et d'identité étendue. La première est plus importante et fondatrice, mais son affirmation a tendance à progressivement s'effacer au sein d'une société ultra numérisée qui semble

[43] Phrase librement inspirée d'une maxime de Voltaire : « chaque science, chaque étude, a son jargon inintelligible qui semble n'être inventé que pour en défendre les approches », in *Œuvres complètes,* Garnier tome8.djvu/323 - Wikisource, disponible en ligne

lentement valoriser les attributs d'identité étendus des personnes. En effet, il semble être accordé plus d'importance à l'ère de l'interconnectivité aux éléments d'une identité étendue et secondaire plutôt qu'aux attributs d'identité primaire et racine fixés dans un État de droit. Depuis l'émergence de la mondialisation, l'inflation des échanges et des interactions humaines a également suscité une mondialisation des identités. La société numérique engendre divers bouleversements de fond et de forme, ainsi l'informatique contribue sans cesse à accroître le(s) réceptacle(s) d'informations disponibles de chaque personne évoluant dans l'espace numérique. Comme le souligne l'Académicien et écrivain franco-libanais Amin Maalouf « *bien que la population de la planète ait presque quadruplé en cent ans, il m'apparaît que, dans l'ensemble, chaque personne est plus consciente que par le passé de son individualité, plus consciente de ses droits,* (…), *plus attentive à sa place dans la société* (…) *aux pouvoirs dont elle dispose, à son identité* (…) » ; « (…) *on peut légitimement se demander si la mondialisation ne va pas conforter la prédominance d'une civilisation ou l'hégémonie d'une puissance* [comme les GAFAM / BHATX[44] ou plus largement les États-Unis] »[45]. Il est ainsi primordial qu'un corpus législatif[46] encadre et protège les individus de tout abus de leur identité en ligne. Un droit à une identité numérique émerge. Ce phénomène de mondialisation numérique semble néanmoins bénéfique pour l'Humanité dès lors qu'il n'enferme pas les individus dans des appartenances et des considérations identitaires qu'ils n'ont pas délibérément choisies et acceptées. À l'ère digitale, la capacité à définir, collecter, présenter puis vérifier des sous-ensembles d'informations d'identité de manière standardisée et reconnue par les services en ligne représente un processus social et informatique dont le but est de permettre à chaque individu de prouver en ligne qui il est parmi d'autres individus. Avant d'étudier ce nouvel espace, il est important de définir ce processus que traverse chaque identité numérique et qui se déroule en deux temps distincts, le premier étant l'identification et le second l'authentification. Le premier temps consiste à convaincre une personne que ses informations peuvent être capturées de manière fiable par un ensemble d'identifiants numériques personnels désignés comme « attributs » ou « données ». Cette capture « d'attributs » repose souvent sur des attestations matérialisées dans un ou plusieurs certificats officiels - généralement physiques comme une carte d'identité ou un passeport - délivrés puis certifiés par une entité publique à laquelle chaque personne peut légitimement faire confiance. Ainsi, à l'origine de toute identité et identification se trouve en principe une source d'autorité publique reconnue par des tiers vérificateurs. Le second temps d'authentification consiste à ce qu'un internaute partage et vérifie - à la suite d'une demande de vérification et pour accéder à des services numériques - ses attributs d'identification déjà préalablement enregistrés lors de son inscription. De cette façon et en théorie, grâce à la vérification des documents d'état civil d'une personne puis à la génération

[44] GAFAM est l'acronyme des cinq plus grandes entreprises du Web américain - *Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft* dominant le marché numérique mondial en proposant des systèmes d'identification numériques à leurs utilisateurs. *BHATX* est l'acronyme de *Baidu*, *Huawei*, *Alibaba*, *Tencent*, *Xiaomi*, les cinq plus grandes entreprises technologiques chinoises.
[45] MAALOUF Amin, « Les identités meurtrières », *op. cit.*, p.133.
[46] Il est fait référence à différents droits fondamentaux étudiés au cours de cette recherche, notamment au droit au respect de la vie privée, au consentement au droit à l'oubli ou déréférencement spécifié dans le RGPD, au secret des correspondances ou des affaires, au droit à l'identité, à la lutte contre le harcèlement en ligne, la diffamation et les rumeurs numériques.

d'identifiants numériques personnels propres à chaque internaute, ces preuves numériques permettent d'accéder à nouveau auxdits services en ligne, en leur assurant que les personnes sont bien qui elles prétendent être. Si certaines de ces premières définitions et considérations liées au concept d'identité font régulièrement débat en sciences sociales avec leurs contestations, un certain consensus émerge pour une nécessité de définir la notion d'identité. Comme le propose avec pertinence le docteur en philosophie et sciences sociales Alex Mucchielli, l'identité serait un « *ensemble de significations apposées par des acteurs sur une réalité physique et subjective, plus ou moins floue, de leurs mondes vécus, ensemble construit par un autre acteur. C'est donc un sens perçu donné par chaque acteur au sujet de lui-même ou d'autres acteurs* »[47]. Cette définition est assez générale pour faire émerger un premier constat systémique propre à l'identité, permettant de se distinguer d'autrui en affirmant sa propre singularité. De cette façon, l'identité semble contextuelle, c'est-à-dire unique et propre à chaque situation. Depuis plusieurs années, certains juristes évoquent une « *libre autodétermination informationnelle des personnes* »[48], également mentionnée dans une étude annuelle du Conseil d'État en 2014[49]. En pratique, cela implique que les interactions sociales d'un individu ne soient pas conditionnées et altérées par une utilisation imprudente de ses données à caractère personnel, notamment par des tiers de confiance. Cette nouvelle forme d'identité subjective est aujourd'hui plus que jamais au centre de toutes les attentions et pourrait, à long terme, contribuer à redéfinir ce rôle historique d'attribution de l'identité par un État de droit et ses institutions. Une personne est une somme de différentes motivations dont chacune subit un changement permanent, au gré de ses interactions sociales. En pratique, l'identité sociale est bien souvent vécue « (…) *comme un tout* »[50] par les personnes, c'est-à-dire qu'en cas d'atteinte par un tiers, c'est « *toute la personne qui vibre* [qui est atteinte] ». Nous soutenons ainsi une vision duale de l'identité, à la fois racine et en contexte, à la lumière des technologies blockchains[51] et de l'identité numérique décentralisée (IND) qui est étudiée plus loin.

1.1.1 Les contours de l'identité au regard de la philosophie

Il apparaît essentiel de déterminer les conditions selon lesquelles la notion d'identité peut exister. Le philosophe américain Quine Willard explique qu'une identité implique préalablement une insertion d'existence propre à une chose, à un concept ou encore à une personne « *il n'existe pas d'entité sans une identité* »[52]. Cette expression signifie que l'identité est l'essence même de toute chose, aucune définition

[47] MUCCHIELLI Alex, « L'identité », Ed. Que sais-je ? PUF 2009, disponible à l'adresse suivante
[48] EYNARD Jessica, « L'identité numérique ; quelle définition pour quelle protection » , p.39.
[49] CE, Recommandation, « Renforcer la place de l'individu dans le droit à la protection de ses données (« autodétermination informationnelle ») pour lui permettre de décider de la communication et de l'utilisation de ses données à caractère personnel » *Conseil d'Etat, Étude annuelle 2014 - Le numérique et les droits fondamentaux,* consulté en ligne le 20 novembre 2021.
[50] MAALOUF Amin, « Les identités meurtrières », *op. cit*., p.34.
[51] Le terme est utilisé au pluriel tout au long de cette étude pour insister sur les multiples aspects et variantes informatiques de cette technologie. *v. infra*, I, Titre 1, 2.3.1.1
[52] WILLARD Quine, « Relativité de l'ontologie et autres essais », 1969, No entity without identity, traduit de l'anglais par Jean Largeault, Paris, Aubier, 1977, p.35.

ni existence n'est possible sans l'allocation préalable d'une identité. Pour certains individus, les caractéristiques sont facilement identifiables comme leurs traits physiques tandis que pour d'autres elles sont plus complexes à déceler comme leurs traits psychiques ou leur capacité d'apprentissage. Ce constat s'applique d'ailleurs aux animaux dont certaines capacités peuvent excéder la simple existence de leur identité corporelle. Bien que chaque être vivant d'une communauté animale donnée soit génétiquement unique, l'ensemble de cette population possède une faculté collective propre : chaque castor est unique, mais tous possèdent la faculté innée de savoir construire des barrages dès leur naissance. Ici, identité personnelle et collective se côtoient. Cet aspect universel de l'identité était déjà évoqué par Aristote : « (…) *à ce qui est chez l'homme technique, sagesse, intelligence correspond chez certains animaux quelque autre faculté naturelle du même genre* »[53]. La notion d'identité ne serait-elle qu'une question de perspective : un serpent qui mue garde-t-il la même identité lors de ce processus de transformation physique ? Cette question peut se transposer à la nature humaine, à l'unique condition que ce serpent soit aussi doté d'une « *conscience propre* »[54], ce qui n'est pas le cas. Pour l'Homme, la conscience est désignée par la médecine comme un processus de métacognition « *la conscience est ce qui nous permet de connaître notre identité* (...) *qui s'inscrit dans un contexte relationnel qui fait que d'autres cerveaux qui nous font face nous reconnaissent comme une certaine personne et non une autre* »[55]. En accord avec ce principe, le philosophe français Paul Ricœur affirme qu'une identité personnelle est intersubjective, c'est-à-dire qu'elle se développe toujours dans un rapport mutuel avec d'autres individus[56]. Plus précisément, il s'agit de ne pas se confondre avec l'autre, mais de se co-construire grâce à lui. De cette façon, nous sommes tous des Hommes comme les autres, grâce aux autres, et tout en possédant notre propre « *soi* » face à « *autrui* ». Cette relation d'équilibre, social et empathique, fait naître la notion d'identité sociale comme nous l'envisageons dans notre étude. Selon le sociologue français Claude Dubar, il existe deux principaux courants de pensée concernant le concept d'identité, l'un dit « *essentialiste* » et l'autre « *nominaliste* »[57]. Le premier se fonde sur des croyances originelles intrinsèques à tout individu, presque transcendantes et selon lesquelles l'identité permet une distinction fondamentale entre les individus avec une forme de permanence dans le temps. Le second réfute cette permanence et distinction spécifique des individus pour se concentrer sur les modes d'identification de l'identité, c'est-à-dire ses éléments matériels d'expression. Une mobilisation mixte de ces deux courants est utilisée dans cette recherche afin de comprendre l'identité vécue des personnes au plus proche du réel. L'histoire de la philosophie occidentale considère majoritairement que l'humain est une personne en raison de sa faculté à décider en toute autonomie et en toute conscience, c'est-à-dire avec une capacité à rationaliser ses actes selon son propre système de valeurs, lui-même défini simultanément de façon

[53] BOUFFARTIGUE Jean, « Les animaux techniciens, réflexions sur l'animal faber vu par les anciens », 2006, en ligne, Université Nice-Sophia Antipolis, consulté le 20 août 2021.
[54] MUCCHIELLI Alex, « L'identité », *op. cit.*, pp.79-80.
[55] GAYON Jean et al., « L'Identité, dictionnaire encyclopédique », Ed. Gallimard, 2020, in *Follio Essai*.
[56] RICOEUR Paul, « Soi-même comme un autre », Ed. Seuil 1990, ISBN 2-02-011458-5, disponible en ligne
[57] DUBAR Claude, « La crise des identités : l'interprétation d'une mutation », 2010, PUF, pp.2-6, disponible en ligne

collective et individuelle. Ce système de valeurs qui fonde l'identité personnelle repose en principe sur la continuité entre la mémoire passée et présente d'une personne, c'est-à-dire sur sa faculté de raisonnement et sur ses propres souvenirs ainsi qu'expériences personnelles[58]. Par conséquent, l'identité dont l'Homme peut se prévaloir existe grâce à sa capacité de (re)mémorisation du passé tout autant que d'anticipation de l'avenir[59]. C'est aussi ce que le neurophysiologiste français Alain Berthoz désignait comme un « *voyage mental dans le temps* »[60].

Cependant, il s'agit de ne pas confondre l'identité vécue d'une personne, c'est-à-dire son identité psychologique, de son identité primaire et légale évoquée plus loin. La première est une représentation identitaire, partiellement façonnable, profonde et en constante mutation. La seconde ne nous appartient pas et peut représenter une forme d'enfermement de notre identité psychologique[61]. Notre identité unique et globale subirait une confrontation et négociation permanente entre ces deux identités. Nous retiendrons l'hypothèse selon laquelle l'identité est en permanence négociée. Pendant la petite enfance et dès qu'un enfant débute l'apprentissage de la parole, s'enclenche le système d'identification et d'apprentissage de son propre nom. Cette programmation bien plus large par l'éducation consiste à greffer des qualités et des défauts sur ce que nous acceptons plus tard comme être notre identité. Ce premier mécanisme de création identitaire, d'une première identité, contribue selon le philosophe danois Søren Kierkegaard à annihiler l'être profond d'une personne : en attribuant des étiquettes aux personnes, cela contribue à annihiler toutes les autres choses qu'elles pourraient être sans ces étiquettes sociales. Face à ce constat, que devenons-nous faire de toutes ces tentatives d'assignation identitaires dont nous faisons sans cesse l'objet ? Il semble que nos revendications identitaires traduisent notre désir de changer certaines revendications identitaires déjà existantes. Étymologiquement, l'identité permet de caractériser deux ou plusieurs êtres qui sont de même nature. En latin, être « soi-même » se désigne par le terme « *ipse* » ou « *ipséité* » en français[62]. L'ipséité représente ainsi une manière d'exister et d'être. Il s'agit d'une forme de fidélité à soi-même, de constance autonome, au-delà d'une simple permanence à soi. Pour le philosophe français Paul Ricoeur, l'ipséité constitue une composante majeure de l'identité d'une personne. Il décline ainsi l'identité avec deux notions, l'une « *identité-idem* » et l'autre « *identité-ipse* ». La première représente une identité stable dans le temps, inchangée et immuable, et la seconde constitue

[58] LOCKE John, médecin et philosophe anglais décrivait en 1969 qu'une « personne est un être intelligent pensant, qui a de la raison et de la réflexion, et qui peut se considérer comme lui-même, la même chose pendante, à différents moments et en différents lieux », The Works, vol. 1 An Essay concerning Human Understanding Part 1 | Online Library of Liberty, consulté en ligne le 20 août 2021.
[59] Pour John LOCKE, l'individu est constitué par la continuité du corps et la personne par la continuité de sa conscience : « L'identité d'une personne s'étend aussi loin que la conscience peut atteindre rétrospectivement toute action ou pensée passée » in *Essai sur l'entendement humain*, chap.27, II.
[60] BERTHOZ Alain, « Anticipation et prédiction », Odile Jacob, 2015.
[61] En France, l'identité pivot d'une personne (son nom, prénom, sexe) ne lui appartient pas. Cela peut engendrer un enfermement identitaire pour certaines personnes dont l'identité pivot et primaire ne correspond plus à leur identité psychologique (personnes transgenres, personnes dont le nom de famille est difficile à porter). Si cet exemple semble anecdotique lorsqu'appliqué en France, il prend tout son sens dans le cadre d'un pays et d'un État autoritaire : l'identité pivot et racine des personnes peut être fabriquée de façon à enfermer les personnes dans des bulles identitaires strictement contrôlées et assujettis à une vision spécifique de l'identité (illustration par exemple pendant la guerre Russie - Ukraine avec l'endoctrinement des personnes).
[62] RICOEUR Paul, *op. cit.*, consulté le 18 août 2021, disponible en ligne

une forme de maintien dans sa projection de soi, malgré certains changements de caractères de l'identité dans le temps. Pour mieux comprendre les contours de la dimension philosophique de l'identité, l'expérience de pensée philosophique du Bateau de Thésée[63] régulièrement évoquée en littérature s'avère d'une précieuse aide. Utilisé depuis l'Antiquité, cet aphorisme a été repris par de nombreux philosophes modernes et porte le nom du héros grec Thésée. Cette légende expose que son bateau fut réparé un grand nombre de fois, au point de ne plus avoir une seule pièce d'origine. Il est ainsi question de savoir si la reconstruction planche par planche de ce bateau de Thésée engendre une dégradation voire une disparition de l'identité originelle de ce dernier. En d'autres termes, reste-t-il le même bateau qu'en amont de sa restauration ? Au fond, cette problématique peut aussi trouver à s'appliquer au concept d'identité et à la définition que chaque individu peut lui donner. Ces deux aphorismes soulignent une forme de lien paradoxal entre le changement et la permanence, c'est-à-dire entre l'identité d'une chose face à son propre changement dans le temps, au point de se redéfinir dans un temps long. Dès lors, l'appréciation philosophique de l'identité semble particulièrement dépendante d'une approche subjective, c'est-à-dire reposant toujours sur la perception de celui qui l'étudie. Le philosophe français Paul Ricoeur déjà cité perçoit l'identité comme un « *traqueur d'individualité* » incubée dans une « *identité narrative* » construite et revendiquée de façon durable, consciente ou latente, par chaque individu[64]. Toutefois, le concept d'identité narrative n'est pertinent que si l'on considère que l'individu possède une totale liberté de décision, ce qui n'est pas nécessairement le cas étant donné les nombreuses pressions et contraintes sociales qui existent lors du processus de construction identitaire d'une personne. Dès lors, l'identité narrative caractérise-t-elle une illusion personnelle à la portée parfois auto-réalisatrice ? Vivons-nous dans l'illusion de notre propre identité ? Sommes-nous réellement l'acteur principal de notre propre fiction identitaire à l'ère numérique ?

Il semble que cette capacité de construction individuelle de notre identité subjective soit en réalité fortement limitée et conditionnée par l'environnement social et notamment éducatif dans lequel chaque individu évolue. L'identité peut être circonscrite à plusieurs niveaux de généralité, comme l'exemple de deux objets similaires (des verres sortis d'une même usine) possédant en apparence la même identité générique et pourtant des propriétés différentes (différence de modèles ou encore de numéros de série). La philosophie préfère une approche subjective de l'identité tandis que le droit privilégie une approche objective. C'est ainsi que le philosophe français Vincent Descombes estime que « *reconnaître le 'droit de la subjectivité', c'est voir dans la volonté d'être soi une attitude morale. L'homme qui fait valoir ce droit - l'homme moderne qui adhère aux valeurs de l'individualisme - veut être responsable de lui-même. Il ne peut être satisfait de lui-même que s'il peut s'attribuer à lui-même, à son propre choix, la*

[63] Plutarque, « Vies des hommes illustres », in *Parallèles, ou vies comparées*, traduction Alexis Pierron, 39p. Disponible en ligne

[64] TETAZ Jean-Marc, « L'identité narrative comme théorie de la subjectivité pratique. Un essai de reconstruction de la conception de Paul Ricœur », in *Études théologiques et religieuses*, 2014, pp. 463-494. Disponible à l'adresse suivante

responsabilité de ce qu'il est »[65]. Ernest Renan[66], l'un des plus grands penseurs et prosateurs du 19ème siècle, dans sa célèbre conférence prononcée à la Sorbonne en 1882, avait fourni au nationalisme allemand, après l'annexion de l'Alsace-Lorraine, une réponse historiquement et philosophiquement fondée sur une identité-nation « *une grande solidarité, constituée par le sentiment des sacrifices qui ont été fait et de ceux qu'on est disposé à faire encore* », combattant ainsi le modèle d'une identité ethnique. Les juristes de la couronne britannique d'Edouard VI différenciaient comme le rappelait l'historien germano-américain Ernst Kantorowicz « *Les deux corps du roi : un corps naturel et un corps politique* »[67]. Cela démontre avec pertinence une distinction conceptuelle entre le corps et l'esprit. Nous soutiendrons ainsi que cette idée de segmentation des identités permet d'appréhender avec pertinence les différentes composantes d'une identité numérique au regard de ses divers contextes d'utilisation. Il est possible de distinguer l'identité revendiquée par l'individu de celle perçue par son entourage. Selon le psychanalyste germano-américain Erik Homburger Erikson, le concept de crise d'identité possède deux volets indissociables et constitutifs de l'identité d'une personne : l'identité objective que reconnaissent des individus à un individu, et l'identité de l'individu face à lui-même, une identité subjective. Dès lors, l'individu ne réussirait pas à être accepté par la communauté à laquelle il est rattaché, s'il ne parvient pas à ajuster ensemble ces deux facettes. Dans nos sociétés modernes, la crise d'adolescence est en réalité une crise de l'identité et plus précisément de l'évolution d'une identité de l'enfant vers celle de l'adulte. Il convient d'évoquer les différences culturelles et sociales qui existent entre une société traditionnelle et moderne, la première soumettant les jeunes individus à des pratiques cérémoniales, des rituels afin de symboliser une évolution depuis le statut d'enfant à celui de jeune adulte (la crise d'identité est donc ritualisée) et la seconde tentant d'individualiser le processus de crise d'identité auquel un jeune individu devra affronter seul (sans rituels) l'évolution de son identité physique, psychologique et sociale. Cette différence d'accompagnement dans la construction identitaire d'un enfant est nette, d'un côté, la crise d'identité est accompagnée et systématisée par le collectif social, et de l'autre, elle est une affaire individuelle et restreinte au cercle familial. De son côté, la philosophe et conférencière française Julia de Funès dans son récent ouvrage sur l'identité[68] se lance dans une critique de toutes les facettes de l'identité et conclut qu'il s'agit d'un concept incertain et que chercher une identité ne peut conduire qu'à une impasse. Elle propose de s'individualiser, de rechercher sa propre singularité pour retrouver le sentiment individuel de soi. A ce stade, certains écosystèmes de l'univers numérique comme les réseaux sociaux représentent un nouveau refuge pour les jeunes générations soumises à des crises identitaires inévitables et nécessaires. Si ce refuge numérique semble plutôt bénéfique en permettant à ces internautes de faire société au sein de communautés spécifiques, il semble que la gestion de ces communautés soit sujette à une dépendance informatique excessive et susceptible

[65] DESCOMBES Vincent, 2013, « Les embarras de l'identité », Ed. Gallimard, emplacement 1801 sur 4825.
[66] RENAN Ernest, « Qu'est-ce qu'une nation ? » nouvelle réédition en 2023, Ed. 1001 nuits, 50p.
[67] KANTOROWICZ Ernst, « Les deux corps du Roi », 1989, Ed. Gallimard, en ligne, in *Rev. Sci. Soc. Polit., 2, Persée*, consulté le 20 août 2021, p.84.
[68] De FUNES Julia, « Le siècle des égarés, de l'errance identitaire au sentiment de soi », Ed. L'Observatoire, 2022.

d'engendrer des manipulations par les fournisseurs de services en ligne. En influençant ces communautés en raison de leurs algorithmes, les réseaux sociaux interviennent directement dans la construction identitaire profonde des jeunes générations, parfois sans protection face à leurs effets négatifs, tels les harcèlements, les rumeurs en ligne ou les violations de données personnelles. Comme l'explique le philosophe français Franck Fischbach[69], le terme d'aliénation ou « *alienatio* » emprunte une première signification juridique en caractérisant pour un individu, un acte juridique de transfert ou de dépossession de la titularité de l'un de ses droits. Au XIXè siècle, ce sens premier évoluera grâce au philosophe allemand Georg Wilhelm Friedrich Hegel pour désigner « (…) *le pouvoir de se séparer de soi-même, de se faire autre que soi et de se reprendre, de se réaffirmer dans son identité à soi* ». Concrètement, Hegel soutient que la conscience personnelle d'une personne ne peut parvenir à rejoindre la conscience collective et sociale du monde, qu'à l'unique condition de se démunir et d'aliéner sa propre conscience, l'aliénation étant « *un mal pour un bien* »[70], c'est-à-dire un passage que chaque individu emprunte de façon temporairement négative, pour que son identité sorte enrichie et adaptée au monde extérieur. Aujourd'hui, la notion d'aliénation possède une forte connotation négative en raison d'une réappropriation au milieu du XIXè siècle par divers penseurs successifs[71]. Cette notion d'aliénation prend tout son sens au regard de l'expansion rapide de nos attributs d'identité étendus au sein d'un univers numérique. Pourtant, nous émettons l'hypothèse que de nouvelles solutions informatiques permettraient de limiter ce phénomène en redonnant à chaque personne une souveraineté et une maîtrise individuelle sur ses données. En définitive, la théorie de « *l'identité sortale* » proposée par le philosophe autrichien et britannique Ludwig Wittgenstein[72], devient une piste privilégiée pour cette étude. Elle considère que chaque critère d'identité dépend de son objet, tout en conservant une part d'unicité. L'identité d'une personne diffère d'une autre dès lors que les deux sont des personnes (la personne étant ici l'objet). Penser l'identité ne doit pas simplement revenir à penser de façon systématiquement déterministe, c'est-à-dire à fixer des appartenances identitaires pour chaque personne au risque de les enfermer dans ces appartenances. Il s'agit également d'accepter l'identité comme l'expression et le partage de récits personnels différents et sociaux. Jumelé au concept de « *la vie privée en contexte* »[73] décrit par la Professeure en sciences de l'information Helen Nissenbaum, selon lequel à chaque flux d'informations doit correspondre un contexte d'utilisation en accord avec les besoins des utilisateurs, une vision de l'identité en contexte semble faire sens. Par extension, cette forme d'identité contextuelle fait appel à un cloisonnement des différentes parties de l'identité d'une personne, ce qui est privilégié dans cette thèse afin de former un champ de recherche cohérent.

[69] FISCHBACH Franck, « L'aliénation : un concept encore utile aujourd'hui ? » Séminaire Université de Lorraine, 4 oct. 2021.
[70] GAYON Jean et al., « L'Identité : dictionnaire encyclopédique », 2020, in *Folio Essai*, Gallimard. ISBN : 978207283413.
[71] Il est fait référence aux travaux préalables de Karl Marx et Bruno Bauer évoqués par Alex Mucchielli in *L'identité*, p.179
[72] MUCCHIELLI Alex, *op. cit*., p.673.
[73] NISSENBAUM Helen, *Stanford University Press, 2009*, citée par Claire Levallois-Barth in « L'identité numérique : quelles définitions pour quelles protections », (sous la dir. de) Jessica Eynard, Ed. Larcier, 2020, Dalloz Librairie, p.189.

1.1.2 Les contours de l'identité au regard de la sociologie

Certains auteurs comme le philosophe français Vincent Descombes, déjà cité, permettent de comprendre la relation indissociable qui existe entre l'identité et la société *« Peut-on dissocier la constitution de la cité inscrite dans les textes* [l'identité juridique et politique d'une nation] *de celle qui est inscrite dans les cœurs* [l'identité sociale et culturelle des citoyens] *?* »[74]. Admettre que les identités sont le fait de processus sociaux et historiques précis, mais imprévisibles, permet de comprendre l'ampleur paradoxale de cette notion à l'échelle individuelle et collective. L'écrivain, dramaturge, philosophe et homme d'État Johann Wolfgang von Goethe écrivait « *c'est en vain que nous entreprenons d'exprimer la nature d'une chose. Nous nous efforçons en vain de peindre le caractère d'un être humain ; rassemblons par contre ses manières d'agir, ses actes, et nous verrons apparaître une image du caractère* [de son identité] »[75]. D'un point de vue historique et social, l'identité d'une personne se matérialise par son nom et son prénom qui représentent deux variables stables par lesquelles une identité singulière et minimale peut s'exprimer[76]. Le sociologue américain Erving Goffman désignait le nom et le prénom comme des *porte-identités*[77]. Si toutes les sociétés et cultures recourent à l'usage unanime de cette même méthode historique d'affirmation de l'identité, il convient d'observer que ce processus de désignation varie selon chaque culture. En effet, s'il est aisé de se souvenir des noms et des prénoms de chacun au sein de sociétés de tailles restreintes, cela s'avère plus complexe dans nos sociétés contemporaines, référence faite à la loi permettant aujourd'hui le double nom de famille[78].

Depuis quelques siècles, ce processus de désignation nominatif est juridiquement encadré par un état civil stable. Ainsi, ce processus désormais écrit est institutionnalisé en vertu des principes de stabilité sociale et de protection juridique. Cela peut aussi s'expliquer par une importante croissance démographique des populations depuis le XIXè siècle. Cette croissance a engendré un besoin d'identification fort pour les États, dont une identification administrative fiable des identités est un élément clé pour le bien commun de la société. En effet, elle permet par exemple d'assurer une justice pour tous ses administrés. En ce sens, la permanence d'un système d'identification fiable comme le papier permettait aux autorités administratives d'identifier, d'enregistrer et de suivre avec une relative précision ses administrés. En France, s'instaure progressivement au XIXè siècle le nom de famille. Un siècle plus tard s'y ajoutera le prénom, dont l'usage dépasse la simple transmission familiale - comme pour le nom - pour se diffuser au quotidien dans le domaine scolaire, professionnel ou personnel. Comme l'expliquait le sociologue américain Anselm Leonard Strauss, le nom et le prénom nous caractérisent aujourd'hui dans nos relations sociales et administratives en formant « *un lien indissoluble entre le nom*

[74] DESCOMBES Vincent, *op. cit*., emplacement 3858 sur 4825.
[75] VON GOETHE Johann Wolfgang, « Traité des couleurs », Ed. Triades, 1973, p.71.
[76] ALFORD Richard, « Naming and Identity » in HRAF.
[77] GOFFMAN Erving**, «** Stigmate: les usages sociaux des handicaps **»**, 1975 consulté en ligne le 21 août 2021, p.75.
[78] Loi n°2002-304 du 4 mars 2002 relative à l'attribution d'un double nom de famille à la naissance.

et l'image de soi »[79]. Toutefois, ce processus nominatif n'est pas un système d'identification parfaitement fiable en raison de la possible et régulière existence d'homonymes. Dès lors, nous supposons dans cette recherche qu'aucun système d'identification ne sera jamais parfait, bien que les mécanismes d'identification actuels soient particulièrement efficaces.

La sociologie admet que des mécanismes relationnels sont au cœur du système de construction des identités au sein des communautés, des groupes et plus généralement des sociétés. Ces logiques relationnelles relèvent d'une triple caractérisation[80], les groupes extérieurs à nous (« *ils* »), les groupes internes auxquels on se rattache (« *nous* ») et enfin la relation entretenue entre ces deux premiers groupes (relation entre « *ils* » et « *nous* »). Cette représentation permet d'envisager la manière dont les personnes s'identifient collectivement par leur différenciation collective. C'est ainsi que naissent les identités nationales, professionnelles et personnelles. Selon la société étudiée, il existe d'innombrables groupes d'appartenance dont les identités revendiquées sont souvent complexes à appréhender, car vécus et ressentis à la fois subjectivement et collectivement. Historiquement, l'identité au sens identitaire est une notion développée en 1970 avec l'historien américain Philip Gleason[81]. Il constate à l'époque une utilisation massive du terme d'identité par de nombreux experts en sciences sociales, sans pour autant que ces derniers n'arrivent à le définir avec précision « *l'identité est une chose, c'est ce qu'elle est* ». Gleason démontre que le concept d'identité est initialement apparu dans les sciences sociales américaines en 1955 pour permettre aux individus (Américains) de se situer au sein d'une société d'autres groupes sociaux auxquels ils se rattachent formant ainsi une identité nationale, notamment par leurs caractères distinctifs, identité religieuse, origines ethniques. Cette idée se rapproche du concept d'identité narrative de Paul Ricoeur évoqué précédemment, c'est-à-dire une identité construite par l'individu qui déciderait de choisir quelle (ré)interprétation donner à son passé. Elle apparaît comme « *un phénomène pathologique, source de 'confusion' et de désorientation* »[82] avec lequel chaque personne doit procéder à une intériorisation consciente de qui elle est, et gérer cette représentation consciente et inconsciente lors de ses interactions sociales, désormais numériques. Finalement, comme l'a démontré Philip Gleason, le terme d'identité est source d'embarras, car utilisé dans les sciences sociales américaines sans même posséder une définition précise. Dès lors, son usage et son sens ont pris certaines définitions parfois opposées, qui se retrouvent aujourd'hui dans notre langage commun. Si l'identité semble être un élément fondamentalement personnel et intime, les sciences sociales semblent nuancer cette première impression afin de mettre en exergue la dépendance sociale et extérieure d'une identité personnelle au monde. La célèbre maxime « *l'Homme est un animal par nature politique* »[83] du

[79] STRAUSS *A*nselm, « Miroirs et masques, une introduction à l'interactionnisme », 1993, Revue des sciences sociales du politique, consulté en ligne le 21 août 2021, pp.142-146.
[80] MUCCHIELLI Alex, *op. cit*.
[81] GLEASON Philip, « Identifying Identity: a semantic history », in Journal of American History, vol. 69, no 4, mars 1983, pp. 910-931.
[82] DESCOMBES Vincent, *op. cit*. Emplacement 463 sur 4825.
[83] JAULIN Annick, « La nature de l'animal politique humain selon Aristote », Éd. Sorbonne, 2017, disponible en ligne

philosophe grec Aristote, énoncerait ainsi une loi naturelle selon laquelle l'Homme est destiné à vivre en société. Six siècles plus tard, le sociologue allemand Norbert Elias ajoutera « *on ne peut opposer individu et société comme deux entités que sur le plan du langage* »[84]. Ce constat est aussi partagé par le sociologue Émile Durkheim pour qui « *l'homme n'est un homme que parce qu'il vit en société* »[85]. La culture est ainsi au centre de la création et du maintien de toute vie sociale, et par extension de toute identité collective ou individuelle. Finalement, trouver son identité et ses appartenances, c'est faire communauté. Le célèbre anthropologue français Claude Lévi-Strauss témoigne dans son ouvrage « la pensée sauvage (1964) » de la manière dont la singularité individuelle des personnes n'intervient pas en contradiction avec leur intégration au sein de groupes sociaux. Depuis son point de vue anthropologique, il explique en quoi ce processus d'intégration d'individus externes à une société (des étrangers ou encore une nouvelle génération) engendre une perturbation de l'ordre institué. La communauté doit systématiquement fournir ou laisser une place à l'individualité de chaque nouvelle personne entrante au sein de son groupe. Ce constat est soutenu par l'auteur et académicien français Amin Maalouf qui estime qu'il est primordial d'introduire et de favoriser un concept proche de celui d'identité solidaire, c'est-à-dire d'encourager la capacité de l'Homme à se mettre à la place de leurs compères en cultivant de multiples appartenances réciproques.

L'identité sociale d'une personne regroupe ainsi l'ensemble de ses appartenances qui forment ensemble sa personnalité, mais dont les combinaisons et priorités varient en permanence « *si chacun de ces éléments* [d'appartenances] *peut se rencontrer chez un grand nombre d'individus, jamais on ne retrouve la même combinaison* [d'appartenances] *chez deux personnes différentes, et c'est justement cela qui fait la richesse de chacun, sa valeur propre, c'est ce qui fait que tout être est singulier et potentiellement irremplaçable* »[86]. Selon le philosophe indien Amartya Sen, tout individu possède plusieurs identités « *Puisque chacun possède plusieurs identités, il lui faut à chaque fois choisir, parmi les différents groupes qui peuvent réclamer son allégeance, celui qui va prévaloir à telle occasion* »[87]. De ce fait, l'identité est avant tout un phénomène social permettant de revendiquer des identités sociales selon deux appartenances, l'une de classe, correspondant à un critère commun et partagé par des individus et l'autre communautaire et sociale. Combinées, ces deux appartenances forment l'identité sociale. Séparées, elles ne permettent pas systématiquement de créer un sentiment identitaire suffisant pour que des individus puissent former un groupe social, source de revendications identitaires compréhensibles et acceptées de tous. Nous constatons dans les parties dédiées à l'identité numérique auto-souveraine et au Métavers étudiés plus loin, que ces deux types d'appartenance font probablement défaut à leur adoption massive, contrairement à la blockchain Bitcoin qui représente une nouvelle forme de quasi-nation

[84] DUMA Jean, "Histoires de nobles et de bourgeois : Individus, groupes, réseaux en France. XVè-XVIè siècles", Presses universitaires de Paris Nanterre, p.187.
[85] DURKHEIM Emile, « Éducation et sociologie », PUF, Coll. Quadrige, nouvelle édition 2022, p.55, en ligne à l'adresse suivante
[86] MAALOUF Amin, *op. cit*. p.17.
[87] DESCOMBES Vincent, 2013, « Les embarras de l'identité », Ed. Gallimard, emplacement 179 sur 4825.

technocratique[88]. Karl Marx exprimait « *ce n'est pas la conscience des hommes qui détermine leur être ; c'est inversement leur être social qui détermine leur conscience* »[89]. Selon de grands auteurs des sciences sociales comme le Professeur en sciences politiques autrichien Joseph Schumpeter ou le sociologue français Pierre Bourdieu, il existe trois typologies d'identité de classe[90], celle temporelle (la capacité d'une classe sociale à ne pas se confondre à d'autres au fil du temps), celle culturelle (toutes les formes de revendications culturelles, politiques, sociales, économiques ou encore physiques propres à une classe sociale) et celle collective répondant à l'intérêt supérieur du collectif et à sa capacité de représentation et d'action. Comme évoqué précédemment, l'identité collective primait sur l'individualité de chaque personne, toute action pensée à travers le prisme commun du « *nous* ». À l'inverse, nos sociétés contemporaines ont tendance à ériger une identité personnelle, individualiste et autonome en tant qu'objectif et figure de réussite sociale. Le sociologue français Emile Durkheim désignait ce phénomène social et culturel comme un culte de l'individu par lequel la société cède certaines de ses valeurs collectives au profit de valeurs personnelles. Nous constaterons que de nombreuses applications informatiques liées aux technologies 3.0 donnent sciemment ou non et de façon exacerbée une nouvelle forme de culte individuel, communautaire et financier, avec le Métavers et les NFT par exemple qui sont étudiés plus loin.

Toutefois, les sociétés traditionnelles et contemporaines restent des organisations sociales structurées. Le philosophe canadien Charles Taylor considère qu'à partir du XVIIIe siècle, nos sociétés modernes et occidentales sont entrées dans un processus de « *désocialisation* » par lequel la « *vie sociale* » et les « *affaires sociales* » se sont progressivement rationalisées pour laisser place à la pression individuelle et à l'influence sociale[91]. Ainsi, dans nos sociétés modernes, les individus sont à l'aise avec une libre auto-détermination ainsi qu'avec une désocialisation inconsciente de leur identité, en opposition aux sociétés traditionnelles. De façon complémentaire, l'anthropologue français Louis Dumont expliquait que l'individu moderne se « *pense en individu* », c'est-à-dire qu'il possède un pouvoir de décision concernant les conditions de satisfaction de soi et de son estime. Il s'agit en quelque sorte d'un droit de l'individu à l'émancipation identitaire, c'est-à-dire à la capacité de se définir selon ses propres conventions et souhaits. Si cette possibilité n'a jamais été aussi vraie à l'ère numérique notamment du Web 3.0 l'influence quotidienne de certains réseaux numériques sur notre identité n'a jamais été aussi importante et paradoxale. Depuis quelques années, un nouveau constat identitaire s'impose par une volonté de dégenrer l'identité des personnes, c'est-à-dire de supprimer les catégories masculine et féminine de certains contextes physiques et numériques. Ainsi, deux questions subsidiaires semblent importantes sur le sujet : pourquoi les identités de genre existent ? Sont-elles toujours pertinentes aujourd'hui ? En France et en Europe, l'identité de genre est le fruit de notre histoire et de notre culture

[88] V. Annexe 3, Focus 1 à 6.
[89] EGE, Ragip, « À propos de l'ouvrage de Karl Marx : Contribution à la critique de l'économie politique. Introduction aux Grundrisse dite 'de 1857' », 2016, in *Cahiers d'économie Politique*, disponible à l'adresse suivante
[90] GAYON Jean et al., *L'Identité : dictionnaire encyclopédique*, 2020, Folio Essai, Gallimard. ISBN : 9782072834134.
[91] DESCOMBES Vincent, *op. cit.*, emplacement 2088 sur 4825.

sociale et religieuse. Utilisés depuis le XIIè siècle[92], ces termes sont aujourd'hui toujours largement utilisés, y compris sur les titres d'identité officiels. Il s'agit de supprimer l'utilisation des genres pour l'identité civile et légale des personnes - dans la continuité de la récente suppression de l'utilisation du terme « Mademoiselle »[93] par les institutions publiques - du fait que cette distinction de genre n'est plus ni nécessaire ni justifiée, mais simplement le fruit de notre histoire et culture. Supprimer les genres permettrait d'apporter une réponse simple à un double constat social et informatique, en raison d'un nombre croissant de citoyens revendiquant la possibilité de changer de genre au cours de leur vie, car ne se reconnaissant dans aucune des deux catégories traditionnelles (« homme » ou « femme »). Sa suppression permettrait d'instaurer un principe conceptuel de minimisation de l'identité des personnes, en contribuant à réduire la quantité importante d'attributs et de données personnelles pouvant être récoltées (par exemple seuls les attributs indispensables comme biométriques pourraient être récoltés). De cette façon, la fonction d'une personne ne primerait plus sur la personne qui serait alors plus librement revendiquée. En conclusion, il semble que le concept d'identité représente avant tout un moyen efficace, mais complexe, d'évoquer la diversité des Hommes et de leurs singularités. Si un individu souhaite être perçu à sa juste valeur, il s'agit de lui permettre d'exprimer ce qu'il pense posséder de plus estimable dans sa singularité. Nous étudions comment l'identité numérique décentralisée permettrait de renouer avec l'utopie d'une identité individuellement et collectivement souveraine et *agentive*[94]. Cependant, conférer une trop grande autonomie et responsabilité aux internautes pourrait également amener à des dérives non maîtrisées. Nous tenterons d'identifier un équilibre entre l'importance de cette théorie et les outils informatiques appropriés et innovants actuellement à disposition.

1.1.3 Les contours de l'identité au regard du droit

L'identité est définie à l'échelle internationale de manière complémentaire par plusieurs organisations transnationales. En 2015, un groupe d'experts rattachés aux Nations Unies et travaillant sur la mise en place d'objectifs de développement durable à l'échelle internationale a publié une liste d'indicateurs dont l'un d'entre eux souligne que « *fournir une identité légale à tous (y compris l'enregistrement des naissances) d'ici 2030 est un objectif partagé par la communauté internationale dans le cadre des*

[92] DEVELEY Alice, 21 août 2018, « 'M.', 'Mr' : ces abréviations de titres de civilité à ne plus écorcher », in *Le Figaro*, à l'adresse suivante

[93] Circulaire n° 5575/SG du 21 février 2012 relative à la suppression des termes 'Mademoiselle', 'nom de jeune fille', 'nom patronymique', 'nom d'épouse' et 'nom d'époux' des formulaires et correspondances des administrations, disponible à l'adresse suivante

[94] GAYON Jean et al., « L'Identité : dictionnaire encyclopédique », *op. cit.* p.169. L'agentivité est la capacité d'un acteur à agir dans un environnement donné. En sociologie, un agent est un individu qui s'engage dans la structure sociale. Le sentiment d'agentivité caractérise une sensation de contrôle sur ses propres actions et par extension sur les événements de son environnement social.

objectifs de développement durable (cible 16.9) »[95]. En 2018, l'union internationale des télécommunications (UIT) désigne l'identité comme « *la représentation d'une entité sous la forme d'un ou plusieurs attributs qui permettent de distinguer suffisamment l'entité ou les entités dans un contexte* »[96]. En 2019, l'organisation internationale de normalisation (ISO) la définissait comme « *un ensemble d'attributs liés à une entité* »[97] en complétant « *l'identification est un processus de reconnaissance d'une entité dans un domaine particulier comme étant distincte des autres entités* »[98]. De façon paradoxale, la Déclaration des Droits de l'Homme et du Citoyen (DDHC) ne mentionne ni ne définit l'identité. Néanmoins, elle reconnaît indirectement un droit à l'identification dans son article 6 « (…) *tous les citoyens étant égaux à ses yeux sont également admissibles à toutes dignités, places et emplois publics, selon leur capacité, et sans autre distinction que celle de leurs vertus et de leurs talents* »[99]. Dès lors, le droit d'avoir une identité et d'être identifiable semble indirectement reconnu sans pour autant que soit définit de façon précise la notion d'identité. Ces premières définitions proposent un socle juridique commun permettant d'aborder la notion d'identité sous un angle encore une fois général et abstrait. Parce que l'identification des personnes est un processus essentiel pour leur accorder un accès à des services de tous ordres, il convient d'en définir plus précisément les éléments matériels. Le droit a pour rôle de fixer les conditions de fabrication de l'identité physique et numérique dont l'une des composantes majeures repose sur des attributs personnels dématérialisés sous la forme de données circulant en ligne. L'accès à certains services ou interactions sociales requiert une méthode d'identification préalable des personnes ou des utilisateurs. Ces systèmes d'identifications sont en principe fournis par l'État aux citoyens et encadrés par le droit. Il s'agit de bâtir un système d'identification à grande échelle, ce qui nécessite une importante confiance des citoyens, des institutions et des entreprises. Sans une transparence et une confiance juridique totale, un climat de méfiance peut s'instaurer ou subsister vis-à-vis de toute solution technique d'identification, étant donné que l'identité est un domaine sensible qui implique directement la sphère personnelle et psychosociale de chaque individu.

De manière universelle, la plupart des États à travers le monde se positionnent en tant que premier fournisseur d'identité pour les personnes, notamment par un titre d'identité physique papier ou plastique et un certificat de naissance[100]. Ce dernier repose sur un registre physique et/ou électronique qui est tenu

[95] World Bank Group, *identification for development*, consulté en ligne le 25 août 2021, traduction libre de l'anglais, « Providing legal identity for all (including birth registration) by 2030 is a target shared by the international community as part of the Sustainable Development Goals (target 16.9) ».
[96] International Telecommunication Union (ITU), « Telecommunication Standardization Sector, X.1252, Baseline identity management terms and definitions », Avril 2010, traduction libre de l'anglais « identity is the representation of an entity detailed enough to make the individual distinguishable within a context », p.4, 2018, in *Digital Identity Roadmap Guide.*
[97] Traduction libre de l'anglais « Identity is a set of attributes related to an entity », ISO/IEC 24760-1.3.2.1
[98] Traduction libre de l'anglais « identification is the process of recognizing an entity in a particular domain as distinct from other entities ».
[99] Déclaration des Droits de l'Homme et du Citoyen (DDHC) de 1789 | Conseil constitutionnel, consulté en ligne le 25 août 2021.
[100] BENSOUSSAN Alain, « Aujourd'hui l'information [d'une naissance] est communiquée électroniquement à l'administration publique par le médecin de la maternité dès l'accouchement. Un numéro national d'identité est assigné », in *L'identité numérique 5.0.*, Bensoussan Avocats, Ed. Lexing, p.16.

à jour par l'État et son administration au fil du temps. La personne légalement responsable de l'enfant peut recevoir une attestation ou un certificat qui représente donc les informations dans ce registre officiel dont l'État est le garant. Ces informations, stockées dans le cadre du processus d'enregistrement des naissances, comprennent principalement le nom, la date et le lieu de naissance, la nationalité, le ou les parents et parfois d'autres caractéristiques complémentaires (couleur des yeux, sexe, taille). Toutefois, si aux yeux de la doctrine l'identité représente « *l'ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (nom, prénom, date de naissance, filiation)* »[101], certains juristes constatent qu'il existe d'ores et déjà une hiérarchie d'importance entre certains éléments matériels de l'identité. En effet, le nom, le prénom et la date de naissance semblent prioritaires et « *pivots* »[102] par rapport à d'autres critères comme le lieu de naissance. Parce que l'état civil des personnes matérialise et confère une existence identitaire et légale aux personnes[103], ce « *noyau identitaire minimum* »[104] leur octroie une personnalité juridique et un statut juridique en leur donnant accès à des droits de vote et en les soumettant à des obligations (imposition fiscale, etc.). De ce fait, l'état civil d'une personne donne naissance à une identité que nous désignons tout au long de cette thèse comme primaire, racine et légale. Pour les personnes morales de droit français, l'identité juridique d'une organisation naît lorsque le greffe d'un tribunal de commerce enregistre certaines informations minimales (Kbis, représentants légaux, forme juridique, statuts, siège social) permettant l'identification d'une organisation au registre du commerce et des sociétés (RCS) près des 227 tribunaux de commerce français. Ainsi, l'identité des personnes physiques et morales repose sur des traitements humains, administratifs et informatiques. Si le champ d'études de cette recherche s'intéresse principalement à l'identité des personnes physiques, l'identité des personnes morales est également évoquée à travers le prisme de l'identité numérique décentralisée ainsi que dans une partie dédiée aux objets numériques.

Les titres et documents d'identité officiels représentent des supports matériels en réalité étendus et extraits du registre d'état civil qui demeure l'unique source de vérité de l'identité juridique des personnes[105]. Ces titres permettent aux citoyens de prouver leur nationalité et droits afférents. Ils contribuent à faciliter une preuve manuscrite de leur identité légale. Chaque document possède une finalité propre : un passeport sert à « *passer les ports* », c'est-à-dire à voyager, la carte nationale d'identité (CNI) permet une libre circulation sur le territoire national et une carte d'électeur permet aux citoyens de s'exprimer par le vote démocratique. L'histoire du développement de ces supports d'identité mérite un rappel afin de bien comprendre les enjeux actuels et futurs de leur dématérialisation. L'histoire

[101] EYNARD Jessica, « L'identité numérique ; quelle définition pour quelle protection ? », Coll. Larcier, 2020, Dalloz Librairie.
[102] Ce terme est introduit dans la Délibération n°2015-254 du 16 juillet 2015 portant avis sur un projet d'arrêté portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication du téléservice dénommé FranceConnect
[103] La date de naissance permet de définir l'âge d'une personne et donc sa capacité juridique. Le domicile permet de lier une personne à un territoire et à sa juridiction associée.
[104] BERNARD Alain, « L'identité des personnes physiques en droit privé », consulté en ligne le 26/08/21, p.155.
[105] Il est fait référence à l'acte de naissance qui représente une pierre angulaire pour la reconnaissance juridique d'une personne physique.

des titres d'identité prend ses racines après l'essor des déplacements migratoires qui rendait inefficaces les méthodes d'identification traditionnelles par l'usage du nom et du prénom comme évoqués ci-avant. En effet, ces derniers étaient jugés peu fiables, car dépendants de l'interconnaissance et de la mémoire des personnes. C'est le XVIe siècle qui voit naître une première volonté d'améliorer le système d'identification grâce à l'ordonnance Guillemine décrétée en 1539 par François 1er[106]. Cette dernière introduit et impose une normalisation de la langue française pour tous les actes administratifs et juridiques de l'époque, notamment en abolissant l'utilisation du latin pour ces actes. En conséquence et sous couvert d'un renforcement du pouvoir monarchique, elle impose aux paroisses de France l'inscription de tous mariages, naissances et décès au sein de registres paroissiaux. L'état civil apparaît sous sa première forme puis sera institué sous sa forme moderne après la Révolution française[107]. Puis la IIIe République marque un tournant dans l'histoire de l'identification de l'État envers ses citoyens. Au-delà du recours systématique à l'état civil[108] pour délivrer des titres d'identité aux Français, les personnes immigrées se voient obligées par la loi du 8 août 1893 relative au séjour des étrangers en France et à la protection du travail en France[109] de s'enregistrer afin d'accéder et de prouver leur droit au séjour. Cette première loi, précurseur en termes d'obligation d'identification, sera plus tard en 1917 complétée par une carte nationale d'identité imposée à tous les travailleurs coloniaux. Après 1918, le concept de carte nationale d'identité est étendu à toute la population française, afin de garantir une identification fiable ainsi qu'une citoyenneté officielle aux Français. Dès lors, l'identité d'une personne et son état civil sont deux concepts indissociables. Pourtant, leurs liens sont régulièrement questionnés afin de désigner d'autres réalités pour exprimer le besoin de revendiquer de nouvelles appartenances matérialisées par de nouveaux attributs étendus de l'identité des personnes. Si le droit organise sa propre vérité concernant l'identité *civile et primaire* des personnes, peut-il en être autrement pour l'identité *subjective et secondaire* des personnes ?

Le professeur de droit Alain Bernard distingue *l'identité permanente* (fixée par le droit) de *l'identité revendiquée* (le rôle fixé par la société), la première étant nécessaire à la seconde et la seconde indissociable de la première. Ce dernier perçoit ainsi la société comme « *un gigantesque filet* »[110] grâce auquel chaque personne est reliée aux autres, de façon plus ou moins directe et complexe. L'indétermination et l'indisponibilité juridique de l'identité en droit français s'expliquent par la diversité des fonctions qu'elles jouent dans la vie juridique des personnes. Cette indétermination est due à l'évolution constante de la notion d'identité, que les professionnels du droit préfèrent limiter à certains éléments matériels et immuables. Avec une ambition similaire, l'indisponibilité de l'identité des

[106] Cette Ordonnance est le plus ancien texte législatif encore en vigueur en France ; Ordonnance du Roy sur le fait de justice, consultée en ligne le 21/08/2021.
[107] BENSOUSSAN Alain, avocat, « C'est la révolution française qui retire la tenue des registres des mains de l'église catholique pour la confier à l'État, et ainsi créer l'identité dite régalienne », in *L'identité numérique 5.0*. Ed. Lexing, p.16.
[108] Sous la forme de fichiers centraux détenus par les pouvoirs républicains.
[109] Loi du 8 août 1893 relative au séjour des étrangers en France et à la protection du travail national, consulté en ligne le 21 août 2021.
[110] BERNARD Alain, *op. cit.* p.133

personnes est complémentaire à son indétermination juridique : elle rend en principe complexe et indisponible la modification d'un ou plusieurs éléments matériels de l'identité d'une personne (nom, prénom)[111]. Par exemple, la lecture des données biométriques des citoyens français sur les puces de leurs passeports et cartes nationales d'identité électronique étudiées plus loin, n'est légalement autorisée[112] que par des agents assermentés de l'Etat et non par les titulaires physiques de la biométrie, ce qui démontre l'indisponibilité de nos identités notamment au regard de leur accessibilité[113]. Cependant, il semble que « (…) *petit à petit, le droit a laissé place à une volonté, toutefois contrôlée, de s'immiscer dans les éléments principaux de l'état que sont le nom, le prénom et le sexe* »[114]. Bien que l'association d'un nom et d'un prénom puisse toujours être frappée par l'homonymie[115], constatons que cette association permet toujours de rendre un individu relativement unique et facilement identifiable, notamment grâce à la biométrie dans les cas prévus par la loi. Les identités numériques (pseudos et avatars de réseaux sociaux) remettent parfois en question cette unicité de l'identité d'une personne, bien que seuls ses attributs et données d'identité civile lui permettent de procéder à des actes juridiques de la vie courante. Dans une majorité de situations, il semble que l'état civil et l'identité personnelle soient frappés par les principes d'indissociabilité, d'immuabilité et d'indisponibilité réciproques. Toutefois, l'identité personnelle - grâce aux progrès de l'identité numérique - semble en voie d'émancipation de l'état civil qui l'a vu naître : une nouvelle forme d'identité numérique choisie apparaît, dont les contours sont parfois aussi déterminants qu'une identité civile selon les écosystèmes numériques où elle se manifeste dans les Métavers et les réseaux sociaux notamment. L'état civil est également confronté à des contraintes et des limites, notamment en ce qui concerne la fiabilité et l'authenticité des informations matérielles dérivées de celui-ci, telles que les cartes d'identité et les passeports, ainsi que la fraude documentaire liée aux actes d'état civil qui ne sont pas suffisamment sécurisés, dépourvus de composants de sécurité biométrique ou d'hologrammes. De plus, il est complexe de mettre à jour des documents d'identité qui peuvent présenter une confusion entre l'état civil des personnes et leurs documents d'identité, qui ne sont en réalité que des supports dérivés résumant à un moment donné certaines informations minimales de leur état civil.

---

[111] En droit français, la modification de son nom de famille est possible directement auprès du ministre de la Justice, de manière entièrement dématérialisée, et uniquement en cas de motif légitime (articles 61 à 61-4 du Code civil). En Grande-Bretagne, ce processus est plus simple administrativement (un court formulaire est à remplir), rapide (1 à 4 semaines) et moins coûteux (~42£). Ce processus est public et permet l'utilisation légale d'un nouveau nom, un choix effectué par plus de 85 000 personnes chaque année en Grande-Bretagne.

[112] « Seuls les fonctionnaires de la police nationale chargés du contrôle aux frontières, individuellement désignés et spécialement habilités, et ayant la qualité d'officier ou d'agent de police judiciaire, ont accès aux informations résultant de l'interconnexion entre PARAFES et le fichier des personnes recherchées et le système d'information Schengen [base de données biométriques]. », Fiche Question. Disponible à l'adresse suivante

[113] SENAT, Proposition de loi relative à la protection de l'identité, 1er juin 2022, « […] limiter aux seuls agents habilités à cet effet, la possibilité de lire les empreintes digitales inscrites sur le titre d'identité pour s'assurer qu'elles correspondent à celles du porteur du titre », disponible à l'adresse suivante

[114] SIFFREIN-BLANC Caroline, « L'identité des personnes : une identité pour soi ou pour autrui », consulté en ligne le 26 août 2021, 2016, in *Presses de l'Université Toulouse 1 Capitole*, p.3.

[115] L'homonymie peut toutefois être écartée grâce à d'autres attributs d'identité racine inscrits dans l'état civil (domicile, date et lieu de naissance, etc.).

Sans rentrer dans une classification trop complexe des types de données personnelles pouvant exister, il est admis par les juristes que l'agrégation de quelques données personnelles suffit amplement à caractériser et retrouver l'identité racine ou étendue d'une personne. Par exemple, les données personnelles étaient caractérisées en 2007 par le groupe de travail « article 29 »[116] sur la protection des données « *il convient de relever que si l'identification par le nom constitue, dans la pratique, le moyen le plus répandu, un nom n'est pas toujours nécessaire pour identifier une personne, notamment lorsque d'autres 'identifiants'* [numériques] *sont utilisés pour distinguer quelqu'un.* (...) *On reconstitue ainsi la personnalité de l'individu pour lui attribuer certaines décisions. Sans même s'enquérir du nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes, la possibilité d'identifier* [en ligne] *une personne n'implique plus nécessairement la faculté de connaître son identité.* »[117]. Avec la multiplication des dispositifs technologiques couplée à l'évolution des pratiques et des interactions sociales toujours plus numérisées, les individus n'ont jamais émis autant de données[118]. À l'échelle communautaire, l'article 8 de la Convention Européenne des Droits de l'Homme (CEDH), entrée en vigueur le 3 septembre 1953, a posé le fondement du droit au respect de la vie privée et par extension celui de l'identité des personnes « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* »[119]. Dès lors qu'une personne possède ce droit à la naissance, les fondements de l'identité personnelle, domicile, famille et interactions sociales sont respectés. Progressivement, la CEDH adapte et élargit la définition et la protection de l'identité face à ces tâtonnements sociaux, politiques et technologiques successifs. Elle « s'*affranchit de toute limite dans tous les choix existentiels - sexe, corps, vie et mort - de l'individu* »[120], car « *la notion de vie privée comprend des éléments se rapportant à l'identité d'une personne telle que le nom* ». Il semble que les évolutions technologiques et préalablement sociales se confrontent de façon croissante à la jurisprudence européenne en faveur de la reconnaissance d'une identité humaine universelle. En effet, une jurisprudence européenne pose les fondements d'un droit à l'autonomie personnelle « *bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8* »[121]. Comme l'explique Claire Levallois-Barth, Maître de Conférence et enseignante-

[116] Le 25 mai 2018, le Conseil européen de la protection des données (EDPB) a remplacé le Groupe de travail 'Article 29', in « L'identité numérique ; quelle définition pour quelle protection ? », Jessica Eynard, Coll. Larcier – Ed. Dalloz Librairie Paris.
[117] *Op. cit.,* Avis 4/2007 sur le concept de données à caractère personnel, consulté en ligne le 30 août 2021.
[118] « Total data volume worldwide 2010-2025 » publié en juin 2021 in *Statista* en ligne, consulté le 30 août 2021, traduit de l'anglais « 181 zettabytes de volume de données créées, capturées, copiées et consommées dans le monde entier de 2010 à 2025 » ; International Data Corporation estime que la sphère de données mondiale passera de 33 zetta en 2018 à 175 zettaoctets en 2025.
[119] Notons que cette convention permet à tout citoyen européen de pouvoir invoquer ce texte pour se défendre, à la différence de la DUDH dont la portée est plus symbolique et morale.
[120] EYNARD Jessica, « L'identité numérique ; quelle définition pour quelle protection ? » *op. cit.*, p.31.
[121] CEDH, 29 avril 2002, Pretty c. Royaume-Uni, 2346/02, in *Revue générale du droit*, consulté en ligne le 30 août 2021.

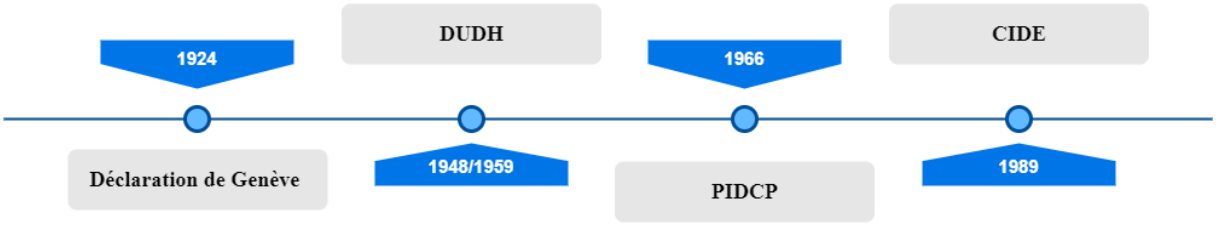
chercheuse à Télécom Paris « *l'enjeu porte donc sur le respect du libre arbitre de chacun et donc de notre liberté de choix. La possibilité même pour la personne de se présenter comme elle l'entend, de vivre sa vie en définissant ces identités alternatives, participe au respect de ses libertés fondamentales, notamment la liberté d'expression et de communication, de l'appartenance à une communauté ou d'une activité politique* »[122]. Ainsi, au sens du droit communautaire, l'identité semble être protégée et encouragée dans son développement au-delà des définitions nationales de l'identité civile habituellement admises par les États membres. Pour illustration, la CEDH déclare « *le droit pour chacun d'établir les détails de son identité d'être humain* » au point de constater l'ubiquité de cette notion dans la jurisprudence européenne. La CEDH admet ainsi un respect et une sécurité juridique, non seulement de la notion d'identité au sens des moyens concourant à son identification (identité légale), mais aussi de différentes composantes de l'identité sociale « *la Cour bâtit ainsi une véritable politique de l'identité, fondée sur la tolérance et l'acceptation des différences* ». En résumé, la CEDH semble s'orienter vers l'établissement conceptuel d'une identité universelle accessible à tous et qui garantirait une égalité de traitement et de reconnaissance, une absence de discrimination, ainsi qu'une autonomie aux citoyens européens.

1.1.3.1 Le droit à l'identité : raison d'être et textes internationaux fondateurs

Le droit à l'identité fait directement référence au droit de chaque enfant à se voir attribuer une identité civile dès sa naissance. Cette attribution permet à l'individu de bénéficier d'une personnalité juridique qui est indispensable pour bénéficier d'une protection juridique efficace et pérenne. L'identité constitue effectivement une condition préalable à tous les autres droits et demeure un enjeu majeur pour tout État de droit[123]. L'acte de naissance d'une personne peut être perçu comme un visa pour un droit à la vie : il matérialise l'existence juridique de l'individu et lui permet de la prouver. L'acte de naissance représente ainsi l'acte fondateur de l'état civil, et ses actes subsidiaires et futurs (mariage, divorce, décès). Cet acte comprend le prénom, le nom, le sexe, la date et l'heure de naissance de la personne, son lieu de naissance, ceux de ses parents, ainsi que leurs noms, dates, professions et lieux de naissance. Pourtant, ce sont près de 51 millions de naissances qui ne sont pas enregistrées chaque année, soit près de 166 millions d'enfants dans le monde. Ce fléau de non-déclaration des enfants entraîne des conséquences sociales et économiques désastreuses pour la société, notamment des difficultés d'accès aux services publics (justice, santé, éducation) et privés (banques, emploi), pour n'en citer que quelques-uns. Dans une majorité de ces cas, ces situations résultent d'une absence d'enregistrement au sein d'un état civil de confiance. Il serait plus juste de parler des droits à l'identité au pluriel, la conception unique de

[122] EYNARD Jessica et al., « L'identité numérique ; quelle définition pour quelle protection ? » *op. cit*., p.187.
[123] « Sans un acte de naissance justifiant son identité, l'enfant peut se voir privé d'accès à ses droits les plus fondamentaux (…) une identité légale à la naissance, un droit pour chaque enfant », in *Observatoire en ligne d'IN Groupe*, 19 mai 2022, disponible à l'adresse suivante

l'identité regroupant un ensemble de conventions internationales qui consacrent puis protègent certains droits fondamentaux des personnes, dont celui de l'identité. Ce droit à l'identité est couvert par plusieurs traités et conventions internationales illustrées ci-après par ordre chronologique :



(i) La Déclaration de Genève sur les droits des enfants[124] représente le premier texte fondateur à reconnaître en cinq articles l'importance d'un droit à l'identité pour chaque enfant. Cette déclaration internationale (non contraignante) est adoptée le 26 septembre 1924 par la Société des Nations (SDN)[125]. Ce texte énumère les besoins fondamentaux de l'enfant et les responsabilités qui incombent en principe aux adultes pour y répondre. Il exprime ainsi la reconnaissance du droit de l'enfant au développement, à l'assistance, au secours et à la protection.

(ii) En raison de sa vocation universelle, la Déclaration Universelle des Droits de l'Homme (DUDH) représente une seconde reconnaissance en devenant désormais un socle du droit international (non exclusivement réservé aux enfants) qui reconnaît un droit à l'identité juridique « *chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique.* »[126]. Une décennie plus tard, ce principe sera spécifiquement appliqué aux enfants en vertu de la règle n°3 de la Déclaration des droits de l'enfant du 20 novembre 1959 « *l'enfant a droit, dès sa naissance, à un nom et à une nationalité* »[127].

(iii) Cependant, il faudra attendre la ratification et l'adoption du Pacte international relatif aux droits civils et politiques (PIDCP) du 16 décembre 1966, pour que la DUDH et la Déclaration des droits de l'enfant confèrent certaines dispositions contraignantes à ses parties signataires (soit près d'un demi-siècle écoulé entre la Déclaration de Genève et le PIDCP).

(iv) Si ces quelques traités-cadres ont permis de poser les fondements juridiques d'une forme de droit international à l'identité, il convient d'admettre que c'est la Convention internationale

[124] Déclaration de Genève sur les Droits de l'Enfant, 1924, in *Humanium*, consulté en ligne le 30 avril 2021.
[125] Le rôle de la SDN est d'assurer le maintien de la paix dans le monde : lutter pour les droits des enfants lors des conflits, pour une prévention contre les guerres, une négociation et une résolution des conflits. Après la Seconde Guerre mondiale, la SDN sera remplacée par l'ONU (décision prise à la conférence de Yalta en 1945).
[126] *Ibid.* Art. 6, consulté le 3 mai 2021.
[127] Déclaration des Droits de l'Enfant du 20 Novembre 1959 - Texte intégral, in *Humanium*, consulté en ligne le 3 mai 2021.

relative aux droits de l'enfant (CIDE)[128] qui en constitue la pierre angulaire depuis 1989. En effet, elle caractérise un consensus juridique inédit au sens de la communauté internationale en représentant la convention relative aux droits de l'homme la plus ratifiée de l'histoire : 195 États ratificateurs excepté les États-Unis et la Somalie[129]. La CIDE et ce droit à l'identité pour les enfants sont initialement à l'initiative du Fond des Nations Unies pour l'enfance (UNICEF). D'une part, la CIDE réaffirme dans son article 7 la garantie d'un droit au nom et à la nationalité pour chaque enfant des États signataires[130], et d'autre part dans son article 8[131], elle impose à ces derniers de faire respecter ces mêmes droits au sein de leurs juridictions respectives. Dès lors, cette convention possède une portée symbolique importante qui, couplée à une contrainte juridique sans précédent[132], en fait un outil au service d'un droit à l'identité. À partir des années 2000, cette volonté d'adoption puis d'application d'un droit à l'identité universel se renforce. Le 10 mai 2002, l'Assemblée générale des Nations Unies adopte la résolution S-27/2, dite « *Un monde digne des enfants* », dans laquelle les gouvernements réaffirment leur engagement commun pour « *mettre en place des systèmes d'enregistrement de tous les enfants à la naissance ou peu après, et respecter le droit de chaque enfant à un nom et à une nationalité, conformément à la législation nationale et aux instruments internationaux pertinents* »[133].

Malgré ces bases légales et internationales robustes, force est de constater qu'à ce jour un milliard de personnes ne disposent pas de document officiel pour prouver leur identité. Si rien ne change d'ici 2030, environ un tiers des pays du monde devront accélérer leur politique de recensement des naissances et de fourniture d'une identité juridique pour leurs citoyens afin de respecter l'objectif n°16.9 des objectifs de développement durable (ODD). Ce même objectif n°16.9 de l'Assemblée générale des Nations Unies a été annoncé au siège de l'ONU en septembre 2015 afin de mettre en place un programme « *universel, intégré et porteur de transformation qui nous conduira à un monde meilleur* », selon une déclaration de

[128] Adoptée le 20 novembre 1989 et entrée en vigueur le 2 septembre 1990 soit trente ans après la Déclaration des droits de l'enfant du 20 novembre 1959.
[129] BENNOUNA Mohamed. La convention des Nations Unies relative aux droits de l'enfant, in *Annuaire français de droit international*, volume 35, 1989. p.433-445. Signé par la France le 26 janvier 1990 et ratifié le 7 août 1990 pour une entrée en application le 6 septembre 1990.
[130] Art 7-1 et 7-2 de la CIDE : « 1° L'enfant est enregistré aussitôt à sa naissance et a dès celle-ci le droit à un nom, le droit d'acquérir une nationalité et, dans la mesure du possible, le droit de connaître ses parents et d'être élevé par eux ; 2° Les États parties veillent à mettre ces droits en oeuvre conformément à leur législation nationale et aux obligations que leur imposent les instruments internationaux applicables en la matière, en particulier dans les cas où faute de cela l'enfant se trouverait apatride ». *v*. unicef.fr
[131]Art. 8-1 et 8-2 : « 1° Les États parties s'engagent à respecter le droit de l'enfant de préserver son identité, y compris sa nationalité, son nom et ses relations familiales tels qu'ils sont reconnus par loi, sans ingérence illégale ; 2° Si un enfant est illégalement privé des éléments constitutifs de son identité ou de certains d'entre eux, les États parties doivent lui accorder une assistance et une protection appropriées, pour que son identité soit rétablie aussi rapidement que possible ».
[132]Art. 41 : « Si une disposition relative aux droits de l'enfant figurant dans le droit national ou international en vigueur pour un État est plus favorable que la disposition analogue dans cette convention, c'est la norme plus favorable qui s'applique ».
[133] ONU, « Un monde digne des enfants - Assemblée générale - 6e séance plénière », téléchargé en ligne ou accessible ici le 3 mai 2021.

l'ancien Secrétaire général de l'ONU, M. Ban Ki-moon[134]. Autrement dit, l'identité juridique est et restera d'ici 2030, au cœur des préoccupations juridiques de nombreuses institutions internationales. Toutefois, selon l'UNICEF « *il est clair qu'à moins que le rythme de l'enregistrement des naissances ne s'accélère considérablement dans tous les pays, en particulier en Afrique, nous manquerons de loin la cible 16.9 des ODD* »[135]. De même, le Conseil des Droits de l'Homme (CDH) a adopté la disposition n°43/L.3 le 19 juin 2020, en se déclarant « *1° profondément préoccupé par le fait que* (…) *237 millions d'enfants n'ont toujours pas d'acte de naissance malgré les efforts qui sont faits* (…) *; 2° Rappelle aux États l'obligation qui leur est faite d'enregistrer toutes les naissances sans discrimination aucune, et leur rappelle aussi que chaque enfant devrait être enregistré immédiatement après sa naissance dans le pays où il est né,* (…) *conformément au droit international des droits de l'homme* (…) ; 3° *Réaffirme que le fait de garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances, d'ici à 2030 peut contribuer à prévenir, entre autres, la pauvreté, la marginalisation, l'exclusion* (…) »[136].

Assurer l'organisation de l'enregistrement des naissances est une nécessité au bon développement social, démocratique et économique d'un État. Pour cela, il doit pouvoir être en mesure technique d'identifier puis d'administrer sa population, c'est-à-dire de former une nation notamment par une personnalisation des titres d'identité aux couleurs de la nation. En réalité, l'État est tout aussi garant que bénéficiaire de l'identité des personnes. Pour cela, ses ressources publiques comme l'imposition doivent être stables, ce qui implique une identification à la source de ses administrés, si possible dès leur naissance. Une connaissance rigoureuse de sa population permet de construire un registre d'état civil qui bénéficie aux ayants droits qui y sont inscrits, et un cercle vertueux s'instaure grâce à une identification fidèle. Cette identification des personnes est également nécessaire aux diverses décisions, projections et politiques macroéconomiques, budgétaires ou monétaires. Lorsqu'un État ne dispose pas de système d'identification efficace, cela peut mettre en péril sa démocratie, car en l'absence d'un registre d'état civil fiable et de documents officiels correspondants, la fraude électorale peut se développer. Dans de telles situations, l'identité juridique des individus devient une façade trompeuse et parfois une illusion source de méfiance pour les citoyens.

Sans existence et protection juridique ou encore sans accès à l'éducation, les enfants sont exposés à tous les trafics : travail sous contrainte, trafics d'organes et traite des êtres humains, abus physiques, psychologiques entre autres. Plus généralement, l'absence d'identité légale engendre un impact social et psychologique destructeur, tout au long de la vie d'un enfant. Le fait de ne pas être enregistré à l'état civil peut causer un sentiment d'exclusion chez un enfant, surtout s'il fait partie d'une communauté où

[134] « L'Assemblée générale adopte un de développement durable ambitieux pour 'transformer notre monde' d'ici à 15 ans », Couverture des réunions communiqués de presse, in *UN Press*, disponible à l'adresse suivante
[135] Workshop « Mission 100 : vers une identité juridique à 100% d'ici 2030 », ID4AFRICA financé par UNICEF, note conceptuelle de l'atelier du 16 juin 2022.
[136] Enregistrement des naissances et droit de chacun à la personnalité juridique - Conseil des droits de l'homme, consulté le 3 mai 2021.

les autres membres sont enregistrés et profitents d'avantages liés à cet enregistrement. En principe, un état civil requiert une répartition territoriale condensée et doit permettre de s'adapter aux changements démographiques. Cela nécessite une relation fluide entre les centres de déclaration comme les hôpitaux, les mairies et ceux de l'état civil. En 2020, le Haut commissariat pour les réfugiés (HCR) estime à 10 millions le nombre d'apatrides dans le monde, dont un tiers d'enfants[137]. Par conséquent, la mise en place de dispositifs nationaux d'identification fiable des personnes reste aujourd'hui un défi informatique, économique, social et juridique pour de nombreux États. Ce défi économique est directement lié à la possibilité de déployer des infrastructures dédiées à l'identification des personnes. L'UNICEF constate ainsi « *une corrélation entre le revenu national par habitant et la mise en place d'un système efficace d'enregistrement des faits d'état civil dans un pays. Plus un État dispose d'un budget public élevé, plus il pourra créer des centres d'état civil (y compris des centres mobiles, pour les régions les plus difficiles d'accès), les équiper (notamment en matériel numérique), mais aussi recruter et former des agents d'état civil* »[138].

Dans de nombreux pays, l'émission de titres d'identité tels que les actes de naissance nécessitent un acte administratif payant pour les citoyens, notamment en Afrique subsaharienne « *où les 20 % d'enfants les plus pauvres ont deux fois moins de chance d'être enregistrés à la naissance que les enfants les plus riches* ». Cependant, le coût administratif en question ne constitue qu'un aspect direct des dépenses, souvent accompagné de coûts indirects qui sont tous liés à ce même processus (tels que le transport nécessaire pour enregistrer son état civil, la perte de salaire des parents durant leur déplacement et leur absence au travail, la perte des documents d'identité). L'aspect économique est étroitement lié à des considérations d'ordre juridique, c'est-à-dire au droit en vigueur dans les pays susmentionnés. Il semble que seul un régime juridique transparent permette de proposer un enregistrement national quasi gratuit pour ses citoyens et tout particulièrement pour les enfants. En réalité, de nombreux pays possèdent toujours des régimes juridiques disparates, voire obsolètes, tant au regard des coûts d'enregistrement que des délais administratifs de délivrance des titres d'identité lorsqu'ils existent. L'aspect économique précité représente donc un facteur déterminant dans l'implémentation et l'encadrement juridique accordé à tout état civil. De plus, cela s'accompagne souvent de contraintes informatiques en complément des contraintes juridiques susvisées. En principe, pour garantir la protection des libertés fondamentales des citoyens, un état civil numérique doit respecter un cahier des charges technique assurant une conformité et une protection des informations d'identité. En pratique, de nombreux États ont mis en place des dispositifs qui ne respectent pas ces critères, que ce soit en termes de sécurité informatique, de conformité technique ou de protection juridique des données personnelles. Les conséquences de ces insuffisances ou inadéquations peuvent être graves : vol de données personnelles,

[137] « L'apatridie », publié le 5 juin 2020, in Forum réfugiés, consulté à l'adresse suivante
[138] Assemblée nationale, Rapport d'information n°3349 déposé par la commission des affaires étrangères, en conclusion des travaux d'une mission d'information sur les enfants sans identité (Mme Laurence Dumont et Mme Aina Kuric), consulté en ligne le 29 avril 2021.

utilisation discriminatoire des données et violation de la vie privée des personnes, destruction et/ou modification des données du registre d'état civil sans fondement légal. Couplé à un manque de moyens humains, matériels et administratifs, l'état civil est ainsi limité dans sa capacité d'enregistrement autant que dans sa pertinence, dès lors qu'il est présumé faillible. Pour illustrer ce propos, l'état civil sénégalais est administré par des agents bénévoles ou contractuels (environ 50%) dont les connaissances et formations à la procédure administrative sont régulièrement incomplètes et parfois lacunaires[139]. La numérisation progressive des états civils à travers le monde reste aujourd'hui très hétérogène malgré une réelle volonté internationale de standardisation et d'harmonisation juridique et informatique[140]. Relativement complexe pour les raisons évoquées précédemment, de nombreux pays en voie de développement mettent en place des projets d'états civils numériques qui ne respectent peu ou pas encore les bonnes pratiques des pays développés, principalement par manque de moyens informatiques. S'ajoutent à ces problèmes structurels des problématiques organisationnelles, comme le manque de communication entre certains ministères ou institutions et organisations qui développent des projets séparés dont la finalité est pourtant la même, celle de développer un état civil numérique fiable « *l'UNICEF insiste sur la nécessité d'inclure l'enregistrement des naissances et la délivrance d'un acte associé dans tous les projets qui concernent l'état civil. La France doit impérativement défendre la même position que l'UNICEF* »[141]. Il convient également d'évoquer la discrimination culturelle et sociale en forte opposition avec le droit à l'identité familiale[142]. Concrètement, une inégalité de genre existe dans certains pays et de manière prononcée, en défaveur des femmes et par extension de leurs enfants. Parfois, seuls les hommes possèdent la capacité juridique de déclarer leurs enfants[143]. Le résultat de ces traits culturels, que les pays développés ont pour rappel également traversé, est inévitable : faute de ressources financières et de temps, la plupart de ces hommes ne parviennent pas à enregistrer la naissance de leurs enfants, ce qui conduit souvent à ce que ceux-ci n'aient qu'un nom d'usage. En pratique, dès que deux parents possèdent une même capacité juridique, les probabilités de déclaration augmentent significativement. Enfin, il est souligné qu'en cas d'absence, de contestation de paternité ou de décès du père, les femmes représentent l'unique chance pour un enfant d'être déclaré pour obtenir une existence légale. Ainsi et d'une certaine façon, les coutumes culturelles de certains pays accentuent et aggravent leur déficit d'identification. Depuis 2019, l'UNICEF préconise cinq mesures

[139] FOUQUET Kevin, « L'état civil sénégalais aujourd'hui de l'enregistrement à l'archivage, les difficultés d'un outil de bonne gouvernance et de respect des droits humains », « (…) en outre, seulement 14 % des agents sont fonctionnaires. Le reste est soit contractuel (50 %) soit bénévole. Le personnel est donc dans une situation précaire, sachant que leur rémunération est faible, et que leur situation se précarise fatalement … », 11 juin 2020, consulté en ligne, p.77.

[140] « Les 'CNIL' mondiales prennent position sur les grands débats internationaux en matière de protection des données personnelles CNIL », consulté le 12 novembre 2021 à l'adresse suivante

[141] Rapport Assemblée nationale. *op. cit*. Disponible à l'adresse suivante

[142] Une protection et une assistance aussi larges que possible doivent être accordées à la famille, qui est l'élément naturel et fondamental de la société, en particulier pour sa formation et aussi longtemps qu'elle a la responsabilité de l'entretien et de l'éducation d'enfants à charge. Le mariage doit être librement consenti par les futurs époux, Art. 10, HCDH | Pacte international relatif aux droits civils et politiques, consulté en ligne le 3 mai 2021.

[143] En Indonésie, les mères célibataires ou encore les mères qui ne disposent pas de certificat de mariage ne sont pas autorisées à enregistrer leur enfant et filiation auprès de l'état civil. Parallèlement, l'état civil du Bhoutan ne reconnaît pas les enfants de père inconnu.

particulièrement pertinentes pour fournir puis protéger, dès leur naissance, le droit à l'identité des enfants : « *1. Délivrer un acte de naissance* [ou plutôt une preuve d'identité] *à chaque enfant dès sa naissance. 2. Donner à tous les parents, quel que soit leur genre, les moyens d'enregistrer leurs enfants à la naissance. 3. Relier l'enregistrement des naissances aux services sociaux. 4. Investir dans des solutions technologiques sûres et innovantes afin de faciliter l'enregistrement des naissances. 5. Inciter les communautés à exiger l'enregistrement de la naissance de chaque enfant* ». À la lumière de ces constats relatifs à l'importance de l'identité et des droits des enfants et par conséquent des adultes, il est émis l'hypothèse que certaines caractéristiques informatiques des technologies blockchains puissent représenter un outil technique majeur au service d'une identité numérique accessible et juridiquement reconnue par tous.

1.1.3.2 Droit naturel, revendications identitaires et identité universelle

Le droit naturel prend son fondement dans la nature humaine. Il prend racine dans le comportement naturel des personnes, dans leur instinct supposé inné à respecter les autres personnes, elles aussi assujetties à ce droit naturel. Il est réputé universellement valable et applicable à toute personne, quel que soit le lieu où la temporalité, l'époque choisie. En termes juridiques, la loi naturelle est une « *règle considérée comme conforme à la nature* [de l'homme] *et à ce titre reconnu comme de droit idéal* »[144]. Plus simplement, le droit naturel est une forme de ressenti juridique, latent ou exprimé, qui serait ancré au plus profond de l'humanité. Contrairement au droit positif qui évolue et sanctionne selon l'évolution des mœurs sociales, le droit naturel est fixe. Selon le philosophe anglais John Locke, le droit positif et le droit naturel ne sont pas opposables, mais plutôt cumulatifs. Le droit naturel, selon Locke, est universel et transcende les lois édictées par les gouvernements. Il est fondé sur les principes de la raison et de la justice naturelle, et est applicable à tous êtres humains. Pour Locke, les individus ont des droits naturels tels que la vie, la liberté et la propriété, qui sont antérieures à l'existence de l'État que ce dernier doit protéger. Pour lui, l'origine naturelle de tout Homme est d'être par essence dans « (…) *un état de parfaite liberté, un état dans lequel, sans demander de permission à personne, et sans dépendre de la volonté d'aucun autre homme, ils peuvent faire ce qui leur plaît, et disposer de ce qu'ils possèdent et de leurs personnes, comme ils jugent à propos, pourvu qu'ils se tiennent dans les bornes de la loi de la Nature* »[145]. En somme, John Locke a défendu l'idée que le droit naturel est supérieur au droit positif et que ce dernier doit être en conformité avec le droit naturel pour être moralement juste. Le gouvernement est tenu, selon lui, de protéger les droits naturels des individus et de respecter leurs libertés individuelles, et ce, même si cela implique de limiter son propre pouvoir. L'étude des fondements du Web 3.0 nous

[144] CORNU Gérard, « Vocabulaire juridique », in Association Capitant, 8e éd., 2007, PUF coll. Quadrige.
[145] LOCKE John, « Traité du gouvernement civil », 1690, Traduction française de David Mazel en 1795 à partir de la 5e édition de Londres en 1725, p.17, disponible à l'adresse suivante

amène à supposer que ces fondements du droit naturel rejoignent l'idée qu'une loi cryptographique auto-régulée par des communautés en ligne serait supérieure au droit positif.

Le droit interne dispose depuis longtemps de principes universels en vertu de l'article premier de Déclaration des droits de l'homme et du citoyen de 1789 qui édicte « *Les hommes naissent et demeurent libres et égaux en droits. Les distinctions sociales ne peuvent être fondées que sur l'utilité commune.* »[146]. Le caractère universel et inaltérable du droit naturel peut également être lié à la volonté d'assurer un droit universel à l'identité pour tous les individus. Cette idée d'une universalité de l'identité était déjà exprimée par l'académicien français Amin Maalouf avant la croissance de l'ère numérique 1.0 « *Par regroupements régionaux successifs* [via internet]*, l'humanité allait atteindre un jour le rassemblement suprême* [une identité universelle] »[147]. Toujours selon l'académicien « *Le postulat de base de l'universalité, c'est de considérer qu'il y a des droits inhérents à la dignité de la personne humaine* [c'est-à-dire que chacun puisse vivre avec honorabilité et décence] ». En pratique, pour atteindre une telle identité universellement attribuée et revendiquée à l'échelle planétaire, plusieurs questions se font jour, à savoir comment créer une source mondiale d'identité (numérique) à laquelle tout le monde peut faire confiance, mais qui n'est ni détenue ni contrôlée par une entreprise ou un gouvernement en particulier ? Vivons-nous une guerre des identités ou simplement des revendications politiques dues à une liberté d'expression favorisée par le numérique ? Comment faire en sorte que la mise en avant des identités n'entraîne pas la radicalisation des débats, c'est-à-dire une forme de fragmentation de la société civile ? Étymologiquement, l'universel est ce qui « *s'étend à la terre entière* »[148], c'est-à-dire à toute personne. Selon le dictionnaire Larousse, il est possible d'attribuer plusieurs sens au terme « universel »[149]. Toutefois, nous considérons les sens suivants dans le cadre de notre recherche « *qui embrasse la totalité des êtres et des choses : une valeur universelle.* » ; « *qui a le caractère de l'universalité* » et « *ce qui est universel : s'élever du particulier à l'universel* ». L'universel est en principe ce qui prend en considération et inclut tous les cas sans exception. L'universalisme de l'identité représente l'identité concernant l'humanité entière, c'est-à-dire le fait même d'exister et d'avoir une identité.

Ces quelques concepts distingués, il faut à présent approfondir la notion d'universalité technologique, qui fait référence dans cette recherche au caractère universel de l'identité numérique. Dans l'univers en ligne, le concept d'universalité renvoie à une accessibilité et à une ouverte des systèmes d'information, en principe sans frontières ni distinctions pour ses internautes. Certains juristes sont précurseurs et ont compris que l'aspect universel de l'identité numérique est une nécessité « *L'identité numérique*

[146] Déclaration des Droits de l'Homme et du Citoyen de 1789. Conseil constitutionnel. Consulté le 5 septembre 2022 à l'adresse suivante
[147] MAALOUF Amin, *op. cit.* « Les identités meurtrières », « […] les nouveaux moyens de communication offrent à un très grand nombre de nos contemporains, à des gens qui vivent dans tous les pays et sont porteurs de toutes les traditions culturelles, la possibilité de contribuer à l'élaboration de ce qui deviendra demain notre culture commune », p.112 et pp.147-189.
[148] Etymologie d'universel. cnrtl.fr. Disponible à l'adresse suivante
[149] Larousse. Définitions, in *Dictionnaire de français Larousse*, consulté le 5 septembre 2022 à l'adresse suivante

opposable en droit, supranationale, garante de la protection totale des données personnelles, est une nécessité absolue dont l'industrie numérique ne saurait s'exonérer plus avant »[150]. Une identité numérique universelle consisterait, par sa simple existence, à affirmer en ligne notre appartenance à la civilisation humaine. Une telle possibilité permettrait à toute personne de rejoindre une humanité numérique composée de simples existences individuelles et vérifiées. Cette preuve d'existence numérique permettrait également d'ouvrir la reconnaissance de droits associés, selon les fonctionnalités et limites informatiques qu'un tel système impliquerait. Une identité numérique universelle devrait permettre aux personnes de revendiquer leur singularité et certaines de leurs appartenances, car l'uniformité empêche toute identité singulière. L'académicien Amin Maalouf pose la question de savoir si nous devrions nous réjouir du fait que les hommes deviennent de plus en plus semblables[151]. Une réponse en deux temps semble possible, d'une part, l'uniformisation des Hommes peut conduire et faciliter une identité universelle, et d'autre part, elle peut également contribuer à détruire la diversité culturelle. Ainsi, la promotion des identités en ligne ne menace pas l'universalité d'une identité numérique décentralisée, comme nous l'étudions plus loin, mais la renforce au contraire par la diversité. Avec une identité numérique par conception ouverte et interopérable, chaque personne peut ainsi rejoindre une forme d'identité universelle en ligne au sein de laquelle elle peut revendiquer certaines de ses parcelles et appartenances identitaires.

Toutefois, une distinction importante doit être faite entre un système d'identité numérique universelle et un système universel de preuves d'identité numérique. Le premier a vocation à servir de système d'identification et d'authentification commun à l'ensemble des personnes physiques, tandis que le second a pour vocation plus particulière de servir de socle puis de passerelle numérique au service d'autres systèmes d'identité traditionnels (état civil, identité numérique 2.0 par exemple). Ainsi, un système d'identité universel est plus large et utopique qu'un système de preuve d'identité à vocation universelle dont l'objectif est de parfaire les systèmes d'identité déjà existants. L'identité numérique décentralisée (IND) étudiée plus loin, représente un nouveau socle technique au service du contrat social de John Locke. Avec une IND, le pouvoir législatif demeure aux mains des fournisseurs d'identité, tandis que le pouvoir exécutif est transféré aux internautes qui en ont le contrôle. Les technologies blockchains pourraient être utilisées en tant que registre ouvert de données, permettant d'y ancrer certaines informations d'identité de façon immuable et décentralisée sur Internet[152]. En d'autres termes, mettre en place un système universel et décentralisé de preuves d'identité permet dans une certaine mesure de tendre vers une identité numérique grâce à la réappropriation des comportements et des identités numériques par les internautes. A cet égard, le Forum économique mondial (« World Economic

[150] BENSOUSSAN Alain, *op. cit.*, « L'identité numérique 5.0 », p.47.
[151] MAALOUF Amin, « Faut-il vraiment se réjouir de voir les hommes de plus en plus semblables ? », *op. cit.*, "Les identités meurtrières", p.120.
[152] De FILIPPI Primavera, « Blockchain and the law », « Au fil du temps, les blockchains pourraient ancrer de nouvelles infrastructures publiques et même potentiellement des systèmes mondiaux et transnationaux, accessibles à toute personne disposant d'une connexion Internet », in *Harvard University Press*. Emplacement 109 sur 7004.

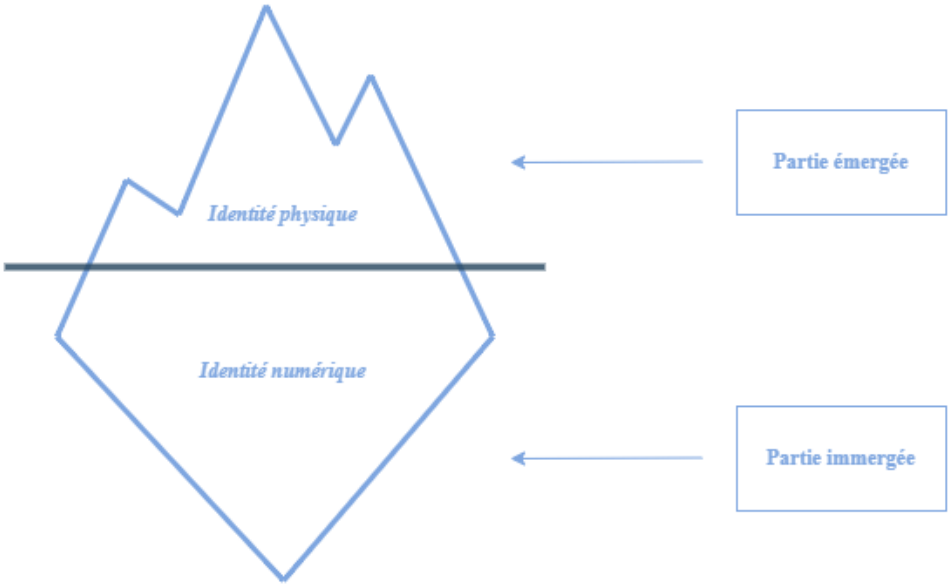
Forum – WEF ») propose de démontrer l'omniprésence et l'importance de l'identité numérique pour les droits des personnes en soulignant l'utilisation nécessaire des nouvelles technologies comme les blockchains[153]. Il semble ainsi que dans cette société moderne et numérique, les personnes prennent conscience de leurs appartenances identitaires, peut-être plus qu'auparavant. La technologie blockchain et l'identité numérique décentralisée permettent de nouvelles formes d'expression en ligne dont la vocation est d'être aussi universelle que possible. Atteindre une identité numérique universelle grâce aux technologies 3.0, comme l'identité numérique auto-souveraine, suppose toutefois un caractère d'unicité et d'opposabilité de son identité numérique envers des tiers. Pour que ces conditions soient respectées, chaque personne doit à la fois être l'émettrice ou le fabricant de ses propres preuves d'identité. Si en théorie, l'identité numérique auto-souveraine assure un tel fonctionnement, il s'avère en pratique qu'un tiers de confiance souverain (administration régalienne) demeure presque systématiquement requis pour l'émission d'identifiants et de preuves d'identité numérique primaire (civiles) et parfois même secondaire (étendues). Par conséquent, le droit à une preuve d'existence numérique universelle est souhaitable[154] et techniquement possible en utilisant le nouveau concept informatique de l'identité décentralisée qui prend déjà de l'ampleur grâce aux nouvelles technologies blockchains. Finalement, un système de preuve d'existence numérique universelle semble s'imposer grâce au nouveau concept technico-social d'une identité numérique décentralisée[155] reconnue, interopérable, sécurisée et industrialisable.

[153] Selon notre étude, l'identité numérique décentralisée (IND) pourrait être rajoutée à ce schéma publié par le World Economic Forum. Strategic Intelligence | World Economic Forum. Consulté en ligne le 02 mars 2023.

[154] A toutes les époques, il s'est trouvé des gens pour considérer qu'il y avait une seule appartenance majeure, tellement supérieure aux autres en toutes circonstances qu'on pouvait légitimement l'appeler 'identité'. Pour les uns, la nation, pour d'autres la religion, ou la classe. Mais il suffit de promener son regard sur les différents conflits [du XIXe siècle] pour se rendre compte qu'aucune appartenance ne prévaut de manière absolue, *op. cit.* Amin Maalouf, in « *Les identités meurtrières* », p.19.

[155] Nous considérons tout au long de cette thèse que le terme *d'identité numérique hybride* fait référence à une identité numérique 2.0 et/ou 3.0 dérivée d'une identité physique matérialisée par un titre d'identité. Une *identité numérique hybride* est ainsi une *identité numérique dérivée* d'un titre d'identité physique, civile et légale. V. Glossaire.

1.2 Exploration du concept d'identité en iceberg



Si l'identité était un iceberg, sa partie émergée constituerait son identité primaire, racine, objective, c'est-à-dire légale comme suggéré dans les parties précédentes. Sa partie immergée représenterait son identité secondaire, subjective, c'est-à-dire étendue. D'après une perspective globale, ces deux parties forment un tout unique, une identité globale. Il est également possible de se concentrer sur l'une ou l'autre de ces parties (émergée/immergée) selon les observations de chaque individu. Cet iceberg peut en effet être analysé d'autant de façons distinctes qu'il peut exister d'observateurs différents pour le décrire. En fonction de sa ligne de flottaison (ajustable), sa partie émergée peut paraître selon les contextes d'identité, plus importante que celle immergée et vice versa. En analysant ce concept à son paroxysme, si chaque Iceberg (analogie pour une personne) est unique par ses caractéristiques et qu'il se déplace différemment selon les océans sur lesquels il navigue (analogies aux cultures et sociétés), l'identité de chaque Homme serait comparable à un iceberg se laissant dériver sur les différents océans qui forment l'humanité. Cette analogie nous permet de souligner l'adoption possible d'une conception relativiste et globale de l'identité. Pour approfondir ce concept, une analyse de la partie externe (émergée) et interne (immergée) est possible, la partie externe représentant qui nous sommes au regard de la société, c'est-à-dire la part de l'être exposé à la socialité renvoyant une image sociale et externe de l'identité, la partie interne constituant notre identité subjective et psychologique, fortement influencée (parfois même en conflit et en contradiction) avec la partie externe de l'identité. La ligne de flottaison est supposée spécifique à chaque relation entre sa partie émergée et immergée, c'est-à-dire entre l'identité physique et numérique. Pour résumé avec cette analogie, ces deux parties coexistent pour une même personne, parce qu'un iceberg se transforme continuellement selon son environnement, consacrant ainsi la complexité du concept même d'identité. Cette étude retient trois éléments majeurs

de l’identité des personnes à l’ère numérique, à savoir leur identité physique, civile et psychosociale. Nous suggérons que ces éléments sont cumulatifs selon les contextes de l’identité globale qu’ils caractérisent.

Chapitre 2 : Chronologie d’une redéfinition de l’identité à l’ère numérique

Avant de retracer une chronologie partielle de l’histoire de l’informatique et de leurs considérations juridiques, depuis l’Internet 1.0 jusqu’à l’Internet 2.0 puis 3.0, deux considérations fondamentales sur le rapport entre l’Homme et l’informatique doivent être rappelées. Tout d’abord, l’informatique est binaire. Lorsqu’un ordinateur applique un modèle, il n’y a en principe plus de négociation sociale possible. Une négociation est toujours possible entre deux personnes, ce qui n’est pas le cas entre deux machines. La négociation en écho à la notion de consentement n’est pas un processus implémenté par défaut en ligne, il doit être conçu et programmé. Ainsi, l’ordinateur devient fatal puisqu’il ne peut négocier le réel à l’inverse de l’Homme. Cela s’observe fréquemment lorsqu’un service en ligne ne répond pas aux besoins d’un internaute, comme une simple omission d'une case à cocher ou l’impossibilité de contacter par téléphone un service, entraînant des délais dans le traitement de la requête. Si l’informatique est inévitable pour l’accès à certains services publics en ligne, il ne l’est pas pour l’identité numérique secondaire des internautes qui se négocie plus librement en ligne avec les réseaux sociaux. Si les technologies 3.0 n’échappent pas à ces principes de binarité et de non-négociation, il semblerait néanmoins qu’elles puissent contribuer à rendre certains processus de gestion de l’identité plus transparents et ouverts, c’est-à-dire partiellement négociés. Ensuite, l’idée selon laquelle tout fichier est un mauvais traitement pour l’Homme ne doit jamais être sous-estimée. L'acte de créer un fichier, qu'il soit physique ou numérique, implique l'établissement d'une relation non pas entre des êtres humains, mais entre un être humain et un objet. Cela signifie que la gestion d'objets peut parfois atteindre un tel niveau que l'humanité des individus en est effacée. En d’autres termes et en complément du point précédent, les relations sociales sont masquées par l'interaction entre l'Homme et la machine. La création d’un fichier introduit la possibilité de mauvais traitement par la réification, c’est-à-dire par la transformation d’un sujet humain en un objet ou identifiant informatique auquel est appliqué un traitement physique ou informatique qui peut dans certains cas être contraire aux règles juridiques ou morales. Ce principe s’applique à tous les fichiers sans exception, et résumer la vie des hommes sur des fichiers implique nécessairement un risque de mauvais traitement possible. Par exemple, si un juge ne jugeait des affaires que par des faits issus de fichiers informatiques et sans que le présumé coupable puisse s’exprimer, alors son jugement se retrouverait déshumanisé et probablement source de mauvais traitements. Les technologies et leurs applications 3.0 peuvent représenter un risque, ces dernières plus ou moins décentralisées offrant la possibilité de stocker de manière immuable des fichiers tels des identifiants et des interactions numériques d'internautes sur des infrastructures décentralisées, comme

les blockchains publiques, ce qui rend impossible toute modification ou suppression. En considérant ces propos, il est suggéré que les données personnelles ne devraient pas être considérées comme relevant du droit commercial, mais certainement du droit des personnes. Les données personnelles font partie intégrante de leurs identités, ce qui implique qu'une marchandisation de ces données n'est pas souhaitable, même si elle est informatiquement d'ores et déjà possible avec le Web 3.0.

2.1 Les origines d'Internet (Web 1.0)

En 1969, l'ancêtre d'Internet, baptisé Arpanet pour « Advanced Research Projects Agency Network », était un projet militaire destiné à répondre à des problématiques de communication stratégique à l'échelle des États-Unis. Ce projet avait pour objectif initial de rattraper leur retard technologique face au progrès technologique de l'Union soviétique[156]. Cependant, le « World Wide Web – *www* », Internet[157], a très vite dépassé l'idée première de ses concepteurs dont le célèbre informaticien britannique Tim Berners-Lee est le principal fondateur[158], avant d'être reprise par la communauté scientifique et universitaire[159]. Ces travaux académiques et scientifiques ont très largement influencé l'infrastructure d'Internet avec notamment la remise en question progressive de sa neutralité[160]. Si Internet a ainsi pu se développer grâce à des financements de l'armée américaine, son expansion résulte également de l'idéologie première de sa communauté d'ingénieurs, pour qui le respect et la protection des droits et des libertés en ligne étaient fondamentaux[161]. Dès ses débuts, la dimension sociale du projet est majeure puisque toutes ses avancées techniques résultent d'idéologies et de multiples communautés qui ont fait d'Internet ce qu'il est aujourd'hui. Ainsi, avant d'être un territoire, Internet est un mouvement social[162], un constat également partagé s'agissant de la révolution du Web 3.0 dans lequel il s'inscrit. À partir du lancement officiel d'Internet le 1er janvier 1989 et avec l'apparition du lien hypertexte et du navigateur NCSA MOSAIC[163], Internet s'étend progressivement sur toute la planète

[156] Le 4 octobre 1957, les Soviétiques lancent le premier satellite artificiel de l'histoire nommé « *Spoutnik* », une course technologique s'annonce.
[157] Issu de l'anglais « *network* » et traduit librement par « *inter* » suivi de « *net* », pour « *réseau* ». Désigne ainsi un réseau mondial de télécommunication reliant des ordinateurs ou des réseaux locaux permettant l'acheminement de données de différente nature (messages électroniques, textes, images, sons).
[158] Timothy John Berners-Lee est un informaticien anglais surtout connu comme l'inventeur du *World Wide Web*. Il est professeur d'informatique à l'université d'Oxford et professeur au Massachusetts Institute of Technology. Le 6 août 1991, ce dernier met en ligne le tout premier site internet qui décrit sommairement le premier mode d'emploi du web et donne accès à son code source, c'est-à-dire au cœur d'Internet, afin que chaque utilisateur puisse le récupérer et contribuer à son expansion : Timothy John Berners-Lee vient d'offrir Internet à l'humanité et nous constatons que Satoshi Nakamoto a fait de même concernant le protocole Bitcoin. Le point de convergence entre ces deux personnages énigmatiques se caractérise ainsi par leur humanisme et désintéressement financier.
[159] L'histoire s'est écrit le 29 octobre 1969, lorsque deux ordinateurs (à UCLA et à Stanford) se sont connectés pour la première fois par communication satellite, faisant de ces deux établissements d'enseignement supérieur les premiers hôtes de ce qui deviendrait plus tard (le 6 août 1991 lorsque Tim Berners-Lee annonce la création du *World Wide Web* Internet.
[160] Il s'agit du principe d'égalité et de traitement (non-discrimination) de tous les flux de données sur Internet.
[161] La liberté d'accès et la quasi-gratuité sont à l'origine d'Internet qui répond en réalité à un besoin de sociabilité.
[162] « Internet History of 1980s | Internet History | Computer History Museum », consulté en ligne le 13 janvier 2022 ; En 1985, Internet comptait environ 2000 utilisateurs/hébergeurs, *v.* PARACHINI A. « 30 ans du web : les grandes dates de l'histoire d'internet », in *Le Quotidien*, 2019, disponible à l'adresse suivante
[163] Wikipédia, l'encyclopédie libre, *Mosaic (web browser)*, consulté le 27 juillet 2021.

pour devenir ce que cette recherche désigne comme l'Internet 1.0 ou le Web 1.0 en anglais (~1990-2005)[164]. Vient ensuite l'Internet 2.0 (~2005-2020) avec lequel apparaît l'émergence des réseaux, c'est-à-dire des premières communautés en ligne, blog et réseaux sociaux. En 2022, ce sont près de 4,9 milliards d'internautes[165] qui consomment du contenu en ligne quotidiennement sur des sites internet tels que Facebook, Amazon ou Google pour les plus célèbres.

Depuis les origines du Web 1.0, Internet 2.0 est devenu plus immersif, plus consumériste au sein duquel l'internaute trouve tout ce dont il a besoin de façon quasi instantanée. Il devient un client potentiel à la recherche de satisfaction de ses propres envies réelles ou latentes. Ce phénomène de commercialisation des données et des identités numériques sur Internet a commencé au milieu des années 1990 en raison d'une structuration de marché principalement duale impliquant des internautes et des professionnels. Ces deux catégories - aujourd'hui non exclusives - fonctionnent de la manière suivante : l'utilisateur est le sujet d'une collecte massive de ses données personnelles en échange d'un accès à des fournisseurs de service qui génèrent des revenus publicitaires indexés sur la valorisation du profilage des personnes et de leurs données récoltées. En d'autres termes, Internet n'est plus simplement devenu un moyen d'accès à la connaissance, mais une fin permettant aux utilisateurs d'échapper à une certaine réalité sociale[166]. À ce stade, il semble impossible d'aborder le sujet des technologies 3.0 sans comprendre l'importance et l'impact des technologies 2.0 qui font autant référence au concept d'identité numérique qu'aux réseaux sociaux en ligne. Quelques décennies plus tard, ces pratiques de développement ont provoqué une centralisation progressive et assumée d'Internet et directement opéré par les fournisseurs d'exploitation et de services, les GAFAM et BHATX[167] détenant et exploitant les serveurs jusqu'à dépasser certaines limites en matière de protection des données et de libertés individuelles. Cette centralisation informatique s'est parallèlement accompagnée d'une centralisation juridique comme l'explique la juriste et docteure en droit Primavera De Filippi : « *bien que la conception initiale d'Internet visait à décentraliser le pouvoir et à encourager la liberté de communication - même au détriment du spam, de la fraude et du crime - au cours de la dernière décennie, il est devenu de plus en plus concentré et réglementé* »[168]. Dans sa nouvelle stratégie publiée en 2021, la Commission européenne insiste

[164] Aussi désigné par *Read only web* en raison d'une lecture seule par l'internaute des informations sur le site internet. Ce schéma unidirectionnel limitait les interactions entre les internautes, car peu ergonomique, accessible et intuitif. Le Web 1.0 permet une simple lecture de données en ligne, le Web 2.0 une lecture et écriture de données en ligne et le Web 3.0 une lecture, écriture et propriété des données en ligne, ce dernier étant une combinaison du souhait originel de décentralisation et de gouvernance par la communauté du Web 1.0 avec les fonctionnalités d'interaction modernes du Web 2.0.

[165] PATARD Alexandra, 26 janvier 2022, « 30 chiffres sur l'usage d'Internet, des réseaux sociaux et du mobile en 2022 », in *BDM*, disponible à l'adresse suivante

[166] En témoignent les phénomènes qui se multiplient de cyberharcèlement ou encore d'isolation sociale au Japon (les « *Hikikomori* »).

[167] GAFAM est l'acronyme des cinq plus grandes entreprises du Web américain -Google, Apple, Facebook, Amazon et Microsoft - qui dominent le marché numérique mondial tout en proposant des systèmes d'identification numériques à leurs utilisateurs. BHATX est l'acronyme de Baidu, Huawei, Alibaba, Tencent, Xiaomi, les cinq plus grandes entreprises technologiques chinoises.

[168] De FILIPPI Primavera, « Blockchain and the Law », in *Harvard University Press*. Emplacement 189 sur 7004.

justement sur l'importance de l'instauration d'une nouvelle confiance numérique[169]. Progressivement, les algorithmes de recommandation et de ciblage[170] exercent une influence de plus en plus croissante et participent à une forme d'enfermement inconscient de l'utilisateur dans une bulle personnalisée dont il n'est plus maître. L'internaute est en quelque sorte réduit à être un temps de cerveau disponible avec peu de capacité de comprendre comment sont gérées ses données dans les coulisses des architectures informatiques des « Big Techs » qu'il sollicite en permanence. Combien de données sont récoltées ? À quelles fins ? Pour quelle valorisation ? Quels impacts pour les personnes et leur identité personnelle, collective ?

Autant de questions non exhaustives dont les réponses ne sont que partielles, comme le soulignait l'ancienne Vice-Présidente de la Commission européenne Margrethe Vestager « *lorsque les systèmes de recommandation choisissent les informations à promouvoir et celles à cacher, ils affectent profondément ce que nous savons sur le monde.* (…) *Le monde que nous voyons à travers ces plateformes semble si réel qu'il peut être difficile de se rappeler qu'il est en fait construit à travers les choix que font les algorithmes sur ce que nous devrions voir* »[171]. D'autres dérives adjacentes, comme la surveillance de masse, les risques de fuites des données à caractère personnel ou la censure, se sont fait jour. À titre d'illustration, selon un rapport du Pew Research Center[172], la majorité des adultes américains s'informent par le biais des sociétés Facebook et Google devenant les gardiennes non officielles de l'information aux États-Unis et dans de nombreux pays du monde. Comme toute révolution numérique, et après un certain temps, le législateur a tenté d'encadrer les activités de l'Internet, mais cette nouvelle ère numérique bouscule l'ordre juridique jusqu'alors institué « *l'Internet a marqué le début d'un nouveau paradigme pour la réglementation - un paradigme où la réglementation serait appliquée par le biais de la règle du code* (...). *Les gouvernements ont étendu leur contrôle en exigeant que les intermédiaires modifient leur code pour maintenir et respecter les lois de leur juridiction* »[173]. En complément du fait qu'Internet est né sans système d'identification natif pour les personnes, c'est-à-dire avec un chainon [technologique] manquant[174], il subit également une crise de son identité. En effet, il s'est écarté de l'utopie initialement imaginée par le World Wide Web en tant qu'espace de liberté inédit permettant aux utilisateurs de partager des informations sans frontière, sans surveillance, et sans censure. Cette concentration technologique, dont l'innovation est aujourd'hui détenue et brevetée par une minorité

[169] Traduction libre de l'anglais : « une véritable transformation numérique doit partir du fait que les citoyens et les entreprises européens ont confiance dans la sécurité de leurs applications et de leurs produits. Plus nous sommes interconnectés, plus nous sommes vulnérables aux cyber activités malveillantes. (...) Se sentir en sécurité n'est pas seulement une question de cyber sécurité. Les citoyens doivent pouvoir faire confiance à la technologie elle-même », Communication Shaping Europe Digital Future, in *EU-Lex*, consulté en ligne le 6 décembre 2021, p.4.
[170] Des algorithmes de plus en plus performants déterminent aujourd'hui quelles sont les images, les vidéos, les musiques, les messages ou les lectures que nous consommons.
[171] RTBF info, « Des algorithmes plus transparents : l'UE va les réclamer à Facebook et Google », publié le 30 octobre 2020, consulté en ligne le 27 juillet 2021.
[172] « 10 facts about Americans and Facebook 2021 », in *Pew research Center*, consulté en ligne le 27 juillet 2021.
[173] De FILIPPI Primavera, *op. cit*. Emplacement 4028 sur 7004.
[174] CAMERON Kim, « The laws of identity on the Blockchain », in *Keynote at the European Identity & Cloud Conference* 2018, accessible en ligne

d'entreprises en situation d'oligopole, s'opère au détriment des internautes et d'un Internet libre, qui n'est en réalité plus que l'ombre de sa philosophie et conception initiale. Ces grandes entreprises technologiques fondent progressivement une forme de monopole numérique, c'est-à-dire un système technico-politique en mutation technologique permanente dont elles seules peuvent maîtriser le fonctionnement. Pour illustrer ce propos au sein du Web 2.0, il n'existe qu'un objet numérique qu'un internaute peut informatiquement posséder et détenir sur Internet, un nom de domaine[175]. Mais avec le Web 3.0, les internautes peuvent en théorie s'approprier des facettes entières d'Internet pour y affirmer leurs droits en ligne et également de nouveaux comportements ou possessions numériques (jetons numériques de type « NFT »)[176] qui sont évoqués plus loin dans cette étude. Il est aujourd'hui nécessaire qu'émerge un Internet plus juste, plus respectueux des internautes dont ils devraient avoir le contrôle. L'émergence d'un Web 3.0, décentralisé puisqu'adossé à des technologies blockchains et des identités numériques décentralisées, semble aujourd'hui s'aligner avec les valeurs originelles des pères fondateurs d'Internet.

2.2 Définir l'identité numérique

Le terme d'identité numérique est souvent complexe à définir. Pour renvoyer à une réalité compréhensible, il est possible de la rattacher systématiquement à son origine : l'identité physique. L'identité numérique serait ainsi un « *processus qui permet de transcrire des éléments d'identité sur support numérique, lequel permet de remonter à l'identité juridique* »[177]. Génériquement, l'identité numérique peut être définie comme toutes les formes de présence et de traces qu'un internaute génère lors de sa navigation en ligne. Selon cette définition, l'identité numérique représente un prolongement de l'identité civile et sociale d'une personne au sein de l'espace numérique. Une identité numérique ne serait alors qu'une multitude de copies en ligne d'une même identité administrative, physique. La nature sans frontière et instantanée de l'environnement numérique permet aux personnes d'exprimer d'une nouvelle façon leur dimension psychologique et sociale, bien loin de l'identité sous sa forme traditionnelle et régalienne. Ainsi, il semble que les citoyens bénéficient progressivement d'une

[175] Chaque nom de domaine est unique et ne peut pas être dupliqué. Si des sites internet peuvent être dupliqués, cela n'est pas possible pour les noms de domaine, ce qui introduit et représente historiquement sur Internet une première notion de propriété et de rareté numérique (les bitcoins étant le second).

[176] V. Parties suivantes. En théorie, ce droit de propriété sur des éléments numériques est possible en raison de certaines applications technologiques telles que les « Non Fungible Tokens - NFT » ou « Tokens non fongibles » qui génèrent un titre de propriété unique et non duplicable du fait de sa traçabilité sur une blockchain publique. Si certains juristes affirment que les NFT ne sont que pure spéculation ou arnaque, il convient de ne pas oublier qu'au sein du Web 2.0 de nombreux internautes publient leurs œuvres intellectuelles au monde entier moyennant une forme de reconnaissance sociale numérique, c'est-à-dire du soutien par des likes, partage, etc. Ainsi, il est indéniable que les NFT ouvrent de nouvelles possibilités pour les internautes tant en matière de propriété que de patrimonialisation digitale. La Haute Cour du Royaume-Uni a statué au profit des NFT considérés comme des biens et que les victimes de vols de NFT peuvent agir aux fins de demander le gel de leurs actifs volés par décision judiciaire. GEE Kate, MARSHALL Alasdair, « NFT's recognized as property », 20 avril 2022. Consulté le 2 mai 2022, à l'adresse suivante

[177] COUTOR Sophie, FAHER Mourad, HENNEBERT Christine, Rapport du Ministère de l'Intérieur, octobre 2020 v.1.0, « Blockchain et identification numérique, BCID, restitution des ateliers du groupe de travail du 8 juillet 2020 sur l'identité numérique », consulté en ligne le 9 août 2021, p.31.

redécouverte dynamique et en ligne de leur identité initialement statique et physique. Il s'agit de déterminer le périmètre de l'identité numérique au regard de ses usages sociaux et technologiques actuels et à venir. Si en ligne une personne est d'abord représentée par des identifiants, c'est-à-dire par sa navigation et parfois ses habitudes numériques, il semble qu'une identité légale n'est pas systématiquement requise pour accéder à certains services numériques[178]. La littérature scientifique définit principalement l'identité numérique sous ses aspects pratiques à travers des éléments informatiques appartenant au Web 2.0 ou Web 3.0. Dans son ouvrage Ego 2.0[179], Pascal Lardellier, Professeur en sciences de l'information et de la communication, consacre l'identité numérique comme un rapport aux autres. Il met en avant le développement de l'ego avec le 2.0, qui forme un « *je expressif numérique* ». Cet Ego 2.0 se développerait ainsi au sein des réseaux sociaux numériques avec la possibilité de s'exprimer et de se mettre en avant dans la sphère numérique et sociale. De son côté, Dominique Cardon[180], Professeur de sociologie, estime que l'identité numérique est « *moins un dévoilement qu'une projection de soi* ». Plus en aval de la chaîne de l'identité, Fanny Georges, sémiologue, Maître de conférences en sciences de l'information et de la communication à l'Université Sorbonne Nouvelle, considère que « *l'identité devient mixte, elle se compose d'informations acquises en face à face et dans les sites sociaux* »[181]. Au cœur de la culture d'Internet, l'identité numérique était historiquement synonyme de distanciation et d'anonymat entre l'identité civile de la personne et leur avatar en ligne soit un alter ego numérique. Internet permettait à l'individu de se bâtir différentes facettes identitaires en se soustrayant à la détermination corporelle. L'identité numérique est ainsi devenue une nouvelle forme d'expression de soi, de façon pseudonyme ou bien assumée. Les portraits complémentaires, mais nécessairement non exhaustifs, qu'évoquent ces auteurs sont aujourd'hui plus que jamais d'actualité, car l'identité numérique mixte, objective et subjective, est nécessairement celle qui naît des interactions avec les systèmes d'information. Dès lors, il est possible de distinguer deux catégories principales d'identité numérique, rattachées aux premières définitions de l'identité :

(i) L'identité numérique *racine* ou *primaire* qui représente le prolongement de notre identité physique et légale au sein de l'univers virtuel. Cette première catégorie comprend l'identité civile d'une personne qu'elle présente en ligne pour prouver en ligne qu'elle est bien qui elle prétend être. Ainsi, l'identité numérique racine représente simplement une extension de l'identité juridique fondée sur les titres d'identité et de l'identité subjective fondée sur des pseudonymes,

[178] SENAT, Rapport n° 432 (2010-2011), déposé le 13 avril 2011, Proposition de loi relative à la protection de l'identité, 1er juin 2022, « La plus grande part des transactions effectuées en ligne ne requièrent pas l'identification précise de l'acheteur : le paiement suffit », disponible à l'adresse suivante. Cette proposition a été adoptée le 27 mars 2012 par la loi n° 2012-410, disponible en ligne

[179] LARDELLIER Pascal, BRYON-PORTET Céline, « 2.0, quelques considérations théoriques sur l'identité et les relations à l'ère des réseaux », in *Les cahiers du numérique*, 2010, Vol. 6, consulté en ligne le 15 septembre 2021, p. 13.

[180] CARDON Dominique, "L'identité comme stratégie relationnelle", in *Hermès*, revue 2009, n° 53 consulté en ligne le 15 septembre 2021.

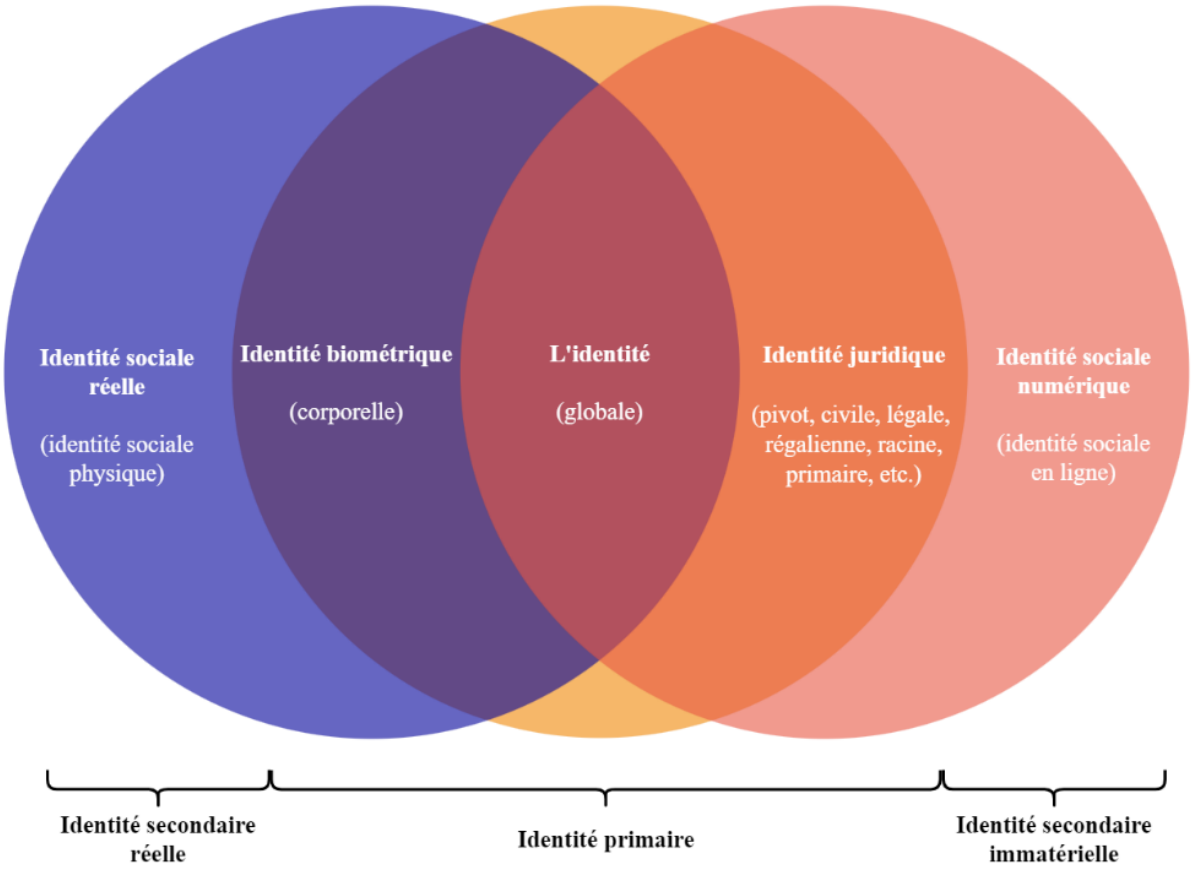
[181] GEORGES Fanny, « Représentation de soi et identité numérique : une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 » in *Réseaux*, 2009, n°154, consulté en ligne le 15 septembre 2021, *v.* également « Eternités numériques : la communauté numérique et la mort », 2020, pp.69-88.

adresses électroniques, et numéros de téléphone d'un individu lorsqu'il navigue sur les services en ligne. Cette identité primaire projetée dans le numérique n'est généralement utilisée que pour certains actes administratifs ou bien juridiques précis et répétitifs afin d'identifier avec fiabilité les internautes lors de l'accès à un service public en ligne via FranceConnect par exemple[182]. En principe, l'identité civile des personnes est stable, c'est-à-dire qu'elle demeure juridiquement inchangée selon qu'elle soit attestée via un support physique, papier, plastique, ou bien électronique avec un identifiant et un mot de passe. La majorité des interactions numériques d'un internaute provient d'un second type d'identité numérique, étendue et prolongée de la première.

(ii) L'identité numérique *étendue* ou *secondaire*. Celle-ci considère toutes les traces d'identité numérique secondaires qu'un internaute génère sur les services en ligne. Cette seconde catégorie comprend nos pseudos et profils de réseaux sociaux, nos avatars de jeux vidéo ainsi que d'autres comptes en ligne de nature commerciale (Amazon, Pinterest, Leboncoin) et interactive (messagerie Signal, Telegram). Ces traces étendues d'identité virtuelle sont le fait de l'internaute, qui décide de la création de ses comptes ainsi que du choix de ses pseudos ou quasi-noms. Une certaine liberté d'utilisation et de gestion est ainsi possible en raison d'un pseudo-anonymat, en relative opposition avec l'identité numérique racine fixée par le droit comme précédemment évoqué. En cas de problèmes liés à cette identité secondaire, il semble que seule la preuve de l'identité primaire puisse permettre d'identifier la personne dont il s'agit (cas de perte des accès ou usurpation d'identité). Toutefois, il existe des exceptions, encore marginales, au sein de l'univers numérique dans lequel une identité secondaire peut être créée sans tiers de confiance en se substituant à une identité primaire, ce qui est le cas du Métavers et de l'identité auto-souveraine (INAS) qui sont étudiés dans de prochaines parties.

[182] *FranceConnect* est une solution d'identification et d'authentification en ligne proposée par l'État pour sécuriser et simplifier la connexion à plus de 900 services numériques à ce jour (2022).

Pour résumer ces propos et enrichir le concept d'identité en iceberg introduit précédemment, il est possible de résumer les facettes qui coexistent pour chaque identité globale en une série de plusieurs cercles concentriques :



Nombreux sont les auteurs et experts qui perçoivent Internet comme un simple prolongement virtuel de l'univers réel, tandis que d'autres le conçoivent surtout comme un espace de liberté sans frontière au sein duquel le pseudo-anonymat (étudié plus loin) est érigé comme un droit fondamental. Si les catégories illustrées sont purement indicatives, elles reflètent tout de même deux visions complémentaires ou bien différentes selon les perceptions de chacun. A la lumière de ces deux positionnements en apparence, il semble que plus les technologies étudiées s'imbriquent, plus l'identité secondaire des personnes tente de se libérer de l'identité primaire attribuée par l'Etat. Nous suggérons que cette volonté de libéralisation de l'identité numérique est nécessaire, pouvant peut-être apparaître utopique pour certains internautes. Aujourd'hui, l'identité numérique d'un adolescent naît bien avant sa capacité juridique[183]. Cet écart temporel entre les comportements numériques en principe impossible pour un jeune adolescent est particulièrement significatif sur les réseaux sociaux au sein desquels ils sont par nature moins avertis et plus influençables que des personnes majeures. A ce titre, l'identité numérique décentralisée peut contribuer à réduire cet écart entre la responsabilité juridique et ces

[183] Pour illustration, de nombreux adolescents créent leurs premières traces numériques sur des réseaux sociaux dès l'âge de 13 ou 14 ans en y produisant des effets juridiques (achat et vente de jeux vidéo, revendications identitaires, etc.) tandis que leur capacité juridique n'existe en principe qu'à leur majorité.

pratiques socio-numériques perturbant l'efficacité des règles de droit[184]. Lorsqu'un internaute navigue sur Internet, les deux catégories d'identités numériques précitées sont utilisées de façon complémentaire et plus ou moins exclusive l'une de l'autre, selon les finalités des services dont bénéficie l'utilisateur. En termes d'usage, les identités numériques primaires et secondaires ont pour vocation d'authentifier les utilisateurs souhaitant accéder à des services en ligne. Toutefois, l'identité numérique secondaire possède une dimension supplémentaire, celle d'une liberté de choix concernant la présence en ligne que souhaite endosser un internaute. Le concept d'identité numérique suscite de multiples questionnements relatifs aux systèmes de gestion, d'identification et d'authentification des identités des personnes en ligne : pourquoi l'identité numérique n'est-elle pas unique et universelle ? Pourquoi un individu ne peut-il pas, aussi simplement que dans l'univers physique, être reconnu de son alter ego numérique ? Quel niveau de transparence et de confiance existe-t-il en ligne pour les internautes ? Comment garantir l'authenticité de leurs identités et l'application de leurs droits fondamentaux en ligne ? L'État possède-t-il la capacité de se positionner comme un fournisseur d'identité numérique ? L'intervention du secteur privé est-elle possible pour dématérialiser nos identités et par quel cadre de protection pour les données personnelles ?

Pour certains spécialistes, il s'opère au sein de la sphère numérique un double catalyseur qui conforte la conceptualisation d'une identité numérique primaire et secondaire, comme le rappelle le chercheur français en sciences de la communication et de l'information Olivier Ertzscheid « *en amont il contribue à alimenter le grand réservoir de l'identité globale ; en aval il offre de nombreuses occasions nouvelles de puiser dans le réservoir de données disponibles pour forger des identités contextuelles* »[185]. Parce que l'univers physique et virtuel fusionnent progressivement, cette relation d'interdépendance en amont et en aval entre l'identité et son évolution dans l'espace numérique, redéfinit le sens traditionnellement porté à l'identité et tend vers une nouvelle forme d'identité, l'identité *phygitale,* déjà évoquée. Une identité numérique, qu'elle soit imputée à une personne morale, physique ou même à un objet numérique, implique nécessairement selon l'avocat Alain Bensoussan la réunion de trois éléments, une constatation par un tiers de la naissance, création d'une entité singulière, une attribution d'un ou plusieurs identifiants uniques et un enregistrement de ces derniers au sein d'un registre numérique centralisé ou décentralisé selon les cas. Ces trois éléments permettent de caractériser simplement et de façon impersonnelle si une identité numérique est caractérisée ou non. Mais il est souligné que l'enregistrement se fait avec un mot de passe, un code secret unique, enregistré de façon chiffrée par les services en ligne et trop souvent réutilisé, donc partagés entre divers services en ligne[186], ce qui accroît

[184] ADAM Louis, « accès des mineurs aux sites pornographiques : qu'est-ce que la vérification d'âge en 'double anonymat' », Publiée le 17 février 2023, in *Le Monde*, en ligne à l'adresse suivante

[185] ERTZSCHEID Olivier, « Genèse : qu'est-ce que l'identité numérique ? », Ed. *Open Press*, chap. 1, consulté en ligne le 9 août 2021.

[186] Il s'agit donc d'un secret qui est, certes chiffré, mais aussi largement partagé de multiples fois lorsque des internautes utilisent les mêmes mots de passe pour des services en ligne pourtant différents (ce qui augmente le risque de révéler ce secret en cas de failles chez un de ces services en ligne qui le détient). Notons que les mots de passe sont en théorie systématiquement

le risque d'usurpation d'identité ou de violation des données. Le processus d'élaboration d'une identité numérique est en réalité un processus particulièrement social et itératif. C'est ce que souligne le sociologue français Dominique Cardon dans son Essai « *Le design de la visibilité* ». Ce dernier identifie trois éléments de ce processus[187] : l'internaute fragmente puis déploie différents segments de son identité numérique selon les services en ligne qu'il utilise, une identité en ligne ne peut se construire qu'en interaction avec des processus de dénigrement et de reconnaissance sociale, et la perception d'une identité numérique influence par extension l'identité primaire d'une personne (autrement dit la vie sociale d'une personne est régulièrement impactée par les interactions avec son identité numérique). Bien qu'une recherche de singularisation et d'unicité représente l'une des principales motivations des internautes, il convient de dire que certaines de ses facettes restent largement soumises aux normes sociales et collectives telles que le mimétisme ou encore la recherche de sensationnalisme (Ego 2.0).

Depuis l'essor du Web 2.0 et la multiplication des services en ligne, il est apparu indispensable au législateur européen d'organiser un corpus législatif pour encadrer les services numériques et assurer la protection des citoyens européens. Ainsi, l'Europe s'est dotée de Règlements, avec le Règlement eIDAS[188] sur l'identification électronique, l'authentification et les services de confiance en ligne et le Règlement général sur la protection des données RGPD[189] qui sont étudiés au titre deuxième de cette recherche ainsi que dans la deuxième partie. Dès 2005, c'est-à-dire avant les premières lois de protection sur les données personnelles en Europe, les règles PIPL[190] en Chine où celles CCPA[191] aux Etats-Unis (Californie), l'architecte et ingénieur sur l'identité numérique chez Microsoft Kim Cameron, publiait les « *sept lois de l'identité* »[192]. Il existe probablement une corrélation inédite entre ces sept principes et les fondements des lois sur la protection des données, dont le législateur européen s'est inspiré. Avant d'identifier la qualification juridique de la notion d'identité numérique en droit communautaire, il convient de distinguer deux terminologies suggérées par des juristes spécialisés[193], les données d'identification personnelle versus les données à caractère personnel. En effet, il existe de nombreux flux de données et autant de catégories juridiques associées pour en rendre compte. Les données

chiffrés au sein des bases de données des services en ligne, mais de nombreux manquements à ce principe demeurent ce qui signifie que des mots de passe sont encore régulièrement stockés tels quels dans des bases de données non chiffrées.

[187] CARDON Dominique, « Le design de la visibilité », in *Réseaux*, n° 152, 2008, consulté en ligne le 15 septembre 2021, pp.93-137.

[188] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, disponible à l'adresse suivante

[189] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE, disponible à l'adresse suivante

[190] Loi Personal Information Protection Law (PIPL) en Chine, équivalent du RGPD européen, entrée en vigueur le 1er novembre 2021.

[191] Loi California Consumer Privacy Act (CCPA) entrée en vigueur en Californie le 1er janvier 2020, inspirée mais assez loin des exigences du RGPD.

[192] CAMERON Kim, « The Laws of Identity », « Contrôle et consentement de l'utilisateur ; Divulgation minimale pour une utilisation limitée ; Parties légitimes ; Identité dirigée ; Pluralisme des opérateurs et des technologies ; Intégration humaine ; et Expérience cohérente à travers les contextes », in *identityblog.com* le 11 mai 2005, consulté en ligne le 28/10/2021.

[193] EYNARD Jessica et al. « L'identité numérique ; quelle définition pour quelle protection ? », Ed. Larcier, 1ère édition 2020.

d'identification personnelle ne représentent pas des données personnelles, car elles ne renvoient qu'à l'identité civile d'une personne, mais aussi parce qu'elles représentent généralement des identifiants techniques et par exemple biométriques. À l'inverse, les données personnelles font appel à une quantité infinie d'informations qui permettent de définir l'identité numérique - civile ou revendiquée - d'un individu. Par conséquent, il convient de distinguer ces deux formes de données afin, d'une part, de ne pas les confondre, et d'autre part de ne pas amalgamer leurs encadrements juridiques respectifs avec le Règlement eIDAS (données d'identification personnelle) et le RGPD (données personnelles), tous deux faisant l'objet d'une étude détaillée dans les chapitres suivants. Nonobstant sa consécration par l'usage, il serait plus juste de substituer le terme d'identité numérique par celui de « *moyens d'identification électronique* ». Certains juristes répondent positivement à cette définition restrictive[194], tout simplement parce que le Règlement eIDAS étudié dans la deuxième partie de cette étude propose une définition précise de l'identification électronique « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* »[195]. De même, l'authentification représente « *un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* ».

Dans un univers numérique où la collecte de données d'utilisateurs est essentielle pour offrir des expériences en ligne de plus en plus immersives et personnalisées, l'application du RGPD de son côté peut sembler plus complexe devant cette réalité commerciale et comportementale en ligne. Cette situation présente à la fois des avantages et des inconvénients. En effet, dans de nombreux cas, l'identité numérique actuelle ne respecte pas certains grands principes du RGPD. A titre d'illustration, il est courant pour les services en ligne de demander à un internaute sa date de naissance pour qu'il confirme sa majorité. À cet égard, il n'y a aucune raison pour cette personne de fournir cette donnée personnelle, car il existe d'autres moyens tout aussi efficace et plus respectueux de sa vie privée de prouver sa majorité[196]. D'autres cas similaires existent, par facilité[197] et parfois par ignorance[198]. Il semble que la

[194] *Ibid*. « (...) comme vous le constatez, je viens pour la première fois d'abandonner l'expression d'identité numérique », *op. cit.*, p.6.
[195] Art. 3.1 du Règlement (UE) n ° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques, *v*. partie dédiée
[196] La preuve de majorité est un sujet particulièrement important, notamment pour les personnes mineures de moins de 13 ans. Selon l'enquête de Génération Numérique, 63% d'entre-elles possédaient au moins un compte sur un réseau social en 2021, enquête disponible en ligne. Mettre en place un processus de vérification minimal et anonyme de preuve de majorité nécessite l'utilisation du *ZKP* (*v*. plus loin) couplé à une identité décentralisée proche d'une identité numérique auto-souveraine (INAS). En effet, protéger les personnes majeures des récoltes massives de leurs âges par des services en ligne est une nécessité à laquelle la solution d'identité fédérée de FranceConnect ne répond pas à l'heure actuelle (2021).
[197] Depuis 60 ans les systèmes de mot de passe sont utilisés alors qu'ils sont peu optimaux pour l'utilisation du Web 2.0. C'est en partie pour cette raison de cybersécurité que les cartes à puce ont été inventées : pour stocker les mots de passe directement au sein de la carte à puce de sorte que lors d'une interrogation de cette dernière, une réponse sans divulgation dudit mot de passe s'opère. En réalité, un code PIN ou un autre mot de passe similaire est parfois requis lors de cette interrogation afin de fournir une sécurité supplémentaire, mais moins contraignante que la simple utilisation d'un mot de passe complexe.
[198] Il existe d'ores et déjà diverses méthodes cryptographiques qui permettent de prouver une information avec certitude sans pour autant en divulguer son contenu ni sa source. Il est notamment fait référence à *la preuve à divulgation nulle de connaissance* ou *Zero-Knowledge Proof (ZKP)* dès 2019 par le Parlement européen.

numérisation de l'identité des personnes multiplie mécaniquement les possibilités d'atteintes aux personnes en multipliant les possibilités d'acteurs malfaisants dans le domaine de l'espionnage commercial, de l'usurpation d'identité ou de tout autre acte malveillant. La définition de l'identité numérique dépend par conséquent de son contexte d'utilisation ainsi que du niveau de confiance requis pour effectuer une interaction en ligne : une relation nécessitant un important niveau de confiance requiert un accès à l'identité primaire de l'internaute, l'État se positionnant comme tiers de confiance. Inversement, une relation dont un niveau de confiance faible ou modéré est suffisant, concerne en principe les attributs secondaires de l'identité numérique. Finalement, l'identité numérique d'une personne devrait à la fois pouvoir être constante dans le temps, pour certains usages indispensables (attributs d'identité primaire), et temporaires pour d'autres usages (attributs d'identité secondaire). Pour cela, nous constaterons que l'identité décentralisée représente un excellent moyen pour que cette identité numérique supposément 'augmentée' puisse permettre à une personne de décliner son identité digitale en autant d'identifiants numériques que nécessaire. Elle permet à ses utilisateurs de désigner chaque personne par la fonction qu'elle exerce au sein de multiples communautés numériques[199], tout en gérant souverainement[200] le cycle de vie propre à chacune de ces personnes et de leurs fonctions. Comme nous l'expliquerons dans les parties suivantes, il convient de ne pas confondre les certificats d'identité numérique 2.0 avec ceux 3.0 propre à l'identité décentralisée. Si les certificats numériques 2.0 sont aujourd'hui à la base de nos identités numériques, leurs multiplications peuvent entraîner une perte de contrôle (par un tiers ou la personne en question) pour l'identité des personnes. À cet effet, des certificats numériques 3.0 (attestations vérifiables) étudiés au titre deuxième de cette étude, permettent précisément de générer puis partager de multiples certificats numériques pour une même personne. L'identité décentralisée fait à ce titre référence à un système dans lequel les individus ou les organisations peuvent avoir le contrôle de leurs propres attributs d'identités numériques, plutôt que de s'appuyer sur une autorité centralisée pour gérer et vérifier leurs identités. Dans ce système d'identité décentralisé, l'identité d'un individu ou d'une organisation est enregistrée dans une base de données plus ou moins décentralisée et sécurisée, à l'aide de la technologie blockchain. Ainsi, chaque identité peut être facilement accessible et vérifiée par d'autres personnes grâce à des moyens cryptographiques.

[199] Ces dernières s'apparentent à des contextes et à des usages divers pour l'identité numérique d'une personne. En d'autres termes, chaque communauté (services en ligne) doit posséder son propre *registre électronique* (qu'il s'agisse d'un serveur centralisé ou bien d'une *blockchain* en principe plus décentralisée). De cette façon, rien ne s'oppose donc à ce qu'une même personne puisse disposer d'une multitude d'identifiants numériques auprès d'une multitude de registres électroniques et de leurs communautés en ligne afférentes.

[200] Selon ce principe « (…) je dois pouvoir garder la possibilité de 'naviguer' ou de 'm'exprimer' dans le monde numérique sans être systématiquement identifié : je reste libre d'utiliser l'identifiant que je souhaite, ou de ne pas en utiliser », *op. cit. L'Identité numérique 5.0*., p.18.

2.2.1 Réseaux sociaux et modèles de gestion des identités numérique (Web 2.0)

Avec l'émergence d'Internet, le besoin d'identification des internautes n'a jamais cessé de croître. Depuis le développement des sites internet puis des réseaux sociaux, en passant par le commerce en ligne jusqu'aux services publics numériques, plusieurs modèles de gestion des identités se sont succédé et forment un Web 2.0 dans la continuité du Web 1.0 évoqué. Il apparaît que ces solutions de gestion des identités numériques sont aujourd'hui coûteuses : l'économie mondiale a dépensé 4,93 milliards USD en 2017 pour la vérification d'identité[201], sans que ce chiffre n'inclue les pertes financières dues à la fraude d'identité, aux obligations et coûts de mise en conformité règlementaire ou encore aux coûts de sécurité informatique. Le coût financier global pour établir une infrastructure d'identification en ligne est considérable. En effet, cela peut entraîner une diminution de la confiance des citoyens et des utilisateurs en ce qui concerne la gestion de leur identité numérique, alors que dans un même temps leurs exigences et leurs besoins en la matière sont en constante évolution. Dès lors, il est possible de distinguer deux principaux courants et modèle d'identité numérique : celui en faveur d'une identité numérique centralisée versus celui en faveur d'une identité décentralisée. Dans les deux cas de figure, la fourniture et l'accès sont déclinables en plusieurs variantes conceptuelles et technologiques que cette recherche étudie dans les parties suivantes. Trois schémas génériques et sous-jacents à toute identité numérique peuvent être identifiés : le modèle d'identité numérique en silo[202], l'identité numérique fédérée[203] et enfin un modèle d'identité numérique centrée sur l'utilisateur[204]. Avant d'aborder plus en détails les différences et complémentarités techniques de ces modèles, il est essentiel de proposer une définition de deux acteurs indispensables sur le marché de l'identité numérique : le fournisseur d'identité[205] et le fournisseur de services[206]. Un fournisseur d'identité est une organisation, à l'instar de la société française IN Groupe[207], qui met à disposition des informations d'identité à destination d'utilisateurs ou de services en ligne. En d'autres termes, il prend en charge la création d'informations d'identité ainsi que la maintenance et la gestion des informations d'identification pour le compte de personnes physiques ou morales. Pour cela, il fournit des services d'authentification aux fournisseurs de services ou aux applications informatiques des parties prenantes. Un fournisseur de services ou prestataire de services représente une entité qui fournit un ou plusieurs services en ligne à des personnes physiques (site internet, réseaux sociaux). Certains fournisseurs de services sont également des fournisseurs d'identité (par exemple lorsque la création d'un compte utilisateur puis l'accès à un service en ligne sont opérés par la même entité). Par souci de simplicité, ils sont désignés de façon générique, en partant du principe

[201] « Global identity verification market size 2017-2027 », traduit de l'anglais, « De 2017 à 2027, les dépenses mondiales sur le marché de la vérification d'identité devraient augmenter de plus de 13 milliards de dollars, passant de 4,93 milliards en 2017 à plus de 18 milliards en 2027 », Statista en ligne, consulté le 18 juillet 2021.
[202] Librement traduit de l'anglais « *Siloed identity* ».
[203] Librement traduit de l'anglais « *Federated identity* ».
[204] Librement traduit de l'anglais « *User centric identity* ».
[205] Librement traduit de l'anglais « *Identity Provider* ».
[206] Librement traduit de l'anglais « *Service Provider* ».
[207] IN Groupe, « Le Droit d'être soi, l'identité est un droit fondamental, IN Groupe contribue à le faire savoir », consultez le site internet à l'adresse suivante

que si le fournisseur de services est également un fournisseur d'identité, ladite entité sera globalement qualifiée de fournisseur d'identité. Avant l'avènement des réseaux sociaux numériques, les réseaux sociaux n'étaient que physiques, c'est-à-dire représentés par de nombreux lieux de convivialité comme des restaurants ou bistrots de quartiers. La révolution des réseaux numériques réside dans le fait qu'ils transposent et reconnectent en ligne la diversité de ces écosystèmes, initialement physiques et indépendants. Ce rapprochement entre écosystèmes physiques et réseaux sociaux numériques a mis en exergue un fossé entre eux. Si revendiquer en ligne les segments de son identité et de sa diversité semble être un réel progrès pour la société, l'enfermement dans une bulle de recommandations algorithmiques ou l'utilisation à mauvais escient de l'anonymat reste des dangers invisibles, mais réels pour les internautes (harcèlement, injures, usurpation d'identité). Les chercheurs et auteurs Jean Lassègue et Antoine Garapon expliquent ainsi que « *le numérique, qui procure aux individus des possibilités qui semblent se renouveler sans cesse, pourrait également se refermer sur eux comme un piège* »[208]. Ainsi, ce qu'a écrit Pierre Bellanger en 2004 semble prendre tout son sens : « *il faut reconquérir notre souveraineté sur les réseaux et systèmes informatiques, y retrouver la maîtrise de notre destin. Telle est la souveraineté numérique* »[209].

2.2.1.1 L'impact des réseaux sociaux sur notre construction identitaire

Les réseaux sociaux sont devenus des espaces presque indispensables pour travailler, pour exprimer sa personnalité, pour se rencontrer, s'informer et apprendre. La liste de ces usages s'étend chaque année un peu plus et ces nouveaux espaces numériques modifient d'ores et déjà nos comportements physiques. L'apparition des réseaux sociaux a précipité l'avènement d'une nouvelle discipline scientifique, la « *captologie* » ou la science de capter notre attention[210]. Cette quasi-science fonctionne avec des algorithmes d'intelligence artificielle (IA) axés sur le ciblage comportemental des utilisateurs. Plus un utilisateur interagit avec ces algorithmes, plus ces derniers peuvent lui proposer des contenus qui le feront réagir, captivant ainsi son attention le plus longtemps possible sur ces services numériques. Cette course au capitalisme de l'attention où chaque utilisateur est progressivement réduit à son temps de cerveau disponible n'est pas sans conséquences pour l'identité subjective et secondaire des personnes. Dans un avenir proche, chaque réseau social permettra à ses utilisateurs la création ou l'implémentation d'avatars numériques, un pas de plus vers le concept de Métavers ou d'un État autoproclamé (v. Liberland[211]) qui sont évoqués plus loin dans cette étude. Dès lors, les réseaux sociaux numériques

[208] LASSEGUE Jean, GARAPON Antoine, « Justice digitale », in *PUF*, p.339.
[209] BELLANGER Pierre, « La souveraineté numérique », Ed. *Stock*, 2014.
[210] OSTOJIC Andréa, « La captologie ou l'influence par la technologie », 2017, in *Sciences Humaines*, consulté le 22 septembre 2022, à l'adresse suivante
[211] V. Annexe 4.

caractérisent-ils une forme de nouvel ordre mondial au sein duquel chaque internaute met plus ou moins fictivement et publiquement en scène son comportement et sa vie personnelle ?

En 2022, un internaute visite en moyenne sept réseaux sociaux chaque mois selon une étude[212], et en 2021 un sondage estime à douze heures le temps d'écran quotidien des Français sur les réseaux[213]. Si ces quelques chiffres sont à nuancer face à la justification du caractère professionnel d'une multitude d'activités en ligne, il n'en demeure pas moins que les réseaux sociaux impactent psychologiquement et socialement la construction identitaire des personnes. Dès 2016, une étude affirme que l'utilisation des réseaux sociaux réduit collectivement la capacité d'attention et peut atteindre la santé mentale[214]. En mai 2017, la Royal Society for Public Health et le Young Health Movement ont publié un rapport examinant les effets positifs et négatifs des réseaux sociaux sur la santé des jeunes. S'ils s'avèrent utiles pour faire société en favorisant la liberté d'expression et la liberté d'information, ils sont paradoxalement « (…) *décrits comme créant une plus grande dépendance que les cigarettes et l'alcool (...) Les taux d'anxiété et de dépression chez les jeunes ont augmenté de 70 % au cours des 25 dernières années.* »[215]. Selon deux autres études publiées en 2019[216] et en 2020[217], plus un(e) adolescent(e) passe d'heures par jour sur les réseaux sociaux, plus il/elle risque d'être déprimé(e) et de perdre confiance en lui/elle. Progressivement, il est constaté que ces tendances semblent se confirmer. Par conséquent, si le « moi profond »[218] est systématiquement impacté par les algorithmes, serait-ce donc l'objectif ultime de ces applications ? C'est certainement le cas dans une perspective commerciale afin d'éviter de prendre le risque de voir fuir les internautes vers d'autres services en ligne. Ainsi, la réponse à la question « *les algorithmes font-ils notre identité ?* » posée par l'auteure Aurélie Jean consisterait à dire qu'ils y contribuent un peu plus chaque jour. Pour les jeunes générations qui représentent une part importante des utilisateurs des réseaux sociaux, il semble que ces derniers aient un effet proportionnellement plus important sur leur construction identitaire que des adultes. Si notre identité vécue est comme nous l'avons constaté dépendante du mimétisme social, alors les réseaux sociaux exacerbent cet effet sur notre identité (physique puis numérique). À cet égard, les réseaux sociaux encouragent la démonstration d'une identité vécue biaisée, voire fausse, un phénomène qui entraîne un mimétisme identitaire des autres utilisateurs qui cherchent à se comporter de façon identique, ce qui engendre un mécanisme de copie sociale aux effets parfois dévastateurs et plus ou moins visibles (addiction aux réseaux sociaux,

[212] Facebook, Instagram, WhatsApp, YouTube, LinkedIn, Twitter, TikTok, in *Hootsuite Inc*. Consulté le 21 septembre 2022, à l'adresse suivante
[213] ASNAV, « L'ensemble de la population estime à plus de 12 h 00 le temps quotidien passé majoritairement sur l'ordinateur et la télévision », « Le 16ème baromètre de la santé visuelle démontre un fort impact des confinements sur la vue des Français », cmavue.org. Disponible à l'adresse suivante, p.1.
[214] HAYLES Katherine, « Lire et penser en milieux numériques : Attention, Récits, Technogenèse », Ed. UGA, 2016, consulté à l'adresse suivante
[215] Royal Society for Public Health. (2017). StatusofMind. rsph.org.uk. Consulté le 13 avril 2021, à l'adresse suivante, p. 3.
[216] JAMA P. BOERS E, AFZALI MH, Newton N, CONROD P. « Association of Screen Time and Depression in Adolescence », 2019, disponible à l'adresse suivante
[217] TWENGE, J.M., FARLEY, E. « Not all screen time is created equal: associations with mental health vary by activity and gender. Soc Psychiatry Psychiatr Epidemiol », 2021, disponible à l'adresse suivante
[218] ZWEIG Stefan, « Sigmund Freud, la guérison par l'esprit ». Livre de Poche, 2010, 160p.

harcèlement en ligne, etc.). Dans ces écosystèmes numériques et sociaux, la représentation du bonheur semble encore plus dépendante et biaisée par les autres que dans la vie réelle. L'omniprésence des écrans et ce besoin de lien ou reconnaissance sociale en ligne sursollicitent l'attention et dégradent les capacités cognitives des internautes. Ces effets négatifs altèrent progressivement les bénéfices que les internautes extraient de ces espaces numériques. Les informations se font comme elles se défont et le ciblage algorithmique de nos préférences peut entraîner la surabondance d'informations parfois trop négatives ou positives au point d'impacter l'humeur et les envies des utilisateurs. Les fausses informations circulant sur ces réseaux, ou encore le besoin insatiable de se tenir au courant des dernières nouvelles en temps réel, peuvent mener des adolescent(e)s fragilisé(e)s à être manipulé(e)s voire harcelé(e)s, dans des domaines aussi cruciaux pour notre société, que leurs opinions politiques ou religieuses, et menant parfois à des discours complotistes. En perdant le contrôle de notre attention et de nos capacités cognitives, cela nous écarte du droit d'être nous-mêmes en ligne, parfois sans en comprendre l'urgence et la mesure. Une autre problématique majeure de ces réseaux numériques concerne leur gouvernance. Si en droit la problématique n'est pas tant l'interdiction de récolter des données, qui est en réalité simplement encadrée par le RGPD dans de nombreux cas, des gouvernements peuvent influencer voire contraindre certains réseaux sociaux à faire un usage non légitime de leur plateforme, par exemple à des fins géopolitiques (référence au réseau social TikTok). Utiliser un réseau social dans un État de non-droit s'avère être risqué pour les utilisateurs, en raison des détournements possibles par un gouvernement pour en faire un outil de propagande ou de surveillance de masse, ce qui souligne l'importance du pseudo-anonymat consacré plus loin. En 2022, le Conseil d'Etat[219] a publié 17 recommandations dans une étude dédiée aux enjeux et opportunités des réseaux sociaux appliqués à la puissance publique (institutions, collectivités, ministères). Certaines de ces recommandations opérationnelles sont particulièrement pertinentes, car reposent sur le principe selon lequel l'identité numérique décentralisée (IND) permettrait de mieux contrôler l'usage qu'un utilisateur souhaite faire des réseaux sociaux qu'ils utilisent.

2.2.1.2 L'identité numérique centralisée et en silo

Pour rappel et en complément des propos précédent, le terme d'identité numérique 3.0 fait écho à une évolution vers un Web 3.0, également nommé « *Web social* » ou « *Web sémantique* »[220]. L'utilisation de ce terme provient de l'histoire d'Internet que les parties visent à retracer chronologiquement. En résumé, le Web 1.0 permet une simple lecture de données et d'informations en ligne, le Web 2.0 une lecture et une écriture d'informations et enfin, le Web 3.0 permet une lecture, une écriture et une propriété des données en ligne (ce dernier étant une combinaison du souhait originel de décentralisation

[219] Conseil d'Etat, « Réseaux sociaux : placer l'utilisateur au centre », Evénement du 27 septembre 2022, disponible à l'adresse suivante, p.17.
[220] Wikipedia contributors. « Web sémantique », consulté le 6 juillet 2022, à l'adresse suivante

et de gouvernance par la communauté du Web 1.0 avec les fonctionnalités d'interactions modernes du Web 3.0). Aujourd'hui et demain, le Web sera ainsi un agrégat 1.0, 2.0 et 3.0. Au stade de cette réflexion, les termes « Internet 2.0 » et « technologies 2.0 », et respectivement « Web 3.0 » et « technologies 3.0 » font référence aux technologies, mais aussi aux concepts théoriques correspondants et traités dans cette recherche. L'identité numérique étant au cœur de notre étude, il est essentiel de distinguer ses différents types de fonctionnement informatique pour comprendre l'origine et l'avenir de l'identité en ligne. Tout d'abord, le modèle d'identité numérique en *silo* est à ce jour le modèle de gestion des identités numériques le plus répandu. Il consiste à ce que chaque service numérique consommé serve à la fois de fournisseur d'identité et de fournisseurs de service. En d'autres termes, tous les sites internet auxquels un internaute se connecte avec un nouveau nom d'utilisateur et un nouveau mot de passe créés lors de l'inscription[221], comme pour les réseaux sociaux[222], ainsi que les plateformes de messagerie et tout serveur, font partie de ce modèle d'identité centralisé et en silo. Si au début de l'ère d'Internet une centralisation des données de quelques internautes apparaissait comme une solution simple et efficace, au fur et à mesure de son expansion, cette centralisation des données a progressivement soulevé plusieurs problématiques comme le soulignent certains juristes[223]. En effet, cette identité en ligne centralisée offre une faible marge de manœuvre pour les internautes : la création systématique par l'utilisateur d'un nouvel identifiant attaché à un mot de passe pour accéder à certains services en ligne s'avère un processus souvent long, peu sécurisé et aujourd'hui source de friction pour les internautes[224]. Pourtant, l'identité centralisée demeure un système d'identification et d'authentification majoritairement utilisé par tous types de services en ligne. Pour remédier à l'oubli, aux vols ou à la perte des identifiants des utilisateurs, d'autres modèles d'identité (également centralisés) ont été développés afin de limiter la friction des utilisateurs entre chaque service en ligne.

[221] La société *Dashlane* - spécialisée dans les solutions de gestion des mots de passe - estime que d'ici 2022, un américain moyen possédera environ 300 comptes web différents et presque autant d'identifiants numériques, in *blog.dashlane.com/world-password-day*

[222] Pour illustration, cela est le cas pour la plateforme Youtube qui fournit une plateforme de contenu vidéo (fournisseur d'un service en ligne) tout en demandant à ses utilisateurs une preuve de majorité pour regarder certains contenus jugés sensibles (vérificateur/fournisseur d'identité). Sur Facebook également, une pièce d'identité peut être requise pour poster des contenus à caractère politique.

[223] « Toute centralisation des identifiants [identité numérique] et, pire, des moyens de les exercer pose la question de leur usage abusif (potentiellement sans laisser de traces) en cas de violation de la sécurité informatique », *op. cit. «* L'identité numérique 5.0 », p.30.

[224] Selon le site haveibeenpwned.com près de 11,417,410,545 comptes connus ont été piratés selon plusieurs sources, consulté en ligne le 16 juillet 2021. Les causes de piratage sont généralement provoquées par un manque d'attention des internautes qui (ré)utilisent des mots de passe et/ou identifiants trop peu complexes, mais parfois aussi en raison des hébergeurs de services (serveurs) dont la gestion en matière de cybersécurité est défaillante et entraîne un piratage.

2.2.1.3 L'identité numérique fédérée

Si ce second modèle de gestion des identités numériques est également centralisé sur le plan informatique[225], comme le précédent, une importante différence subsiste dans le fait que le fournisseur d'identité et le fournisseur de services sont deux entités juridiques différentes qui communiquent entre elles. Chaque fois qu'un internaute souhaite accéder au service numérique offert par un fournisseur de services, ce dernier fait appel à son fournisseur d'identité pour authentifier son utilisateur. Afin de simplifier l'accessibilité, l'interopérabilité et la navigation entre les services en ligne pour les utilisateurs, également pour diminuer les risques de piratage, un modèle d'identité numérique fédéré émerge rapidement entre 2003 et 2005. Cette nouvelle méthode d'alliance des connexions d'identité numériques permet à l'utilisateur d'accéder à plusieurs services en ligne grâce à un bouton de connexion (présent sur différents services en ligne, comme ceux indiquant « Connectez-vous avec votre compte Gmail » ou encore « Connectez-vous avec FranceConnect » comme étudié plus loin). Avec ce modèle, plusieurs fournisseurs d'identité établissent des accords entre eux et fonctionnent dans un cadre de confiance technique commun. Cette communication entre le fournisseur d'identité et le fournisseur de service s'effectue par le biais de normes et de protocoles informatiques et organisationnels communs, comme « OpenID »[226], « SAML »[227] ou « OAuth »[228]. Notons que ces protocoles de fédération peuvent être utilisés de façon hybride et complémentaire[229] avec les standards de l'identité numérique décentralisée. Dès lors, si les standards de l'identité décentralisée peuvent fonctionner de façon décentralisée par essence, ils le seront probablement conjointement avec d'autres standards conventionnels et centralisés. Cela signifie que les solutions informatiques utilisées par les utilisateurs finaux seront à la fois centralisées et décentralisées, c'est-à-dire hybrides (un terme utilisé tout au long de cette recherche). Au sein du modèle d'identité numérique fédérée, une organisation peut représenter plusieurs entités, c'est-à-dire qu'elle peut cumuler ou posséder plusieurs rôles en matière de délivrance d'une identité numérique. Ce cadre de confiance peut être encadré par des autorités publiques compétentes, mais aussi privées, c'est-à-dire soumis à des accords contractuels multilatéraux entre plusieurs entités (fournisseurs d'identité, de services, institutions gouvernementales, etc.). Ces standards et ce concept de fournisseurs d'identité tiers et fédérés sont devenus populaires avec l'avènement de certains fournisseurs d'identité et de services de réseaux en ligne tels que Facebook ou Gmail. En pratique, ces standards permettent aux utilisateurs, au lieu de se connecter à un site internet avec un nom d'utilisateur et un mot de passe créés pour ce site, de s'authentifier directement depuis leur compte

[225] Cela signifie que les données sont stockées sur un ou plusieurs serveurs sous le contrôle d'une ou de quelques entités.
[226] OpenID est un standard ouvert et un protocole d'authentification décentralisé promu par la fondation à but non lucratif OpenID Foundation. Consulté le 23 septembre 2022 à l'adresse suivante
[227] Security Assertion Markup Language (SAML) est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre des parties (fournisseurs d'identité et de services en ligne).
[228] Open Authorization (OpAuth) est une norme ouverte de délégation d'accès couramment utilisée comme moyen pour les internautes d'accorder à des sites web ou à des applications l'accès à leurs informations sur d'autres sites web, mais sans leur donner les mots de passe. Consulté le 23 septembre 2022 à l'adresse suivante
[229] Nous considérons tout au long de cette thèse que le terme *d'identité numérique hybride* fait référence à une identité numérique 2.0 et/ou 3.0 systématiquement dérivée d'une identité physique matérialisée par un titre d'identité civile et légale.

Facebook ou Gmail. Cependant, cette méthode repose sur une récupération en cascades des données des utilisateurs, ce qui peut mettre en péril leur vie privée dès lors qu'il existe un manque de transparence concernant cette gestion des données par les fournisseurs de services en ligne (ce qui est souvent le cas). Dans ce modèle, les informations numériques des utilisateurs sont réparties entre plusieurs fournisseurs d'identité au lieu d'être centralisées dans un seul. Cette organisation de fournisseurs d'identité est généralement appelée une fédération, car ses acteurs partagent en principe un identifiant unique pour chaque utilisateur. En résumé, lorsqu'un internaute accède à un compte Facebook ou Gmail par ses identifiants, il utilise un modèle d'identité numérique centralisé et en silo. Lorsqu'ils accèdent à d'autres services avec des informations d'identification issues de ces plateformes 2.0, il s'agit d'un modèle fédéré. Dans ces deux cas, les informations et les données des utilisateurs sont centralisées par le(s) fournisseur(s) d'identité. Finalement, l'approche d'une fédération des identités numériques demeure limitée aux entreprises qui participent et adhèrent à une telle alliance des connexions entre diverses identités numériques et services en ligne parfois concurrents. De plus, ce modèle ne propose pas systématiquement de réponse informatique concrète aux besoins de transparence et de traçabilité concernant l'utilisation des données des utilisateurs, ce qui représente ainsi un défi de taille à résoudre pour susciter une confiance numérique.

2.2.1.4 L'identité numérique centrée sur l'utilisateur

Pour répondre aux limites de fédération systématique de ces identités numériques 2.0 par des acteurs également concurrents (Google, Microsoft), une solution d'offres de connexions centrées sur l'utilisateur également appelée « identité prête à l'emploi » est apparue. Il s'agit d'une offre de connexion proposée par un fournisseur de service afin de s'enregistrer et de s'authentifier auprès d'autres services en ligne (également grâce à un bouton de connexion). Ce modèle est ainsi un mixte entre l'identité en silo et l'identité fédérée et réunit leurs avantages grâce au principe d'un mot de passe unique pour accéder à plusieurs services tout en offrant une nouvelle souveraineté technique compte tenu de son fonctionnement. Ce modèle implique toutefois qu'un utilisateur stocke directement dans son appareil personnel ses informations d'identification délivrées en amont par un ou plusieurs fournisseurs d'identité comme évoqué. Ainsi, l'utilisateur possède le contrôle de ses données sur son propre appareil numérique à la différence des modèles précédents. Il peut s'agir de n'importe quel matériel ou périphérique informatique, avec ou sans clavier et écran, qui nécessitent une authentification, tel qu'un code PIN. Étant donné le niveau actuel d'adoption et de sophistication des téléphones mobiles, ces derniers constituent un support particulièrement approprié pour ce modèle de gestion d'identité, qui dans ses versions plus décentralisées donne naissance à une identité numérique décentralisée (IND) ou auto-souveraine (INAS), deux notions étudiées plus loin (émission et stockage cryptographique des données d'identité directement sur le téléphone mobile des utilisateurs). En théorie, ce modèle repose sur une

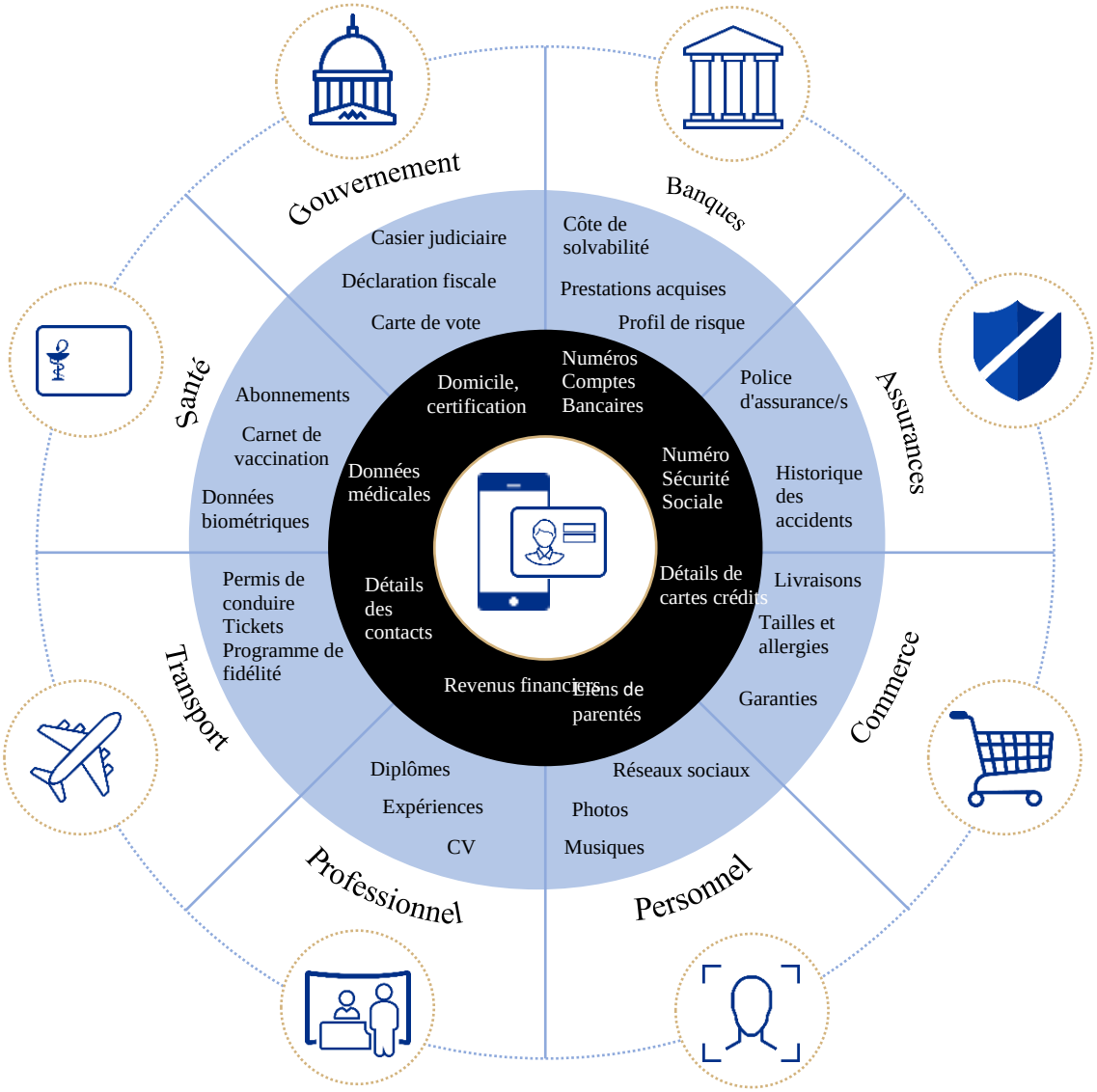
maîtrise technique de l'utilisateur sur ses données d'identité, une modalité en accord avec la volonté de la Commission européenne que les citoyens reprennent le contrôle de leur identité numérique[230]. Dans les faits, ce modèle peut être considéré comme un modèle plus ou moins informatiquement décentralisé dans lequel le fournisseur de services peut s'authentifier à l'aide d'une clé stockée dans son périphérique informatique (en lieu et place d'un nom d'utilisateur et d'un mot de passe stockés sur les serveurs d'un tiers en ligne). Le fait que l'utilisateur ait la capacité de gérer ses données sur ses propres appareils et la possibilité de sélectionner les informations à partager avec les différents fournisseurs de services conduit à considérer ce modèle comme étant l'une des évolutions technologiques et chronologique du modèle d'identité numérique décentralisée qu'il inspire et incube.

2.2.2 Marchés, acteurs et perspectives de l'identité numérique

L'histoire de l'identité remonte aussi loin que l'existence de l'humanité et de son besoin d'identification. En d'autres termes, la nécessité d'identifier les individus est intrinsèque aux activités culturelles et sociales de l'Homme. Avec le numérique naissent certaines asymétries concernant l'exercice de nos droits hors ligne et en ligne, tant l'identité des personnes est profondément transformée comme le confirme une étude récente : « *si l'on considère que l'individu moyen dort environ 7 à 8 heures par jour, l'internaute type passe désormais plus de 40 % de sa vie éveillée en ligne. Le temps que nous passons en ligne continue également de grimper, la moyenne quotidienne ayant augmenté de 4 minutes par jour*

[230] V. parties suivantes.

(+1,0 %) au cours de l'année écoulée »[231]. Pour appréhender de façon holistique la taille du marché de l'identité, de ses divers secteurs et cas métiers[232], nous reprenons ce schéma récapitulatif :



Source : www.pwc.ch/en/insights/fs/digital-identity.html

Dans un environnement numérique omniprésent, les bénéfices d'une identité numérique reconnue et interopérable sont nombreux, à la fois pour les citoyens, les administrations publiques et les États, les fournisseurs (d'attributs) d'identité, ainsi que pour les fournisseurs de services. Rappelons à ce titre qu'un fournisseur d'identité peut aussi fournir des services et devenir de facto fournisseur de services.

(i) Grâce à leurs identités numériques, les citoyens peuvent accéder à des services en ligne transfrontaliers de façon simple, économique, fiable et sécurisée.

[231] KEMP Simon, « Digital 2022 : Global Overview Report », in *DataReportal*, 26 janvier 2022, disponible à l'adresse suivante
[232] Schéma issu du rapport de PriceWaterhouseCoopers (PWC), 2021, « Digital identity - Your key to unlock the digital transformation », consulté le 26 septembre 2022 à l'adresse suivante

(ii) Avec une identité numérique interopérable, des fournisseurs d'identité peuvent accéder à de nouveaux secteurs pour lesquels il existe une forte demande d'identification (santé, transport) en proposant leurs solutions d'identification (biométrie, identité numérique centralisée ou décentralisée). Pour les administrations publiques, la mise en place d'une identité numérique citoyenne permet de simplifier certaines démarches administratives redondantes nécessitant un faible degré de vérification d'identité. A cet égard, il est exploré le concept « *d'État-plateforme* »[233].

(iii) Concernant les fournisseurs de services en ligne, ils peuvent offrir leurs services aux utilisateurs via une identification et une authentification simplifiée issue d'une identité numérique étatique légalement reconnue et de confiance, comme la solution FranceConnect déjà évoquée. Ses avantages incluent une conformité juridique par conception, en particulier en ce qui concerne l'identification des personnes dans le secteur bancaire[234], ainsi qu'une réduction des coûts liés à cette identification.

La position de l'État en tant que fournisseur de confiance pour l'identité numérique est essentielle pour les fournisseurs de services privés en ligne qui utilisent les solutions numériques de l'État. La croissance du marché de l'identité numérique dépend des décisions politiques ou juridiques qui impactent directement ou indirectement l'État et ses institutions. Comme l'estime le McKinsey Global Institute, les enjeux économiques liés à l'identité numérique sont nombreux. Les pays qui mettent en œuvre une politique d'identification numérique pourraient dégager une valeur économique en moyenne équivalente à 3 à 6 % du PIB d'ici à 2030[235]. De même, selon un rapport d'information de l'Assemblée nationale en date du 8 juillet 2020, le marché de l'identité numérique devrait représenter plus d'un milliard d'euros d'ici 2029[236]. En 2021, ce marché regroupe de multiples acteurs publics et privés spécialisés dans la gestion de l'identité des personnes[237] et plus généralement dans la fourniture de services de confiance numérique. Si au sein de l'univers physique l'identité relève historiquement d'une prérogative publique régalienne[238], ce constat s'estompe progressivement face à une nouvelle concurrence technologique[239]

[233] CHEVALLIER Jacques, « Vers l'État-plateforme ? » in *Revue française d'administration publique*, 2018/3 (N°167), pp.627-637, disponible à l'adresse suivante
[234] L'ouverture d'un compte en banque nécessite une identification de la personne titulaire du futur compte en banque : un processus d'identification nommé *Know Your Custommer (KYC)* est ainsi imposé aux banques par les directives européennes anti-blanchiment.
[235] Mc Kinsey Global Institute, « Infographic: What is good digital ID? », 17 avril 2019, disponible à l'adresse suivante
[236] Rapport Assemblée Nationale N°3190, « Rapport d'information du 8 juillet 2020 sur l'identité numérique », consulté en ligne le 9 août 2021, p.39.
[237] Notamment avec l'émission d'identités physiques (carte nationale d'identité, passeports) et/ou numériques (FranceConnect), l'accès à des services en ligne.
[238] Notamment grâce à la délivrance de titres officiels d'identité comme la nouvelle carte nationale d'identité électronique (CNIe) fournie par la société IN Groupe à l'Agence Nationale des Titres Sécurisés (ANTS).
[239] Grâce à une récolte massive des données personnelles de leurs utilisateurs, certains acteurs privés proposent une dérivation de l'identité numérique des personnes, en échange d'un accès simplifié à des services tiers partenaires (commerces en ligne, réseaux sociaux, etc.).

privée matérialisée par de nouvelles solutions d'identification et d'authentification numériques[240] (Apple Wallet, Google sign-in)[241] fédérées, et déployées par certains géants du numérique (GAFAM et BHATX précités). L'objectif de ces nouvelles solutions d'identité numérique privées est de proposer des plateformes toutes incluses pour les fournisseurs de services (depuis l'embarquement numérique du client jusqu'à son authentification et la mise en place de publicités ciblées). Lors de la crise de la COVID-19, il y a eu une augmentation significative des levées de fonds pour les entreprises développant des technologies permettant l'identification d'utilisateurs en ligne de l'identité numérique.

Il subsiste un point commun à tous les systèmes actuels et précités de gestion numérique des identités : celui de leur centralisation plus ou moins importante auprès de tiers de confiance. Aujourd'hui, cette notion de confiance numérique - et celle adjacente de souveraineté - peut être renforcée grâce à l'émergence d'une nouvelle méthode de gestion décentralisée de l'identité numérique utilisant une technologie blockchain et de déterminer laquelle des blockchains déjà existantes sur le marché convient le mieux aux besoins des acteurs concernés. En réalité, ces interactions reposent aujourd'hui sur des tiers de confiance (publics ou privés). Les utilisateurs d'Internet sont-ils réellement disposés à reprendre le contrôle de leurs identités numériques ? Selon une récente étude réalisée par la société Accenture, il semble que les personnes accordent naturellement confiance aux institutions publiques dont l'intérêt général représente leur essence : « (…) *(84 %) des personnes interrogées se disent prêtes à partager leurs informations personnelles avec un service gouvernemental en échange d'un service client plus personnalisé* »[242]. Pour autant, l'utilisation de systèmes d'identité numérique décentralisée développés par des sociétés privées, étudiés plus loin, devra faire ses preuves afin d'acquérir une confiance similaire à celle qui est accordée aux institutions publiques. Avant d'introduire l'état du marché européen de l'identité numérique 3.0, une comparaison préliminaire devient pertinente afin d'introduire les apports de cette identité numérique décentralisée par rapport à l'utilisation actuelle d'identités numériques centralisées (2.0) :

[240] Pour rappel, une distinction importante subsiste : *l'identification* n'est pas du fait de l'individu et consiste à ce qu'un service tiers procède à l'enregistrement et à la gestion de son identité numérique ; *l'authentification* est du fait de l'utilisateur qui s'enregistre ou d'identifie afin d'accéder à un service tiers. Toutefois, certains fournisseurs d'identité numérique peuvent fournir conjointement des services d'identification et d'authentification aux internautes. V. Glossaire.

[241] Apple a annoncé en septembre 2021 fournir à certains états américains les permis de conduire et les identifiants civils des citoyens directement depuis son portefeuille numérique 2.0 (Apple Wallet). Le projet avance lentement, car de nouvelles technologies et de nouveaux processus sont ajoutés pour répondre aux différents besoins de ces états. L'échéance de la mise en place de ces « Real ID » est attendue en 2025. « Apple announces first states signed up to adopt driver's licenses and state IDs in Apple Wallet », in *apple.com*, disponible à l'adresse suivante

[242] ACCENTURE, « Citizens Willing to Share Personal Data with Government in Exchange for Enhanced Customer Services Accenture », 24 février 2020, consulté en ligne le 10 juin 2022 à l'adresse suivante

Considérations informatiques et légales	**Identité numérique centralisée (2.0)**	**Identité numérique décentralisée (3.0)**
Identité(s) numérique(s)	• Contrôlée par une ou plusieurs entités souvent avec peu de transparence informatique. • Fragmentation à travers de multiples plateformes et services en ligne. • Techniquement transmissible à un tiers sans obtenir son consentement ou en informer l'intéressé (transparence faible et dépendance totale pour les utilisateurs).	• Partiellement ou entièrement transparent et contrôlée par l'utilisateur. • Portabilité à travers de multiples plateformes et services en ligne. • Techniquement non transmissible à un tiers sans le consentement cryptographique de l'intéressé.
Gestion et sécurité des données	• Utilisation complexe de multiples mots de passe et identifiants. • Les serveurs centralisés de ces services en ligne représentent des cibles préférées (« honeypots ») pour les pirates informatiques (« hackers »). • Vérifiabilité des informations et des données limitées (techniquement chronophage et longue pour les services en ligne).	• Infrastructures blockchains publiques, privées ou hybrides (à clé publique et privée : « PKI »)[243]. • Chiffrement des données de bout en bout et par conception (confidentialité programmée). • Exposition limitée des données en cas d'attaques informatiques grâce à la révocation et à la compartimentation des données (v. « eIDAS-2 »).
Gestion des données à caractère personnel	• Chiffrement partiel et/ou de bout en bout possible bien que non systématique. • Données traçables uniquement par les tiers centralisés de niveaux inégaux de cybersécurité. • Révocation et supression cryptographique des données informatiquement impossible (en raison de leur duplication puis dispersion sur Internet). • Contrôle des données par des tiers plus ou moins de confiance (dépendance technique).	• Attributs supposés portables entre tous les services en ligne (preuves des données vérifiables sur une blockchain ouverte ou fermée). • Centré sur l'utilisateur qui contrôle tout ou partie de ses données grâce à son portefeuille d'identité numérique décentralisée (v. « PIND »). • Suppression possible à tout moment de ses données même après la transmission à un service en ligne.

[243] « Une infrastructure à clé publique (PKI) est un ensemble de rôles, de politiques, de matériel, de logiciels et de procédures nécessaires pour créer, distribuer, utiliser, stocker et révoquer des certificats numériques et gérer le cryptage à clé publique », in *Wikipedia*, consulté en ligne le 22 avril 2021.

		• Divulgation partielle et sélective possible de ses données.

2.2.2.1 L'identité numérique en Europe

Depuis 2014, l'Union européenne a tenté d'harmoniser les services numériques requérant une identité numérique, grâce à l'adoption du Règlement eIDAS déjà évoqué et étudié au deuxième titre de cette étude. Bien que cette stratégie juridique ait eu des avantages, elle a également limité l'innovation et l'adoption massive de solutions d'identité numérique par le secteur privé. Ainsi, seulement de grandes entreprises technologiques ont été capables de concevoir des solutions conformes au Règlement eIDAS et au RGPD, également étudiés plus loin. Les États membres de l'Union européenne ont été contraints, avec le Règlement du Parlement européen et du Conseil du 20 juin 2019[244], de publier des cartes d'identité nationales de nouvelle génération (CNIe), avant le 2 août 2021, sous peine de sanctions financières. Alors que certains pays avaient déjà mis en place les nouvelles règles et standards techniques, comme la taille, la sécurité physique et la capacité numérique avec une puce électronique, imposés par le Règlement pour les cartes d'identité nationales nouvelle génération, d'autres pays, y compris la France, accusaient un retard en raison de divergences politiques et institutionnelles. En pratique, l'application dès 2021 de ce Règlement a pour objet d'harmoniser avec un socle minimum d'interopérabilité les cartes nationales d'identité électroniques tout en assurant leur intégrité et en favorisant leur utilisation pour de multiples usages en ligne et hors ligne. En 2022, l'Allemagne (IDUnion) et l'Espagne (Alastria) ont signé un protocole d'accord visant à collaborer et à échanger des connaissances techniques, réglementaires et opérationnelles sur l'identité numériques. Deux déclarations bilatérales similaires ont été signées entre l'Allemagne et la Finlande ainsi qu'entre l'Allemagne et les Pays-Bas. Il convient également de souligner l'initiative globale et portée à l'échelle européenne, nommée « Gaia-X », qui propose plusieurs infrastructures numériques de confiance en conformité avec le droit communautaire[245]. Ces initiatives conjointes témoignent d'engagements mutuels à développer des solutions d'identité décentralisée industrielles et complémentaires aux solutions d'identité numérique 2.0 déployées au sein de l'UE.

[244] Règlement (UE) 2019/1157 du Parlement et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité et des documents de séjour des citoyens de l'UE et des membres de leur famille exerçant leur droit à la libre circulation, EUR-Lex, consulté le 23 mars 2022 à l'adresse suivante

[245] Le cadre de conformité et labellisation Gaia-X définit ainsi trois niveaux de conformité : (i) *Gaia-X Level 1* est le niveau de base qui garantit que le service adhère bien aux principes fondateurs et techniques de Gaia-X, (ii) *Gaia-X Level 2* va au-delà pour refléter un plus haut niveau de transparence et de sécurité, les services labélisés de niveau 2 devant aussi nécessairement proposer une option permettant aux entreprises de s'assurer que traitements et données sont réalisés sur le sol européen , et (iii) *Gaia-X Level 3* va encore au-delà et prône la souveraineté européenne. Le *niveau 3* garantit une localisation et une opérationnalisation européenne des services, mais également une immunité à l'extraterritorialité de certaines lois non européennes.

A date des années 2021-2022, comme l'illustre le schéma suivant, la France ne possède pas encore de structure permettant de fédérer les acteurs du secteur de l'identité numérique décentralisée. Néanmoins, plusieurs initiatives sont en cours comme l'Alliance Blockchain France (ABF) détaillée plus loin ou le consortium de sociétés nommé Archipels[246]. Ces initiatives ont pour objectifs de créer des infrastructures et des réseaux 3.0 partagés, multisectoriels et centrés sur les utilisateurs.

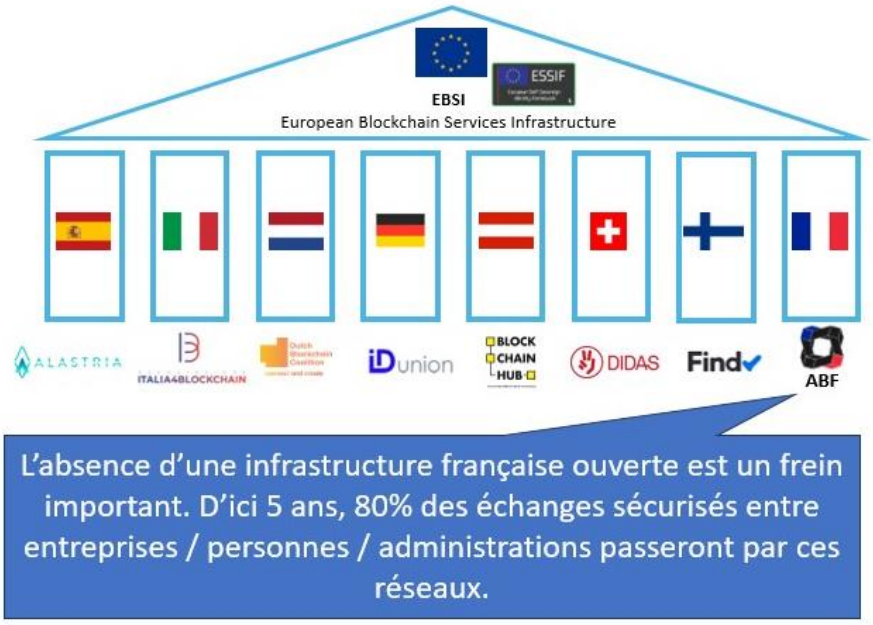


Schéma issu d'une présentation de l'ABF auprès de la DGE le 29 mars 2022.

Les sections suivantes proposent une analyse technico-juridique comparative, bien entendu non exhaustive, mais qui porte attention aux enjeux actuels et futurs de certains États membres précurseurs (l'Allemagne, l'Espagne et l'Estonie) en matière d'identité numérique en Europe.

2.2.2.1.a L'identité numérique régalienne en France : FranceConnect et CNIe

Actuellement en France, deux grands systèmes d'identification numérique sont proposés aux citoyens, FranceConnect et la carte d'identité numérique électronique (CNIe) qui possèdent plusieurs composantes technologiques comme nous allons le voir. Tout d'abord, FranceConnect est un service d'authentification régalien dont l'objectif est de simplifier les démarches en ligne des citoyens français. Techniquement, ce dispositif d'identité fédéré de type « *Single Sign On (SSO)* »[247] fonctionne grâce à un certain nombre d'informations d'identité minimum agrégées (données pivots) et permet aux citoyens de se connecter à de nombreux services en ligne publics et privés ainsi qu'auprès de fournisseurs de

[246] Archipels, « La plateforme WEB 3, pour des données et des identités vérifiables », disponible à l'adresse suivante
[247] Basée sur le protocole « *OpenID Connect* ».

services accrédités comme la caisse d'assurance maladie ou le site des impôts par exemple. FranceConnect est un « *système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives* »[248]. Ce système d'association des identités est né en réponse aux dispositifs d'identification et d'authentification numériques des GAFAM/BHATX. Une différence majeure distingue ce modèle régalien d'identité fédérée de ceux précités des fédérations d'identité des grandes entreprises du numérique. Dans le premier cas, elle n'a pas de vocation commerciale[249] tandis que dans le second cas oui. FranceConnect ne stocke aucune donnée personnelle de ses utilisateurs, car elles ne font que transiter entre les acteurs de ce modèle d'identité numérique de type fédéré, dont seule une trace pseudo-anonyme est conservée (FranceConnect se place en amont ou en aval d'un fournisseur d'attributs d'identité puis masque l'origine de ce dernier). Avec ce dispositif initié en 2015[250], complété depuis le 31 mars 2023 avec la nouvelle identité numérique désignée YRIS[251], l'objectif de l'État français est de rester un acteur incontournable dans la sphère numérique, en représentant une source de confiance numérique. Du point de vue de l'utilisateur, FranceConnect est un simple bouton de connexion intégré à des services en ligne pour l'instant étatiques. Chaque utilisateur se voit attribuer un identifiant unique pour accéder au service. Au cours de cette interaction, des données personnelles primaires sont collectées temporairement par un fournisseur d'identité agréé. Ces données sont ensuite transformées en un identifiant pseudo-anonyme qui est utilisé pour vérifier une correspondance avec les données originales identiques, qui ont été enregistrées et stockées par l'État dans le répertoire national d'identification des personnes physiques (RNIPP). Une fois cette correspondance technique assurée et certifiée, l'identifiant unique est utilisé par FranceConnect comme une preuve de l'identité racine d'une personne, dont l'identification ou l'authentification peut ainsi être réalisée par un tiers fournisseur d'identité. FranceConnect représente ainsi un outil simple d'accès, tout en permettant à ses utilisateurs un enregistrement unique pour de multiples authentifications ultérieures. En 2022, un nouveau service appelé FranceConnect+ a été lancé. Ce service offre un niveau de confiance supérieur, ce qui le différencie du service initial FranceConnect. Il s'agit d'une version actuellement gratuite et en phase d'expérimentation jusqu'en 2024 dans différents secteurs, dont la santé, le secteur social, l'éducation, le transport[252] ou la location de biens immobiliers et de véhicules. L'Assistance publique des Hôpitaux de Paris (AP-HP) expérimente actuellement la solution FranceConnect+ aux fins d'obtenir un niveau de confiance élevé au sens du Règlement eIDAS étudié plus loin et grâce à l'identité

[248] Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, consultée en ligne le 23 mars 2022.
[249] Arrêté du 11 mai 2020 relatif à l'expérimentation visant à étendre le périmètre des partenaires du téléservice « FranceConnect », JORF n°0124 du 21 mai 2020, *v.* art.3 : « ils [les services privés reliés à FranceConnect] ne peuvent commercialiser les données à caractère personnel obtenues dans le cadre du présent arrêté même avec le consentement de l'utilisateur et ne peuvent les transmettre hors de l'Union européenne ».
[250]Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », Légifrance consulté en ligne le 23 mars 2022.
[251] Il s'agit de la nouvelle identité numérique se substituant à compter du 01/04/2023 à l'identité Mobile Connect & Moi (MCEM) permettant d'accéder aux nombreux services de l'Etat via FranceConnect.
[252] Le cas d'usage du transport est pertinent pour l'identité numérique décentralisée, car chaque personne possède un droit sur son voyage dès lors qu'elle possède un moyen de preuve attestant de l'achat de ce droit (billets d'avions, de trains, etc.).

numérique fournie par le Groupe La Poste. En droit interne, l'identité numérique ne possède pas de définition donnée par le législateur et sa présence dans le droit positif semble volontairement restreinte. L'article L.226-4-1 du Code pénal vise l'infraction d'usurpation d'identité sans définir explicitement la notion d'identité numérique pour préférer retenir la formulation suivante « *lorsqu'elle est commise sur un réseau de communication au public en ligne* »[253]. Néanmoins, ce contournement destiné à ne pas se prononcer sur ce qu'est l'identité (numérique) repose sur un principe de neutralité généralement admis en droit.

Les discussions relatives à une identité numérique nationale existent en France depuis plus de 20 ans. Dès lors, il semble pertinent de dresser un succinct panorama français des multiples projets relatifs à l'identité numérique, menés par l'ancienne Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (DINSIC), actuelle Direction Interministérielle du Numérique (DINUM) soutenue par le ministère de l'Intérieur. Depuis plus d'une décennie, plusieurs autres ressources électroniques ont ainsi été développées, comme la plateforme Data.Gouv (2011) ou l'application mobile Alicem (2019) aujourd'hui remplacée par l'application SGIN[254]. Avec ces projets, l'État français affirme ses ambitions concernant l'identité numérique, avec pour objectif de fournir une identification numérique simple et sécurisée, garantie par l'État. A ce jour, le volet numérique de la CNIe très attendue a été consacré par le Décret n° 2022-676 du 26 avril 2022 autorisant le service précité SGIN comme moyen d'identification électronique[255]. Cette application mobile permet aux personnes physiques de prouver leur identité en ligne auprès de services publics et privés et de maîtriser la diffusion de leurs données d'identité, constituant ainsi un premier pas vers une identité numérique contrôlée par les utilisateurs. L'application est à ce jour facultative et d'ici fin 2023, plusieurs expérimentations à échelle réelle auront été menées afin d'envoyer « *des justificatifs d'identité à usage unique, authentiques et sécurisés* [probablement des attestations vérifiables] »[256]. Toutefois, certaines limites existent actuellement pour ces initiatives nationales par un manque de compréhension des fournisseurs de services en ligne et des fournisseurs d'identité, un manque de transparence et de supervision des sous-traitants privés pour le stockage et la transmission des données, un manque de formation du personnel, et certaines ambiguïtés dans les relations public-privé puis une réactivité politique insuffisante. Bien que la création d'une identité numérique française relève d'une responsabilité souveraine de l'État, il faut faire face à une forte influence normative, institutionnelle et politique avant d'aboutir à une identité numérique supranationale, en plus de l'identité numérique nationale. La France est aujourd'hui en retard pour la notification de son schéma d'identification numérique en comparaison à d'autres États membres

[253] Art. 226-4-1 du Code pénal, in *Légifrance*, consulté en ligne le 15 septembre 2021.
[254] « France Identité, gardez la maîtrise de vos données d'identité » in République Française, disponible à l'adresse suivante
[255] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », disponible à l'adresse suivante
[256] NEGRONI Angélique, « Les cartes d'identité vont bientôt être dématérialisées sur smartphone », in *Le Figaro*, 12 juillet 2022, « Pour l'heure [2022], 1000 personnes qui se sont portées candidates testent ce service. En septembre prochain [2023] leur nombre sera porté à 4000 », disponible à l'adresse suivante

qui ont déjà notifié leurs schémas respectifs, dont certains depuis 2018 (Estonie, Espagne, Belgique, Luxembourg)[257]. Sans notification auprès de la Commission européenne, FranceConnect n'accèdera pas au Graal de la reconnaissance mutuelle tant promise par le Règlement eIDAS. Cette latence française prend son origine dans des discordances en matière de standardisation technique et de décisions politiques, mais permet toutefois de positionner la France comme observateur des solutions d'identité numérique déjà déployées par ses voisins européens. Lors de sa notification à venir, la solution de FranceConnect pourrait avoir des difficultés à s'imposer comme modèle du fait de son retard ou encore de son modèle économique majoritairement axé sur les solutions d'identité numérique publiques et non privées. La nouvelle carte d'identité numérique électronique (CNIe) fonctionne grâce à un nouveau standard technique français désigné PACE+PIN[258]. Elle promet une nouvelle méthode d'authentification numérique pour les citoyens français[259], grâce à une capacité d'authentification sans contact et protégée par un code à quatre chiffres connus seulement de son titulaire[260]. Grâce à une nouvelle proposition parlementaire ayant modifié la loi n° 2012-410 du 27 mars 2021 relative à la protection de l'identité, la CNIe sera probablement couplée à des mécanismes d'identité décentralisée ainsi qu'au système FranceConnect, de façon à proposer une identification ainsi qu'une authentification de niveaux substantiels ou élevés en vertu de l'adoption à venir de la proposition d'amendement du Règlement eIDAS (« eIDAS-2 »), étudiés dans la première partie de cette recherche.

Cependant, bien que FranceConnect+ constitue une première étape dans l'établissement d'une confiance numérique en matière d'identité numérique souveraine, il est clair que ce système doit encore relever divers défis sur le plan informatique. En effet, si la croissance du nombre d'utilisateurs de ce système est bénéficiaire[261], FranceConnect propose aujourd'hui un nombre limité de services publics et surtout privés (1300 services en ligne en 2022) en comparaison aux besoins d'identification et d'authentification numériques gigantesques et continus des citoyens. Ainsi, cette croissance effective, mais limitée, du nombre de services en ligne caractérise une certaine difficulté de déploiement informatique du service offert par FranceConnect. De plus, la sécurité informatique de FranceConnect a été mise à l'épreuve en 2022[262]. En outre, la nature centralisée de FranceConnect, qui dépend des interactions fédérées avec des fournisseurs d'identité et de services accrédités, représente un schéma d'identité 2.0 antérieur à l'identité 3.0 et qui tend vers une décentralisation modérée à court et moyen termes. Pour éviter toute

[257] Un aperçu en temps réel des systèmes d'identification électronique pré-notifiés et notifiés des États membres est disponible à l'adresse suivante. Le schéma d'identité numérique français (FranceConnect) a finalement été notifié en février 2021.
[258] Ce nouveau référentiel est dérivé de la norme internationale « Identification-Authentification-Signature European-Citizen-Card (IAS-ECC) », *v.* Wikimedia, disponible à l'adresse suivante
[259] « La carte d'identité contiendra deux puces, l'une réservée à la vérification de l'identité du porteur au moyen de ses empreintes digitales (puce dite 'régalienne'), qui ne pourrait être lue que par les autorités habilitées à procéder à un contrôle d'identité, l'autre réservée à la fonctionnalité mise en place par le présent article (puce 'vie quotidienne'), qui pourrait être lue par des dispositifs diffusés dans le commerce et raccordés à un ordinateur personnel », *op. cit.* Sénat. 1er juin 2022. Proposition de loi relative à la protection de l'identité, disponible à l'adresse suivante
[260] Par analogie, ce système fonctionne comme celui des téléphones mobiles qui possèdent un code maître « code PUC » et un code dérivé d'authentification « code PIN ».
[261] FranceConnect dénombre 30 millions d'utilisateurs en 2022.
[262] DOMENECH Claire, « Des milliers d'euros volés via le site des impôts à cause du bouton FranceConnect », 2022, in *Capital.fr*

confrontation notamment politique entre ces deux systèmes de gestion des identités numériques, une éducation massive couplée à des compromis informatiques seront au cœur des enjeux de la version future de FranceConnect ou encore de l'application SGIN et de leur interface avec la CNIe. En définitive, les constats et défis précédents permettent d'envisager que les solutions d'identité décentralisée en cours de développement (y compris celles adossées sur une blockchain) en France seront compatibles avec l'identité numérique « pivot » de FranceConnect+, mais aussi avec la CNIe[263]. Pour cela, FranceConnect doit avec la DINUM[264] et l'ANSSI[265] comprendre comment appréhender cette future cohabitation technique, notamment au regard de l'adoption prochaine d'un portefeuille d'identité numérique européen étudié plus loin. Pour cela, un cadre juridique spécifiquement dédié et relatif à la non-commercialisation des données collectées doit persister, de sorte que l'Etat ne devienne pas, malgré lui, un fournisseur de données d'identité à vocation commerciale (comme cela tend à être le cas en Espagne). Toutefois, en 2023, il demeure que FranceConnect a été légalement conçu pour se connecter à un site internet de confiance géré par l'Etat et ses institutions. A cet égard, l'arrêté du 8 novembre 2018 donnant naissance et encadrant FranceConnect pourrait être modifié en conséquence afin de permettre à ce système la gestion éventuelle d'attributs d'identités décentralisées (VC, DID)[266] qui sont étudiés plus loin. D'ailleurs, dans un dossier thématique publié en mars 2023, la CNIL aborde et encourage l'utilisation d'une identité numérique décentralisée. Remarquons finalement que la France a fait le choix, contrairement à l'Estonie, de ne pas imposer une identité régalienne numérique unique, c'est-à-dire de laisser le choix à l'utilisateur de confier ses données personnelles à un opérateur de son choix.

2.2.2.1.b Lancement de l'Alliance Blockchain France

Depuis plusieurs années, la Commission européenne a privilégié le financement de technologies essentielles notamment en matière de cybersécurité et d'intelligence artificielle[267] ou encore d'hébergement informatique (cloud) de confiance[268]. Cette volonté est accentuée par un environnement où la confiance numérique est de plus en plus critique et au sein duquel la technologie blockchain peut être un nouveau catalyseur de confiance pour la sécurisation des interactions numériques. Désormais

[263] Actuellement, la composante électronique de la CNIe est désactivée pour des raisons juridiques, c'est-à-dire concernant l'impossibilité légale d'utiliser la partie électronique de la CNIe par des entreprises et services privés. Cela implique que chaque citoyen français reçoit sa CNIe et peut pour l'instant ne s'en servir qu'en tant que document de voyage au sein de l'UE ou comme attestation d'identité en France. La capacité numérique de cette carte est donc désactivée pour le moment, bloquée par défaut en sortie de production, en attendant que des amendements permettent à des entreprises privées et aux citoyens d'interagir avec cette fonctionnalité numérique de la CNIe.
[264] Direction interministérielle du numérique (DINUM)
[265] L'agence nationale de la sécurité des systèmes d'information (ANSSI).
[266] V. *infra*, II, Titre 1, 1.3.1
[267] Proposition de Règlement 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union.
[268] CE, « Cloud computing. Shaping Europe's digital future ». Consulté le 27 septembre 2022 à l'adresse suivante

perçue comme un nouvel enjeu technologique à l'échelle communautaire, la blockchain s'est tout particulièrement affirmée à la suite de la crise sanitaire et au besoin croissant de sécurisation des échanges en ligne. L'Alliance Blockchain France (ABF) naît d'une volonté de proposer des identités numériques décentralisées (en réalité hybrides sur le plan informatique) afin de faciliter le partage de données, de réduire drastiquement la fraude et les litiges en ligne tout en automatisant l'exécution de contrats (contrats intelligents). Il s'agit d'une initiative à but non lucratif qui a pour vocation de proposer à l'échelle nationale une nouvelle infrastructure numérique souveraine et partiellement décentralisée grâce aux technologies blockchains, en commençant par le secteur de l'identité numérique. Avec ses 17 membres fondateurs[269], cette association régie par la loi du 1er juillet 1901 fédère des acteurs publics, académiques et privés français pour favoriser l'émergence et le développement d'un écosystème national de pointe autour des registres électroniques distribués (blockchains), dans un objectif de développement de services digitaux innovants, sans pour autant fournir d'attributs d'identités numériques, mais simplement un écosystème d'acteurs reconnus et de confiance. L'association a également pour objet de développer les initiatives ayant un impact positif sur les valeurs démocratiques et l'environnement. Plus précisément, elle vise à créer des infrastructures de premier niveau gérées de façon mutualisée entre ses membres. En pratique, la création d'un consortium entre acteurs économiques majeurs est un processus long et complexe avec la mise en place d'une gouvernance centralisée ou semi-décentralisée, souvent difficile à équilibrer pour des entreprises ayant des ressources et des stratégies différentes. Jusqu'à présent le principal moyen de garantir la conformité juridique d'un tel regroupement d'acteurs implique l'usage d'une blockchain hybride, c'est-à-dire la création d'un consortium informatique et contractuel entre plusieurs acteurs.

2.2.2.1.c L'identité numérique Estonienne

L'Estonie est régulièrement citée comme étant le pays européen pionner en matière d'identité numérique régalienne. Depuis 20 ans déjà, chaque citoyen estonien (environ 98%)[270] dispose d'une carte d'identité numérique (désormais similaire à la CNIe française) permettant d'accéder à plusieurs milliers de services publics et privés[271], y compris de façon dématérialisée par téléphone mobile. En plus d'une avance temporelle, l'Estonie est un exemple à suivre concernant la dimension technique de son identité numérique. En effet, une blockchain privée et étatique (« *KSI blockchain* ») assure à chaque institution publique une importante sécurité et interopérabilité informatique entre leurs systèmes et services grâce

[269] V. site officiel de l'Alliance Blockchain France (ABF) à l'adresse suivante www.alliance-blockchain.org
[270] Compte-rendu de la table ronde relative à « La transformation numérique de l'école en Estonie et en France », co-organisée par France Stratégie et l'ambassade d'Estonie en France, le 5 mai 2017.
[271] Accès aux infrastructures de transports publics, voter en ligne, ester en justice, récupérer une ordonnance médicale, signer des contrats, créer et gérer une société, enregistrer le nom d'un nouveau-né, etc.

à une plateforme distribuée (« X-Road »)[272]. En complément, ce système qui est en réalité plus *distribué* que complètement *décentralisé* sur le plan informatique[273], assure aux citoyens une confidentialité technique et juridique sur leurs données. Si ce système se montre efficace pour gérer un nombre important de transactions, une certaine opacité technique demeure quant au fonctionnement informatique réel de cette architecture informatique. Si ce manque de transparence peut se justifier par une volonté de ne pas révéler d'éventuelles failles techniques aux yeux des développeurs du monde entier, il est probable qu'une ouverture des codes sources de cette infrastructure bénéficierait à long terme à cette dernière. Pour illustration des propos précédents, une faille de sécurité a été décelée en 2017 sur la CNIe estonienne, impactant plus de 760 000 citoyens[274] (impossibilité d'accès à certains services en ligne et usurpation de l'identité de certains citoyens estoniens). Il ne fait aucun doute que l'architecture informatique 3.0 actuellement utilisée en Estonie sera un jour compatible avec les normes d'identité décentralisée, pour fournir une couche informatique supplémentaire de confiance aux citoyens estoniens. Il convient de noter qu'un compromis informatique (solutions hybrides versus décentralisées) sera probablement nécessaire pour empêcher les citoyens de prendre le contrôle total de l'émission de leurs identités, c'est-à-dire de leur permettre uniquement la gestion et non pas l'émission de leurs données d'identité, comme cela est étudié par la suite.

2.2.2.1.d L'identité numérique en Espagne : DNIe et Alastria

Par le décret n°1553 du 23 décembre 2005, pris en application de la loi 59/2003 du 19 décembre 2003, l'Espagne prévoit la présence d'une puce informatique sur la carte d'identité qui devient ainsi électronique (« *documento nacional de identidad electronica – DNIe* »). Sur cette puce se trouve l'ensemble des données personnelles disponibles sur la version imprimée de la carte, la photographie du titulaire du document, la signature numérisée et le modèle d'empreinte digitale, ainsi que les certificats d'authentification (lesquels permettent l'identification du titulaire) et les certificats de signature (lesquels permettent la signature électronique de documents en ligne)[275]. La DNIe peut être lue par un lecteur de carte ou encore par un téléphone mobile doté de la technologie NFC[276], via une application mobile nommée « Mobbeel »[277]. Cette dernière permet aux citoyens de ne s'identifier qu'une seule fois pour avoir accès à une multitude de services publics et privés (modèle d'identité fédérée similaire à FranceConnect) : automobile, jeux en ligne, voyages et tourisme, etc. Après la lecture de la DNIe, il est

[272] Pour plus d'informations sur les spécificités informatiques de cette blockchain privée et de cette plateforme, disponible en ligne
[273] En sciences de l'informatique, une distinction entre les notions de « distribution » versus « décentralisation » est courante. Il est proposé de la revisiter dans une partie dédiée
[274] « Security flaw forces Estonia ID 'lockdown' », in *BBC News*, 3 novembre 2017, consulté en ligne le 23 mars 2022.
[275] Ministère de l'Intérieur Espagnol (ministerio del interior), Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, 2005, consulté en ligne le 23 mars 2022.
[276] Wikipedia contributors, « Near-field communication (NFC) », 2022, consulté en ligne le 23 mars 2022.
[277] « Mobbeel », consulté en ligne le 23 mars 2022.

vraisemblablement demandé au citoyen de renseigner son code PIN pour accéder au service public ou privé concerné (ce code PIN est similaire au PIN français qui n'a toutefois pas encore activé cette fonctionnalité). De plus, ce code PIN doit être mis à jour tous les 30 mois par le citoyen, qui doit alors se rendre physiquement dans les bureaux émetteurs de DNIe pour ce faire. C'est la loi 6/2020 du 11 novembre 2020[278] règlementant certains aspects des services de confiance électronique qui vient apporter des précisions sur l'accès à des services en ligne via la carte d'identité électronique espagnole. Parmi ces services peuvent être énumérés certains provenant du secteur privé. Il peut en outre s'agir de banques (Kutxabank, Unicaja Banco, Barclays), de services de télécommunications (Vodafone), de compagnies d'assurance (MAPFRE), etc. La capacité numérique de la DNIe 2.0 offre aux citoyens espagnols la possibilité d'accéder à des services en ligne certifiés permettant la signature électronique, des démarches administratives, la prise de rendez-vous chez le médecin et d'autres activités de la vie quotidienne. En droit espagnol, rien n'interdit un accès de la part des sociétés privées aux données personnelles des citoyens disponibles dans la puce de la DNIe (pas d'accès restreint comme en France). Il reste à supposer que les sociétés aient accès aux données disponibles sur la puce auxquelles elles ont strictement besoin pour combler leurs finalités commerciales, comme l'illustre par exemple la société Kutxabank qui ne se cache pas de collecter les données biométriques à des fins commerciales (empreintes digitales et reconnaissance faciale) des citoyens/clients[279]. L'autorité de protection des données espagnole ne se prononce pas à ce sujet. En droit, l'application Mobbeel permet – comme l'application allemande - un niveau d'authentification élevé au sens du Règlement eIDAS en ce qu'elle permet aux citoyens un embarquement (une première identification) à travers leurs données biométriques[280]. En matière d'identité numérique décentralisée, l'Espagne compte parmi les pays de l'UE les plus avancés. En effet, un consortium d'acteurs privés (« Alastria »)[281] est né dès 2019 sur le sujet. Le consortium Alastria suscite un intérêt croissant et compte désormais une centaine d'acteurs et une infrastructure blockchain en expansion. Sa structure (informatique, juridique et en termes de gouvernance) en fait l'un des plus respectés en Europe. Cependant, contrairement au consortium allemand « IDunion », qui a été initié par des acteurs publics et privés allemands, Alastria manque de soutien de la part des institutions publiques espagnoles. Ce dernier élément est crucial afin que les institutions espagnoles ne soient pas vectrices, comme en France, de tels freins politiques concernant l'utilisation de technologies 3.0 au service supposé des droits des citoyens.

[278] WIPO Lex, 2020, accessible en ligne à l'adresse suivante
[279] Kutxabank, « *Particulares* », isponible à l'adresse suivante
[280] Disponible à l'adresse suivante
[281] Disponible à l'adresse suivante

2.2.2.1.e L'identité numérique en Allemagne : le consortium IDunion

En 2021, le gouvernement allemand a dévoilé une nouvelle application d'identité numérique « *AusweisApp2* »[282] couplée à la carte d'identité nationale allemande. Les autorités peuvent ainsi délivrer cette nouvelle carte d'identité électronique à tous les citoyens allemands ainsi qu'aux étrangers âgés de 16 au moins[283]. Au sens du Règlement eIDAS, cette application mobile couplée à la CNI allemande assure un niveau de confiance élevé[284] (au même titre que l'Espagne dont le schéma d'identification électronique est également d'un niveau de garantie élevé)[285]. La société Governikus[286], basée en Allemagne, a été chargée de mettre en œuvre l'implémentation de l'identité numérique de référence allemande. Elle a mis en œuvre l'infrastructure technique afférente dont l'application AusweisApp2, disponible sur Windows, MacOS, Android et iOS. Elle représente ainsi l'application standard pour tous les services en ligne liés au gouvernement en Allemagne. Son fonctionnement est transparent et est fourni sous une licence open source (EUPL 1.2)[287] (contrairement aux applications d'autres pays). Si cette nouvelle CNIe allemande est comparable à celle actuellement déployée en Espagne et en France ainsi que plus généralement dans l'UE (en raison des règles communes qui émanent du Règlement eIDAS), un consortium d'acteurs privés nommé (IDunion)[288] développe actuellement des cas d'usages liés à la blockchain[289] et à l'identité décentralisée et utilisera très probablement les capacités d'identité numérique actuelle de cette CNIe. Par conséquent, le modèle d'identité numérique allemand est bien positionné pour fournir une identité numérique distribuée (IND) ou auto-souveraine (INAS). Le modèle français pourrait s'inspirer de ce dernier, tant sur les plans respectivement techniques que politiques, par exemple en s'inspirant du manifeste politique signé en 2021 par l'Allemagne avec la Finlande pour une coopération sur l'identité numérique décentralisée[290].

[282] Disponible à l'adresse suivante www.ausweisapp.bund.de
[283] *Op. cit., v.* l'adresse suivante
[284] Disponible à l'adresse suivante
[285] Schémas d'identification électronique notifiés conformément à l'article 9, paragraphe 1, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, 2019, page 1 à 3, accessible à l'adresse suivante
[286] Disponible à l'adresse suivante
[287] Décision d'exécution (UE) 2017/863 de la commission du 18 mai 2017 actualisant la licence logicielle open source EUPL afin de faciliter le partage et la réutilisation des logiciels développés par les administrations publiques. Disponible à l'adresse suivante
[288] Disponible à l'adresse suivante
[289] Ce consortium a mis en place une *blockchain hybride* dont les données sont accessibles en temps réel à l'adresse suivante
[290] « Nederland gaat met Duitsland werken aan digitale identiteit, ministerie van Binnenlandse Zaken en Koninkrijksrelaties », 23 septembre 2021, disponible à l'adresse suivante

2.2.2.2 Une blockchain européenne (EBSI) pour une identité distribuée

En 2017, certains chercheurs estimaient[291] déjà que les gouvernements pourraient créer leurs propres blockchains régulés (blockchains hybrides ou privées) afin de tenter de retranscrire certaines règles de gouvernance sociale en code : « *si les gouvernements pouvaient ne pas parvenir à réglementer la technologie blockchain de manière exhaustive, ils pourraient néanmoins s'appuyer sur les blockchains comme moyen d'appliquer leurs propres lois et réglementations de manière plus efficace et automatique*. »[292]. Ainsi, quelques années seulement après ces propos qui semblent se confirmer, le 10 avril 2018, vingt et un États membres ainsi que la Norvège ont accepté de signer une déclaration créant le Partenariat européen pour la blockchain (EBP) et débouchant sur la création d'une infrastructure blockchain européenne commune : « *European Blockchain Service Infrastructure - EBSI* »[293]. Depuis 2020, l'EBSI déploie un réseau consortium de (36) nœuds[294] blockchain à travers l'Europe[295], soutenant des applications centrées sur des cas d'utilisation spécifiques[296]. L'EBSI est la première infrastructure blockchain pilotée à l'échelle de l'UE et pour l'intant uniquement à destination du secteur public. L'EBSI est conçue comme un écosystème favorable au marché, reposant en théorie sur des normes informatiques et juridiques ouvertes et un modèle de gouvernance transparent. L'EBSI a émergé afin de répondre de façon commune à des problématiques récurrentes que rencontrent des projets utilisant la technologie blockchain. Il s'agit d'une infrastructure dite « *multi-chain* », c'est-à-dire interopérable et compatible avec différents protocoles et autres infrastructures blockchains plus ou moins ouvertes (blockchains publiques, privées ou hybrides étudiées plus loin). En théorie, l'EBSI se développe autour de quatre principes fondateurs qu'il nous semble important de résumer puis d'analyser sous la forme d'un tableau :

[291] De FILIPPI Primavera, « Blockchain and the Law », in *Harvard University Press*. *op. cit.*
[292] *Ibid*. Emplacement 3762 sur 7004.
[293] ELIE Pauline, SEGHIER Neil, LANGLOIS-BERTHELOT Thibault, « Blockchain et Digital ID Wallet : vers une identité européenne décentralisée ? », Mai 2022, atelier n°2, Les Temps Numériques, document scientifique disponible à l'adresse suivante
[294] V. Annexe 6, Focus 3.
[295] Notons que seulement 11 des 36 nœuds sont des nœuds validateurs. EBSI. (2018). Commission européenne. Consulté le 1er avril 2022 à l'adresse suivante
[296] Fonctionne pour le moment via des « *Pre Commercial Procurments - PCP* » concernant différents cas d'usages pilotes permettant de sélectionner différents acteurs (initialement et exclusivement du secteur public puis progressivement du secteur privé).

(i) Devenir un bien commun numérique	(ii) Fournir une gouvernance de confiance et une harmonisation des interactions numériques	(iii) Accessibilité et transparence informatique	(iv) Conformité aux règlementations et aux valeurs européennes
L'administration de l'EBSI doit servir le bien commun et il lui incombe de limiter son utilisation aux services publics dans un premier temps, puis de s'ouvrir aux acteurs privés dans un second temps. Le regroupement de ces acteurs permettra d'assurer ce souhait de positionnement en tant que bien public au service des citoyens, des entreprises et des États membres dans leur ensemble. En 2022 l'EBSI représente donc une infrastructure blockchain hybride qui ne doit pas être confondue avec les blockchains publiques. Cette recherche suppose que la blockchain Bitcoin[297] est considérée comme un bien commun numérique universel, et qui est neutre politiquement et socialement. En revanche, l'EBSI est considéré comme un bien commun numérique artificiel, qui est créé par un petit nombre d'acteurs publics et privés et qui est réglementé politiquement, juridiquement et économiquement. Par conséquent, il est supposé que le crypto-actif associé à la blockchain Bitcoin est un jeton	En principe, le système de gouvernance de l'EBSI garantit que les décisions sont prises grâce à un consensus entre ses parties prenantes internes (Etats membres). Cette centralisation politique assure un caractère sur mesure et consensuel des décisions, notamment pour garantir une adéquation juridique et économique des services et infrastructures déployées au sein de l'UE. Il est important que la gouvernance de l'EBSI favorise et maintienne une harmonisation des exigences techniques et informatiques pour éviter la multiplication des différents protocoles blockchains pris en charge, tout en évitant l'apparition de systèmes 3.0 qui seraient incompatibles.	Dans la mesure du possible, le code source des infrastructures et des services de l'EBSI doit être accessible à un grand nombre de développeurs pour permettre un audit et une sécurité informatique maximum. De plus, cette transparence favorise une concurrence saine entre les fournisseurs d'identité, de services et plus généralement pour le secteur privé. Il s'agit néanmoins de reconnaître la dépendance actuelle de l'EBSI envers les blockchains publiques qui sont les principales	L'EBSI doit être en conformité avec l'interprétation actuelle et les mises à jour futures du RGPD ainsi qu'avec eIDAS et d'autres règlementations (notamment lorsqu'une tokenisation financière surviendra, c'est-à-dire lorsque sera associé un crypto-actif - stables ou non - à des fins informatiques et/ou commerciales)[298]. L'EBSI doit en effet respecter toutes les règlementations pertinentes pour assurer la protection des données et garantir la sécurité des transactions effectuées sur sa plateforme.

[297] V. Annexe 3, Focus 6.

[298] L'introduction d'un ou de plusieurs crypto-actifs (jeton d'utilité ou de paiements) au sein d'une ou plusieurs des infrastructures blockchains de l'EBSI est politiquement rejeté à ce jour (2022). En effet, s'agissant d'une *blockchain consortium* soit *hybride*, une méfiance voire une forme de défiance envers les *blockchains publiques* (en raison de leurs crypto-actifs natifs), demeure dans les sphères politiques et institutionnelles européennes.

numérique universel ‘pur’ et incensurable, tandis que les futurs jetons numériques de l'EBSI seraient considérés comme ‘artificiels’. Il est prévu que la blockchain de l'EBSI héberge des jetons numériques artificiels d'ici quelques années, comprenant probablement à terme un euro cryptographique.	Cette harmonisation doit également garantir que seuls les protocoles conformes au droit communautaire sont intégrés, afin d'éviter tout conflit juridique.	sources d’innovation.	

En 2023, l'EBSI se concentre sur trois catégories principales d'utilisation, l'identité numérique décentralisée, la traçabilité numérique et le partage de données en toute confiance. Pour l'identité numérique décentralisée, l'EBSI vise à mettre en place un modèle d'identité plus autonome en Europe qui permet aux utilisateurs de contrôler leur identité au-delà des frontières nationales. Pour la traçabilité numérique, l'EBSI cherche à créer des pistes d'audits numériques fiables, c’est-à-dire à automatiser les contrôles de conformité et les preuves de l'intégrité des données. En matière de partage de données, l'EBSI souhaite faciliter la communication entre les autorités douanières et fiscales de l'UE, notamment pour ce qui concerne les numéros d'identification et le guichet unique d'importation (TVA & IOSS)[299]. Ce fonctionnement de l’EBSI est à ce jour limité par un financement par cas d’usages successifs[300] qui continuera jusqu’à 2023 ou 2024. A partir de 2024 et d’ici 2026[301], une ouverture complète de cette blockchain et une mise à l’échelle seraient possibles. Une reconnaissance technique des blockchains publiques semble importante à soutenir politiquement pour l’avenir de l’EBSI, notamment pour favoriser une innovation durable de tout cet écosystème 3.0 (via une reconnaissance politique et éventuellement juridique avec des règles de droit adaptées). En outre, il est important de noter que l'EBSI doit relever plusieurs défis à court terme, d'ordres informatique, juridique[302] et politique. La mise en place d'une gouvernance impliquant un grand nombre d'acteurs nécessite du temps pour la négociation et la mise en place de solutions encore en phase d'expérimentation. Le 14 février 2023[303], la Commission

[299] « Afin de mieux adapter la perception de la TVA à la réalité du commerce électronique transfrontalier et d’en sécuriser la perception dans le pays de consommation de la marchandise, un nouveau régime optionnel de taxation a été créé : le régime IOSS (Import One-Stop-Shop). Le dispositif mis en place consiste en un guichet unique de TVA, qui permet de simplifier les obligations déclaratives et le paiement de la TVA sur les ventes à distance de biens importés d’une valeur inférieure ou égale à 150 euros ». Réglementation sur le guichet unique de TVA ou IOSS. 2022. V. le portail de la direction générale des douanes et droits indirects à l’adresse suivante

[300] *Op. cit.* Ce financement de cas d’usage spécifiques se nomme en anglais des « Pre-Commercial Procurement (PCP) », qui fonctionnent par phases successives (Phase 1, Phase 2A - actuelle en 2022 - Phase 2B), « European Blockchain Pre-Commercial Procurement », octobre 2021, in *Shaping Europe’s Digital Future*, disponible à l’adresse suivante

[301] DUSSUTOUR Olivier, directeur général de la société Nexus : « Grâce aux travaux européens en cours, nous aurons peut-être la chance de présenter d’ici 2026 les premiers schémas massifs d’identité décentralisée », Propos recueillis lors du Forum International sur la Cybersécurité (FIC) le 09/09/2021, table ronde : « Quels modèles alternatifs pour l’identité ».

[302] A titre d’illustration, des avis divergents existaient entre le fait d’ancrer directement sur la blockchain de l’EBSI des identifiants décentralisés (DID) ou bien simplement des preuves de ces DID.

[303] Traduction libre de l’anglais : « L'objectif de l'European Blockchain Regulatory Sandbox’ est de faciliter le dialogue transfrontalier avec et entre les régulateurs et les superviseurs d'une part, et les entreprises ou les autorités publiques d'autre

européenne a lancé un bac à sable règlementaire (« legal sandbox ») pour l'expérimentation de cas d'utilisation innovants liés à son infrastructure blockchain. Ce bac à sable, qui fonctionnera de 2023 à 2026, soutiendra chaque année 20 projets dont certains concernant l'utilisation de l'EBSI par le secteur public. En d'autres termes, lorsque les blockchains fermées d'entités (entreprises, institutions publiques) seront compatibles avec celles de l'EBSI, alors cette dernière bénéficiera par conception d'une compatibilité de sa blockchain avec celles de toutes les autres entités liées à cette infrastructure informatique. L'EBSI représente en quelque sorte une blockchain d'entreprise(s) politique, et pourrait à terme être compatible (sous réserve d'une volonté politique en ce sens) avec d'autres blockchains plus ouvertes[304]. Bien que les blockchains publiques soient actuellement décentralisées, leur adoption sociale est limitée en raison d'un manque de reconnaissance juridique et politique, ce qui crée une concurrence relative avec l'EBSI qui bénéficie d'un soutien politique et juridique solide.

2.3 La blockchain, une technologie dans la continuité d'Internet (Web 3.0)

La technologie blockchain n'est tout d'abord qu'un type particulier de registre électronique. Si toutes les blockchains sont des registres informatiques, tous les registres informatiques ne sont pas des blockchains. Si un registre est un concept générique décrivant le stockage d'une liste d'informations de même nature, une blockchain l'est également, mais sous la forme spécifique d'une suite séquencée de blocs de transactions répliqués par une multitude d'ordinateurs interconnectés. En effet, le terme de registre électronique désigne un large éventail de technologies visant à stocker, à synchroniser et à conserver des enregistrements dématérialisés au sein d'un réseau informatique. Ce principe de maintien à jour d'un registre de transactions n'est conceptuellement pas nouveau, car les premiers registres physiques et hors ligne remontent environ à 4 000 ans avant Jésus-Christ en Mésopotamie[305]. Ces registres physiques étaient conservés sur des manuscrits en argile ou gravés dans la pierre et étaient utilisés pour enregistrer et prouver les transferts de propriété et gérer les stocks des cultures agricoles. Soulignons que ce concept de registre existait également dans d'autres civilisations en Inde et en Amérique du Sud[306], c'est-à-dire de façon universelle. Les registres sous la forme de livres et de papiers ont largement décliné avec l'avènement du numérique et la dématérialisation massive des informations. La notion de réseaux décentralisés existait aussi avant l'apparition de l'Homme. En effet, certains organismes vivants tels les champignons ont réussi à mettre en place des réseaux biologiques

part. Dans le cadre de ces dialogues, les développeurs de cas d'utilisation peuvent présenter leur cas d'affaires pour recevoir des conseils juridiques de la part des régulateurs. Le cabinet d'avocats Bird & Bird joue le rôle de facilitateur, met en place une interface sûre entre les développeurs et les régulateurs et fournit des conseils juridiques aux cas d'utilisation de la blockchain sélectionnés. Les questions règlementaires peuvent concerner n'importe quel domaine du droit ». « Launch of the European Blockchain Regulatory Sandbox », in *Bâtir l'avenir numérique de l'Europe*, disponible à l'adresse suivante

[304] La blockchain de l'EBSI utilise à ce jour une version privée (Proof of Authority - PoA) de la blockchain publique Ethereum, *v.* Annexe 6, Focus 2 et 3.

[305] DOU Wenyu, « Blockchain, a revolution in e-commerce », 7 août 2018, in *City Business Magazine*, consulté en ligne le 12 janvier 2022.

[306] QUISQUATER Jean-Jacques, *op. cit.*, « Quels modèles alternatifs pour l'identité ».

décentralisés depuis des millénaires, ce qui en fait historiquement l'un des royaumes décentralisés les plus prospères de la planète. Ainsi, la décentralisation serait-elle un gage de longévité pour un réseau biologique comme informatique ? Si cette stratégie fonctionne en biologie (autrement la nature n'insisterait pas pour la reproduire), peut-on en dire autant dans le domaine de l'informatique décentralisée ? Si des analogies existent entre ces réseaux biologiques et informatiques décentralisés, il semble que seul le temps puisse permettre de répondre à cette question. En des termes simplifiés, une blockchain est un vaste répertoire numérique chiffré et stocké sur plusieurs ordinateurs dans un environnement informatique ouvert ou fermé, c'est-à-dire dont les informations sont publiquement accessibles ou non à des tiers. Un tel registre numérique implique la réunion de trois composantes numériques, un consensus social, un accord commun par rapport à un réseau donné, et la réalisation d'échanges et d'interactions de données entre des internautes et des ordinateurs qui se communiquent automatiquement des informations formant ainsi un registre électronique de transactions. Aujourd'hui, le terme blockchain, parfois évoqué par les experts informatiques par le terme d'infrastructure à clé publique décentralisée (« DPKI »)[307], est souvent mal employé. Il n'est pas facile à comprendre pour le grand public parce qu'il fait référence à une variété de concepts informatiques et commerciaux différents, ce qui peut le rendre obscur. Il est toutefois possible de surmonter cette difficulté en raison d'un nombre croissant d'exemples d'utilisation innovants de cette technologie. Il faut faire la distinction entre la technologie elle-même et les applications numériques qui en découlent. Internet est une technologie de rupture dont les sites internet ne représentent qu'une des applications et des cas d'usages possibles[308]. Par analogie, les technologies blockchains sont des technologies de rupture, dont la blockchain Bitcoin ne représente qu'une des applications possibles[309]. Il s'agit donc de penser les technologies blockchains en contexte et par usage, afin d'écarter un risque de confusion entre une technologie, ses multiples variantes informatiques possibles et ses multiples applications sous-jacentes.

Une technologie blockchain n'est que l'agrégat d'ordinateurs appelés des nœuds[310] - plus ou moins nombreux et puissants selon les besoins - qui s'échangent des informations et des transactions de données. Ce n'est donc pas tant l'infrastructure matérielle de cette technologie qui est révolutionnaire, mais plutôt son protocole et ses algorithmes, c'est-à-dire ses mécanismes de communication informatique, souvent regroupés sous les termes de mécanisme de consensus ou plus abstraitement de gouvernance. En principe, ces mécanismes de gouvernance étudiés en Annexes dictent aux ordinateurs une nouvelle façon inédite de s'échanger des informations réciproques. Le fonctionnement d'une blockchain exige que chaque transaction soit vérifiée indépendamment par d'autres ordinateurs des

[307] PAPGEORGIOU Alexander, MYGIAKIS Antonis, et al., « DPKI: a blockchain-based decentralized public key infrastructure system », 1er juin 2020, IEEE Conference Publication, in *IEEE Xplore*. Consulté le 29 juin 2022, à l'adresse suivante

[308] DUSSER Blandine, CLAUDE Hélicia, « Le guide de sensibilisation de la blockchain, pour mieux comprendre cette technologie », in *Rapport DGE*, avril 2022, entreprises.gouv.fr

[309] Bitcoin fonde en l'occurrence le concept de blockchain et représente sa première application à vocation monétaire et financière.

[310] V. Annexe 3 (Focus 1 à 3) et Annexe 6 (Focus 1 à 3).

milliers de fois pour être acceptée, c'est-à-dire ajoutée à la suite du registre des transactions déjà validées. Ainsi, contrairement aux serveurs centralisés qui confirment les transactions en quelques centaines de millisecondes, une blockchain exige que des utilisateurs attendent en moyenne entre 10 secondes et 10 minutes pour obtenir une confirmation selon les règles propres à chaque blockchain. D'un point de vue philosophique, l'émergence de la blockchain en tant que nouvelle couche technologique remonte aux années 1990, portée par des revendications provenant de mouvements libertariens américains, parfois également d'inspiration anarchique et transhumaniste[311]. L'origine de la technologie blockchain prend ainsi racine avec l'avènement de la cryptographie couplée à une recherche d'anonymat. L'approche traditionnelle et centralisée des serveurs et de leurs données est actuellement la plus répandue en demeurant une méthode d'application mature et appropriée pour de nombreux cas d'usages en entreprise. Cependant, cette concentration des données et des échanges d'informations sur une unique machine implique que la base d'informations soit inutilisable, voire détruite, dès lors que cette dernière cesse de fonctionner, par exemple en cas de piratage ou de panne de l'un de ses composants. Pour résoudre cette problématique de sécurisation des données, ces dernières informations vont être distribuées ou décentralisées[312], c'est-à-dire dispersées sur plusieurs machines distinctes, mais dont les échanges d'informations et de données sont communs, interdépendants et soumis à une validation informatique mutuelle. Cette validation de chacune des transactions du réseau est effectuée sous forme de *blocs*[313] de transactions et conditionnée à une acceptation - fixée par des règles de consensus[314] - par les ordinateurs de ce tissu informatique 3.0. L'avantage théorique d'une blockchain est de rendre visibles aux yeux de tous la probité et la transparence des processus de vérification qui s'opèrent sur le réseau.

A ce stade, il semble que la singularité d'une blockchain réside dans le fait que chaque ordinateur du réseau puisse respectivement valider des demandes de transaction, tout en copiant puis en stockant simultanément sur tous les autres ordinateurs chacune des transactions de données effectuées par l'ensemble des utilisateurs du réseau. Pour cela, l'ensemble des transactions validées par chaque machine est regroupé au sein de blocs de transactions successifs et cryptographiquement liés de façon consensuelle les uns aux autres : une chaîne de blocs se forme. De manière générale, les ordinateurs d'un réseau blockchain sont répartis de manière fragmentée, c'est-à-dire qu'ils sont géographiquement distribués dans différentes régions du monde. Cela entraîne une décentralisation du registre et de l'historique des transactions de données. Dans ce cas, le réseau blockchain ne nécessite plus

[311] BOUSQUET Marc, « Tout savoir sur le Bitcoin et les cryptomonnaies », Ed. du Sens, « un homme augmenté et une liberté absolue de l'humain, libéré notamment du poids étatique grâce à la puissance des machines », in *Dossiers Science Hors-Série*, nov. 2022, p. 10.
[312] La doctrine informatique opère une distinction de degré entre la distribution et la décentralisation des données. La première répartit de façon partielle les données, la seconde de façon quasi totale. Il s'agit d'une distinction de degré et non de nature, *v.* Glossaire.
[313] Un bloc de transaction ne peut pas être altéré sans affecter l'intégralité de toute la chaîne située en amont et en aval de ce bloc. La rectification requiert une telle quantité de calcul qu'elle en devient théoriquement impossible à mettre en œuvre.
[314] V. Annexe 6, Focus 1.

l'intervention d'un tiers de confiance centralisé pour assurer la validité, la continuité et le maintien des transactions réalisées. Comme exposé en Annexes[315], ces ordinateurs connectés dédient une partie de leur puissance de calcul pour valider, enregistrer et maintenir en toute autonomie et simultanément, un journal et un historique communs d'échanges effectués entre les utilisateurs de ce réseau décentralisé. Il faut souligner que la nature de ces transactions d'informations peut varier selon la finalité propre à chaque blockchain : transactions financières (sous la forme de crypto-actifs), transactions contractuelles (contrats numériques), transactions sociales (droits de votes électroniques et signature électronique) et transactions phygitales (traçabilité numérique de biens et/ou de produits physiques avec des jetons numériques tels que des NFT[316]). Pour des raisons de lisibilité et de compréhension, cette étude fait référence au terme de blockchain dans son acceptation générale et grand public, excepté lorsque des précisions sont nécessaires pour aborder certains concepts précis, tout particulièrement concernant certaines variantes informatiques que représentent les blockchains publiques, privées ou hybrides expliquées ci-après. Depuis 2020, il est noté que l'AFNOR a mis en place des groupes de travail ainsi qu'une norme sémantique optionnelle pour fournir un vocabulaire commun en français pour de nombreux termes associés à cette technologie 3.0[317]. La technologie blockchain est apparue peu de temps après la révolution d'Internet, ce qui suppose qu'elle est une forme d'héritage technologique en dépit de nombreuses différences[318]. Internet prône initialement un accès gratuit, instantané et anonyme à des informations centralisées sur des serveurs, et la technologie blockchain propose de décentraliser de façon universelle les données afin d'assurer une intégrité et une gestion souveraine, voire optimisée des utilisateurs sur celles-ci. Pour bien comprendre comment la technologie blockchain depuis sa première

[315] V. Annexe 3, Focus 1 à 3.

[316] Il est fait référence au « *jeton numérique non fongible - JNF* » ou « *Non Fungible Tokens - NFT* » qui peuvent selon les contextes prolonger l'existence d'un bien physique au sein de l'univers numérique grâce à des méthodes/standards/propriétés cryptographiques propres à certaines blokchains. La façon la plus simple de décrire les NFT est de les comparer à des posters signés de votre artiste préféré. Par exemple, vous aimez un artiste qui a créé un poster de sa dernière œuvre. Il vient d'émettre 50 exemplaires de ce poster avec sa signature manuscrite, il s'agit donc d'une série unique. Lorsque vous achetez un NFT, vous achetez l'un de ces 50 exemplaires. Pourtant, sur internet, vous pouvez toujours télécharger une copie en quelques clics. Mais ce n'est pas celle qui porte sa signature numérique, et ce n'est pas celle qui porte un numéro de série. Vous n'achetez pas le droit d'auteur de son œuvre, mais vous achetez une copie de l'œuvre signée par l'artiste. Initiés sur la blockchain Ethereum en 2015, il existe en 2022 trois principaux types de *JNF* : (i) les *ERC-20* qui sont des jetons fongibles, tous du même type pour un même contrat intelligent, (ii) les *ERC-721* dont chaque jeton est unique et correspond à un ou plusieurs actifs sous-jacents, (iii) les *EIP-2981* ou plus récemment les *EIP-4907* qui représentent une « norme NFT » pour le paiement de redevances à destination des auteurs lors de transferts entre des propriétaires ultérieurs. Notons qu'en 2023 un nouveau type de NFT devrait être proposé par les développeurs Ethereum (dont Vitalik Buterin) : les *« Soul Bound Token (SBT)* » dont l'objectif est de prouver via l'envoi de jetons *SBT* sur une adresse ethereum la preuve d'une qualité (révocable). Les *SBT* jouent ainsi le rôle d'un certificat dont la particularité réside dans leurs révocations par chaque émetteur : lorsqu'un *SBT* est envoyé sur une adresse, seul son émetteur peut le révoquer et non pas son titulaire et destinataire. Dès lors, un *SBT* pourrait remplir le même objectif qu'une *attestation vérifiable* en sachant que tous deux peuvent implémenter le *ZKP* et donc être en conformité avec le RGPD. Ainsi, RGPD et blockchains publiques sont compatibles à la condition que des mécanismes cryptographiques adéquats permettent aux utilisateurs de conserver un haut degré de maîtrise, de transparence et de confiance sur leurs données.

[317] Voir les travaux de la Commission de normalisation Blockchain, AFNOR/CN, liste des membres (sept. 2022) disponible à l'adresse suivante

[318] Il est fait référence aux standards techniques utilisés, qui diffèrent dans leurs implémentations bien qu'ils trouvent souvent une origine commune.

apparition en ligne en octobre 2008[319] puis sa mise en service en 2009[320] s'est inscrite comme application sous-jacente à Internet, il convient ci-après d'évoquer sa genèse.

2.3.1 Un nouveau type de transaction pour l'émergence d'un Internet de confiance

Depuis 2015, la technologie blockchain connaît une adoption ainsi qu'un intérêt croissant auprès de nombreux acteurs des secteurs publics et privés[321]. La diversité de ces technologies permet effectivement de répondre à de nouveaux besoins sectoriels[322] de façon accessible, transparente, efficace et automatisée. Lors de l'apparition de Bitcoin en 2009, cette première application fiable d'une monnaie cryptographique était indissociable de sa technologie blockchain sous-jacente. Ce n'est qu'à partir de 2015[323] et 2016[324] qu'une séparation conceptuelle de Bitcoin et de sa technologie blockchain émerge dans les mentalités[325]. A partir de cette période, Bitcoin a incarné puis démontré qu'il était pour la première fois possible dans l'univers numérique d'effectuer des transactions de valeur unique et sans que cette dernière soit altérée, c'est-à-dire systématiquement dupliquée. Pour exemple, lorsqu'une personne envoie une carte postale à une autre personne, elle ne possède plus cette carte postale. Lorsqu'une personne envoie un courriel, une image, un message ou encore un document sur Internet, elle les possède toujours sur son ordinateur ou téléphone, seule une copie est envoyée à son destinataire. Cette analogie résume le plus grand défi du numérique auquel Bitcoin[326] a répondu : permettre de réaliser des transactions en ligne tout en attribuant et incarnant une rareté numérique en garantissant une unicité, une authenticité et une intégrité totale de la donnée échangée. Cette même rareté cryptographiquement programmée permet ainsi de désigner et de supposer que la technologie blockchain permettrait un nouvel Internet de la valeur. A ce jour, la blockchain Bitcoin représente également le système informatique le plus sécurisé au monde[327], source d'une confiance numérique inédite, notamment en raison de sa

[319] Le livre blanc (« *White Paper* ») de Bitcoin a été publié par *Satoshi Nakamoto* sur la liste de diffusion *metzdowd.com* le 31 octobre 2008, *v.* « Bitcoin: A Peer-to-Peer Electronic Cash System », disponible à l'adresse suivante
[320] Le premier bloc de transaction de données de la blockchain Bitcoin, aussi nommé Bloc Genesis, a été créé le 3 janvier 2009 à 18h15.
[321] LITAN Avivah, « Hype Cycle for Blockchain 2021; More Action than Hype », in *Gartner.com*, publié le 14 juillet 2021, disponible en ligne et consulté le 16 juillet 2021 ; *v.* également « The strategic business value of the blockchain market | McKinsey », consulté le 16 juillet 2021.
[322] CARSON, Brant, et al. « Blockchain beyond the hype: What is the strategic business value? », McKinsey & Company. 2020. Disponible à l'adresse suivante
[323] Le concept de blockchain, dissociée de son origine (Bitcoin), est apparu en 2015 dans un article de promotion de Bloomberg par Blythe Masters une ancienne cadre britannique de la banque JPMorgan Chase.
[324] Bitcoin est le premier réseau informatique décentralisé à grande échelle et a permis de faire naître d'autres réseaux distribués de nature similaire, mais de fonctionnement plus ou moins différent. Comme l'admet le rapport EU Blockchain Observatory and Forum, il y a eu un « avant » et un « après » Bitcoin : « Les protocoles de consensus peuvent être divisés en deux grandes familles [...] : Ceux qui existaient avant Bitcoin, le consensus basé sur le système Byzantin ; ceux qui n'existent qu'après Bitcoin, famille du consensus de Nakamoto », p.51.
[325] Pour démontrer cela, consultez le nombre de recherche de 2010 à ce jour (sur Google Trend) - des termes « Bitcoin » et « Blockchain » qui possèdent une tendance de recherche similaire au regard de leur indissociabilité initiale (avant 2015).
[326] V. Annexe 3
[327] DELAHAYE Jean-Paul, « Table Ronde du Cercle du Coin : preuve de travail et écologie », consulté en ligne le 12 août 2021, intervention de Jean-Paul Delahaye, informaticien, mathématicien et professeur à l'Université de Lille : « Le calcul qui est

caractéristique anti-fragile[328]. En plus de l'introduction de ce nouveau paradigme de rareté numérique, ces transactions en ligne s'échangent sans nécessairement recourir à des intermédiaires de confiance numérique, dont l'activité principale se résume traditionnellement à vérifier qui envoie quoi, à qui, et comment en contrepartie d'un coût significatif et parfois accompagné d'une lenteur administrative ou encore d'une relative opacité de gestion.

La technologie blockchain propose en effet une solution de confiance mathématique et algorithmique[329] en principe accessible, autonome, durable, sécurisée, quasi gratuite et sans contraintes géographiques. Une nouvelle (crypto)économie numérique de la confiance, impliquant un rôle réduit des intermédiaires centralisés, semble progressivement émerger. Parce que la confiance se crée par la transparence et que la confiance est l'oxygène de l'univers numérique, il convient que cette transparence algorithmique de la technologie blockchain soit compréhensible de tous et non pas seulement des développeurs du Web 3.0[330], comme cela est aujourd'hui majoritairement le cas au sein des écosystèmes blockchains. L'auteure et scientifique Aurélie Jean explique que « *la confiance est un sentiment d'un être humain envers un autre être humain uniquement. Parler de confiance envers un algorithme fait entrer l'utilisateur dans une vision floue des responsabilités de celui-là* »[331]. Si cela est particulièrement vrai pour les algorithmes d'intelligence artificielle, cette réflexion doit est renversée concernant les algorithmes blockchains dont la confiance se veut en principe et par conception plus ouverte, accessible et transparente. Pour anticipation de la partie suivante de cette étude, les blockchains d'entreprises (fermées) et les blockchains publiques (ouvertes) sont deux types de blockchains, chacune avec ses propres avantages et inconvénients. Les premières sont généralement privées et contrôlées par une organisation ou un groupe d'entités, tandis que les deuxièmes sont en théorie ouvertes à tous et contrôlées par tous ses utilisateurs. Les blockchains d'entreprises peuvent offrir une plus grande flexibilité et un contrôle pour les organisations qui les utilisent, ce qui les rend adaptables pour de nombreuses utilisations différentes. Les blockchains publiques ont également leur utilité. Elles sont généralement considérées comme plus sécurisées que les blockchains d'entreprises en raison de leurs structures et du nombre de parties prenantes qui les utilisent. De plus, les blockchains publiques sont utilisées pour leurs crypto-actifs, comme le bitcoin, en raison de leur capacité à gérer avec fiabilité des transactions financières. Nous observons que la technologie blockchain est une base de données supposée décentralisée fonctionnant comme un réseau informatique en réalité organique dont « *l'effet de*

réalisé pour inclure de nouvelle page [de transactions] dans la blockchain Bitcoin en fait un objet informatique extraordinaire et inégalé dans le monde » ; *v.* également la vidéo « Bitcoin Tout Puissant », 1er avril 2022 sur YouTube, consulté le 18 octobre 2022, à l'adresse suivante

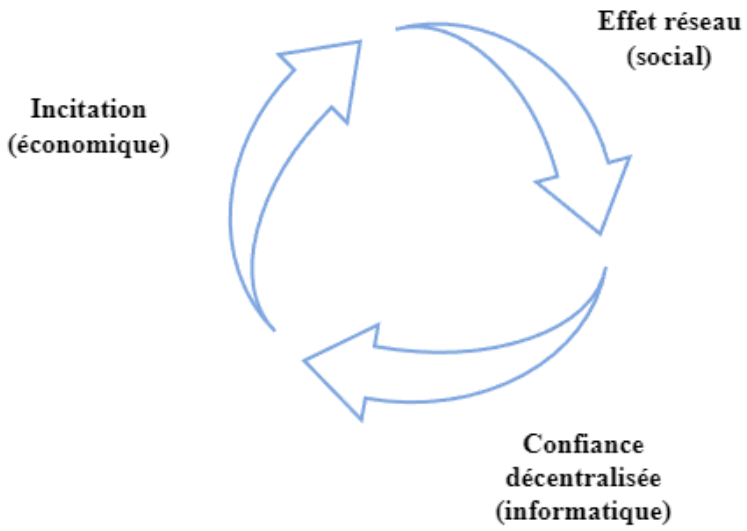
[328] TALEB Nassim, « Antifragile: things that gain from disorder », Random House, 2012, p.430.

[329] LASSEGUE Jean, GARAPON Antoine, « *Justice digitale* », *op. cit.*, Ed. PUF, p.153, « On comprend aisément l'espoir que peut soulever une telle trust machine, une 'machine à produire de la confiance', tant la confiance est un enjeu central de toute relation humaine, qu'elle soit affective, commerciale ou politique ».

[330] Chaque mois, plus de 23 000 développeurs recensés participent activement aux projets publics du Web 3.0, ce qui correspond au nombre total d'employés techniques actuels d'Alphabet ou de Meta, deux entreprises qui réduisent leurs effectifs depuis fin 2022, *v.* GitHub

[331] JEAN Aurélie, « *Les algorithmes font-ils la loi ?* », in *Humensis*, 2021, *op. cit.*, position de lecture dans le livre : 69%.

réseau »[332] et la communauté sont deux fondements indissociables. En effet, « *pour qu'une blockchain soit décentralisée, il est d'une importance cruciale que les utilisateurs standards puissent opérer un nœud* [du réseau] *et qu'il existe une culture suffisante* [dans cette communauté] *pour qu'opérer des nœuds soit une activité courante* »[333]. Par conséquent, il semble possible d'illustrer les fondements d'une blockchain ouverte d'après les relations et synergies suivantes : une incitation économique engendre un effet de réseau social qui débouche sur une confiance numérique renforçant elle-même cette première incitation économique, et ainsi de suite (*v.* illustration suivante).



La technologie de la blockchain assure en principe une résistance maximale aux pertes ou altérations de données potentielles, car toutes les données échangées sont copiées et accessibles sur chaque ordinateur du réseau et elles ne peuvent être altérées ou supprimées sans la validation de tout ou partie des autres ordinateurs de ce même réseau. Par conséquent, si une machine est corrompue, elle peut être isolée sans que le réseau principal soit mis hors ligne ou en maintenance pour les utilisateurs d'une blockchain. Cette résilience théorique des blockchains en fait un outil de choix pour les entreprises souhaitant favoriser des collaborations internes et externes à leur organisation tout en partageant de façon simple, rapide, sécurisée et immuable, leurs informations et données. Cependant, l'immuabilité des blocs et des transactions d'une blockchain dépend étroitement de son niveau de décentralisation, qui englobe par exemple le nombre et la localisation des ordinateurs dédiés, ainsi que le consensus utilisé pour leur communication. Ainsi, il est supposé que seule la blockchain Bitcoin tend aujourd'hui vers un degré de décentralisation pure comme cela est exposé ultérieurement dans cette étude. Si cette décentralisation à tout prix n'a pas nécessairement de caractère essentiel pour le cas d'usage de l'identité numérique, il

[332] Terme popularisé par Robert Metcalfe avec sa théorie de l'effet réseau ou « loi de Metcalfe ».
[333] BUTERIN Vitalik, traduit librement de l'anglais, « The Limits to Blockchain Scalability », consulté en ligne le 6 décembre 2021.

prend tout son sens concernant la notion de monnaie numérique également étudié dans la seconde partie de cette recherche.

2.3.1.1 La blockchain, une technologie pour de multiples procédés et applications

La technologie blockchain peut permettre de répondre à divers enjeux d'innovation sectoriels et métiers tels que les services financiers (« tokenisation » de parts de société)[334], les transports et la logistique (traçabilité numérique de biens physiques), les secteurs publics (e-gouvernement et institutions augmentées), l'assurance (assurance fiable, transparente et instantanée) ou l'identité numérique décentralisée (identité numérique de citoyens, d'entreprises ou même d'objets connectés, possiblement basés sur une blockchain)[335]. Comme l'explique le fondateur de la blockchain Ethereum Vitalik Buterin : « *Il y a largement de la place pour des dispositifs blockchains qui n'impliquent pas que de la* [crypto]*monnaie, et en effet nous avons besoin de plus d'entre eux* »[336]. En effet, la blockchain abrite et regroupe de nombreuses versions technologiques, de la même façon qu'Internet fait aujourd'hui fonctionner et héberge de multiples technologies (intelligence artificielle, objets connectés) et applications (courriels, réseaux sociaux, intranets d'entreprises)[337]. À titre d'exemple, de nombreux acteurs sont déjà impliqués dans l'utilisation de ces réseaux numériques pairs à pairs et décentralisés, notamment en matière de crypto-actifs, de cybersécurité, de traçabilité des biens physiques, de réalité virtuelle avec des identités décentralisées (v. Métavers), de gestion de l'Internet des objets (IdO/IoT) ou encore de création de contrats intelligents (v. AEC) et d'organisations autonomes décentralisées (v. DAO), des sujets étudiés dans des parties dédiées. Il apparaît important de reconnaître la variété des modèles de gouvernance possibles pour chaque infrastructure blockchain, qui peut être classée en trois catégories d'infrastructures, celles ouvertes et décentralisées, celles fermées et privées qui sont centralisées, et celles hybrides à la fois ouvertes et fermées donc considérées comme semi-décentralisées. C'est pourquoi il existe aujourd'hui autant de technologies de registres distribués, que d'écosystèmes et d'acteurs qui lui sont rattachés (v. Annexes 6 et 7). Le grand intérêt que portent de nombreuses entreprises pour la blockchain et pour sa mise en œuvre conséquentes à différentes applications, a donné lieu à de nombreuses tentatives d'adaptation de cette technologie. A ce titre, des précisions essentielles doivent être effectuées concernant (i) les blockchains de type publiques, (ii) les blockchains de type consortiums ou hybrides et (iii) les blockchains de type privées :

[334] La *tokenisation* des actifs consiste à transposer des caractéristiques intrinsèques et spécifiques à la technologie blockchain – sécurité, immuabilité, rapidité, transparence, unicité – à des actifs tangibles (biens immeubles, biens meubles) ou intangibles (parts sociales, caractéristiques d'un personnage dans un jeu vidéo). Concrètement, il est possible de transférer, d'immobiliser ou encore de diviser des représentations virtuelles uniques de ces actifs.
[335] « Elle [la blockchain] propose […] une alternative à la mission également essentielle de conférer une identité (état civil), de certifier la propriété (cadastre) ou encore de garantir les diplômes. », *op. cit.*, « Justice digitale », Ed. PUF, p.152.
[336] BUTERIN Vitalik, « On Nathan Schneider on the limits of cryptoeconomics », 26 septembre 2021. *vitalik.ca*. Consulté le 4 avril 2022, à l'adresse suivante
[337] « La blockchain permet d'identifier, d'immatriculer, donc de certifier l'identité dans un espace déterritorialisé », *op. cit.*, « Justice digitale ». p.140.

(i) Au sein d'une *blockchain publique*, tous les utilisateurs pseudo-anonymes peuvent en théorie envoyer, recevoir et voir l'historique des transactions ou encore participer à la mise à jour de la blockchain (notamment à son algorithme de consensus et à son processus d'émission de crypto-actifs désigné par le terme et concept de « *minage* »)[338]. L'utilisateur d'une blockchain publique n'a pas besoin d'autorisation auprès d'un tiers afin de réaliser des opérations sur ladite infrastructure sur laquelle la collaboration est libre et visible pour tous. Pour les juristes, une blockchain publique peut être perçue comme une forme de contrat d'adhésion[339], ce qui signifie qu'un utilisateur adhère ou non au système tel qu'il est conçu et qu'il ne peut en théorie pas le modifier sans l'accord d'une majorité de tous les acteurs de cette blockchain. En pratique, Bitcoin est l'étalon des blockchains publiques et modifier sa conception informatique relève d'un parcours du combattant[340].

(ii) Contrairement à une blockchain accessible au public, une *blockchain* de *consortium* ou *hybride*, également appelée blockchain d'entreprise, limite l'accès aux données en écriture, mais les rend disponibles en lecture. Cette forme de blockchain pourrait être juridiquement entendue à tout le moins comme un contrat consensuel[341], dans lequel les conditions et les limitations sont négociées entre un petit nombre d'acteurs/utilisateurs dûment identifiés et qui ont mutuellement confiance. Ici, le système blockchain n'est donc plus complètement décentralisé sur le plan informatique et/ou social (*v*. Annexes 7), ce qui signifie que la confiance numérique lui étant attribuée par ses utilisateurs repose sur un ou plusieurs tiers de confiance publics et/ou privés, généralement un groupe d'institutions et de prestataires. Au sein d'une blockchain hybride, seuls les membres du groupe des personnes autorisées peuvent participer au processus de recherche de consensus (gouvernance). L'historique de la blockchain peut être rendu accessible soit à tous les utilisateurs, soit à un ou plusieurs groupes spécifiques. A titre d'illustration, la blockchain Hyperledger Indy[342] atteint un consensus optimal lorsque 25 nœuds et ordinateurs sont opérationnels (ce qui est très peu comparé aux blockchains publiques), et au minimum 8 nœuds sur 25 devant être fonctionnels afin d'assurer la relative résilience informatique de la blockchain déployée[343].

---

[338] V. Annexe 6, Focus 1.

[339] Art. 1110 al. 2 du Code civil : « le contrat d'adhésion est celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties ».

[340] V. Annexe 3, Focus 1 à 4. S'il est mathématiquement impossible de falsifier des transactions sur Bitcoin, l'une des failles possibles réside dans sa communauté de développeurs-bénévoles qui propose de nombreuses mises à jour logicielles du protocole (*Bitcoin Improvement Proposal - BIP*) depuis 2009. Un acteur malveillant pourrait ainsi tenter de soumettre un BIP malicieux à la communauté de développeurs-bénévoles qui, s'ils l'acceptent, pourrait introduire des failles programmées (« back doors ») au sein du protocole. Notons que ce type d'attaque relève principalement de conjonctures politiques et théoriques, très rarement constaté en pratique.

[341] Art. 1109 du Code civil, dans sa version en vigueur depuis le 1er octobre 2016, qui dispose : « Le contrat est consensuel lorsqu'il se forme par le seul échange des consentements quel qu'en soit le mode d'expression (…) ».

[342] Hyperledger Foundation. Hyperledger Indy. Consulté le 29 septembre 2022, à l'adresse suivante

[343] V. *Learningthings.online*, « Introduction to Hyperledger Sovereign Identity, Blockchain Solutions », consulté en ligne le 14/10/2021.

En 2022, cette même infrastructure (Hyperledger), qui est massivement utilisée pour des cas d'usage d'identité numérique décentralisée a été partiellement critiquée pour son manque de décentralisation[344] : « *il est intéressant de noter […] que le point idéal est de 25 nœuds - robustes, capables de survivre à la défaillance de huit nœuds, mais suffisamment rapide pour supporter le nombre attendu de transactions d'écriture sur le réseau - de l'ordre de centaines de transactions par seconde* ». Ces explications techniques sont approfondies dans une partie dédiée aux défis actuels des technologies blockchains. Néanmoins, depuis fin 2022[345], force est de constater que quinze grands acteurs du secteur de l'assurance ont décidé de mettre fin à leur projet commun de blockchain consortium, notamment par manque de connaissances et de débouchés. De même, une autre blockchain de consortium créée en 2017 a annoncé cesser son activité en novembre 2022[346]. En effet, il semble extrêmement difficile, voire impossible, d'amener toujours plus d'acteurs d'un secteur et d'une blockchain hybride, à collaborer dans un temps long (les gains de productivité à long terme sont compensés par une gouvernance parfois jugée trop complexe par rapport aux méthodes de collaboration traditionnelles et bilatérales)[347].

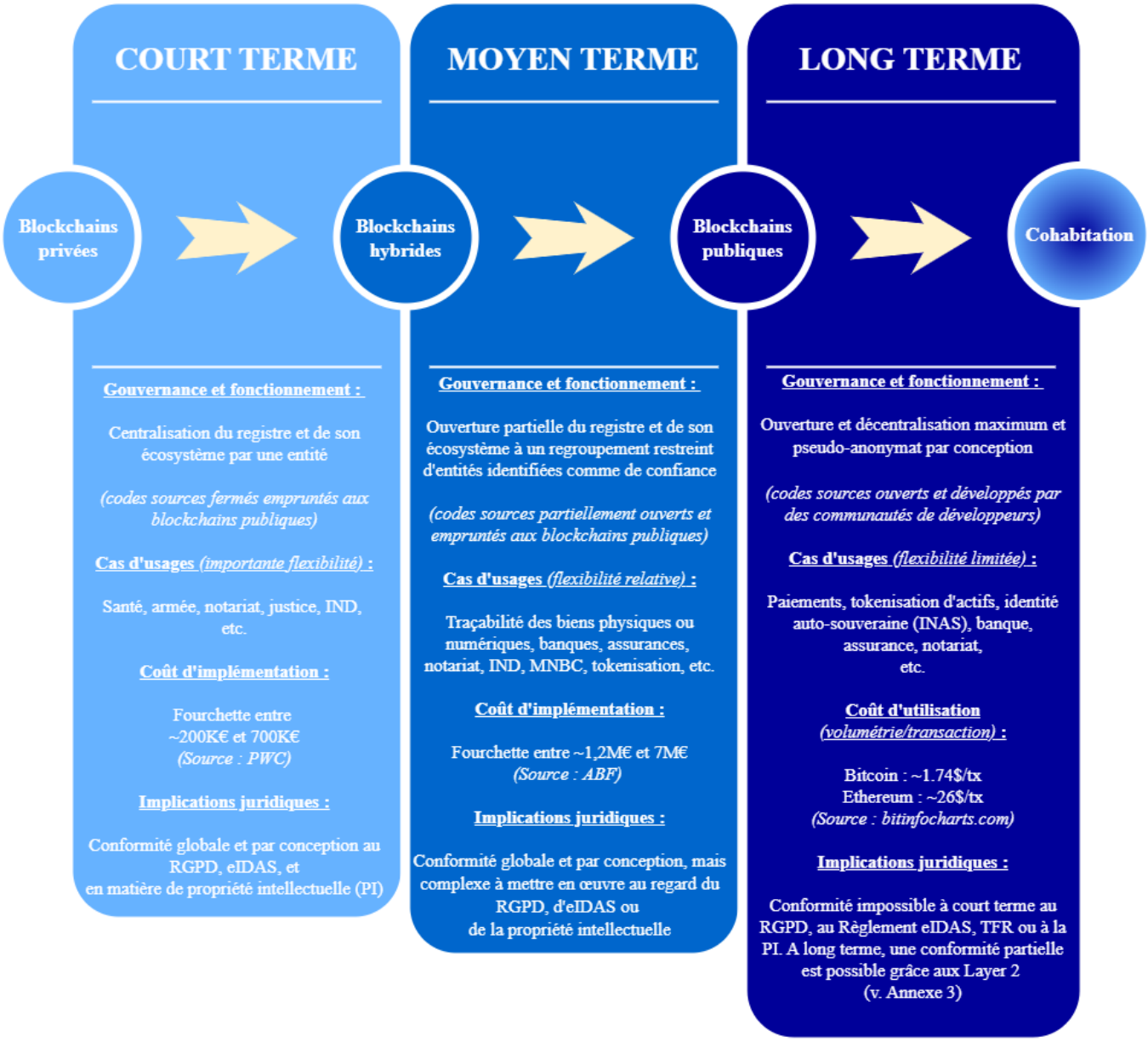
(iii) Dans le cas d'une *blockchain privée*, les informations et les autorisations des utilisateurs sont entièrement encadrées et ne sont pas libres comme pour les blockchains publiques, ni partiellement décidées par un consortium restreint d'acteurs, comme c'est le cas pour les blockchains hybrides. En principe, une blockchain privée est développée par un unique acteur qui désire en garder le contrôle. Dans une blockchain privée, l'historique des transactions n'est plus transparent pour les tiers, mais uniquement accessible à l'administrateur (généralement seul) de la blockchain en question. L'autorisation de mettre à jour la blockchain et de créer des transactions est ainsi limitée et contrôlée par ce même acteur, ce qui fait d'une blockchain privée une forme de contrat unilatéral pour ses utilisateurs au visa des dispositions du Code civil[348]. Ce contrôle absolu par un tiers totalement centralisé fait que les modifications du logiciel sont plus simples et plus rapides à réaliser. Cependant, certaines caractéristiques (attribuables aux blockchains publiques et parfois de consortiums) telles que l'immuabilité et la décentralisation des opérations

[344] YOUNG Kaliya, « Being 'Real' about hyperledger Indy & Aries / Anoncreds », 7 septembre 2022, in *Identity Woman*. Consulté le 12 septembre 2022, à l'adresse suivante
[345] VIVIANI Mathieu, 12 août 2022, « Blockchain : une quinzaine de grands assureurs internationaux jettent l'éponge », in *Les Echos*. Disponible à l'adresse suivante
[346] « IBM, Maersk shutter shipping blockchain TradeLens », 30 novembre 2022, in *Ledger Insights - blockchain for business*. Disponible à l'adresse suivante
[347] « Selon une étude menée fin 2019, l'ère des blockchains privées toucherait même à sa fin et l'avenir appartiendrait aux plateformes privées bâties au-dessus de blockchains publiques, des sortes de surcouches que certaines entreprises proposent déjà. (…) Les toutes nouvelles solutions en matière de blockchains publiques permettent aux entreprises d'exploiter ces dernières, tout en garantissant la confidentialité des données. Il semblerait que l'avenir soit dans cette sécurisation des blockchains publiques », *op. cit.*, « Tout savoir sur le Bitcoin et les cryptomonnaies », p.15.
[348] Art. 1103 du Code civil, dans sa version en vigueur depuis le 1er octobre 2016, qui dispose « les contrats légalement formés tiennent lieu de lois à ceux qui les ont faits ».

peuvent être remises en question, impliquant ainsi une confiance moindre en ces registres pour les utilisateurs désireux d'utiliser des systèmes ouverts et décentralisés. Il est finalement constaté que si une blockchain privée est en réalité un regroupement de serveurs centralisés sous l'autorité d'une même entité, dont seuls les fondements informatiques et algorithmiques sont modifiés par rapport à des serveurs classiques, un tel système est ici supposé conforme au droit puisque son entité administratrice l'est généralement à l'origine (société légalement formée, etc.).

Lorsqu'une blockchain est publique, privée ou hybride, les consensus informatiques utilisés ne sont pas nécessairement les mêmes comme le démontre une Annexe dédiée[349]. Chaque type de blockchain a donc ses propres avantages et inconvénients, qui ont des effets plus ou moins importants selon le(s) domaine(s) d'application. En ce sens, une blockchain privée peut avoir pour vocation de devenir une blockchain de consortium, mais une blockchain de consortium n'a pas pour vocation à devenir une blockchain privée. Dans les deux cas, ni une blockchain privée ni une blockchain consortium ne semblent être en mesure de devenir une blockchain publique, car les blockchains publiques préexistantes bénéficient d'un effet de réseau, d'une expérience technique et d'une confiance plus importante et supposés inégalables sur le long terme[350]. Ce caractère plus ou moins ouvert de chaque type de blockchain rappelle un affrontement bien connu des pionniers d'Internet, celui des logiciels propriétaires contre les logiciels libres qui sont étudiées dans une partie dédiée[351]. Certains spécialistes de l'écosystème blockchain français estiment que les blockchains privées ou hybrides, sans jeton universel ou artificiel associé, ne permettent « (…) *de ne fournir qu'un gain opérationnel marginal au prix de coûts souvent très importants* (…) »[352]. Bien que cette réflexion puisse être pertinente pour les secteurs financiers, elle ne s'applique pas nécessairement au marché de l'identité numérique. En effet, contrairement à ces secteurs, la financiarisation par des jetons virtuels ou crypto-actifs n'est pas encore envisagée à court terme par la majorité des acteurs de l'identité numérique.

[349] V. Annexe 6, Focus 1 à 3.
[350] BABEAU Olivier, Président de l'Institut Sapiens et Professeur en sciences de gestion à l'Université de Bordeaux, explique que « L'effet de réseau est le nouveau paradigme du monopole » in *Le nouveau désordre du numérique : comment le digital fait exploser les inégalités*, Ed. Buchet-Chastel, 2020, 267p.
[351] V, *infra*, II, Titre 1, 1.5.3.1
[352] STACHTCHENKO Alexandre. 11 janvier 2022. « Manuel de survie dans la jungle des poncifs anti-Bitcoin » (version longue consultée en ligne le 12/01/2022).



Le schéma présenté ci-dessus permet d'évaluer l'adéquation de chaque type de blockchain en fonction de différents cas d'utilisation à travers le temps. Il est d'abord possible de supposer que les blockchains privées et hybrides ne sont que des versions technologiques temporaires destinées à être utilisées en attendant que les blockchains publiques puissent répondre à certains des défis informatiques, sociaux et juridiques étudiés tout au long de cette recherche. Pour les protocoles décentralisés, ouverts et publics, l'espoir de ce scénario consiste à répondre à ces défis grâce à l'implémentation future et successive de protocoles dits de seconde couche (« Layer 2 – L2 »)[353], des solutions pour l'instant plus centralisées que décentralisées. Ainsi, le débat des blockchains publiques versus privées n'aurait plus lieu d'être dans le cas où ces implémentations sous-jacentes (L2) deviendraient réalité, car ces blockchains

[353] V. Annexe 3, Focus 4.

publiques toujours décentralisées seraient désormais interconnectées à des protocoles solutionnant ces défis. En effet, la semi-centralisation plus importante de ces protocoles de relais rendrait possible une certaine flexibilité permettant aux entreprises leur participation informatique à ces protocoles ouverts, en conformité juridique et énergétique (v. Annexe 6) correspondant aux attentes sociétales. En attendant cette hypothétique réalité, à court et moyen termes, une entreprise n'a d'autres choix que de privilégier les blockchains privées et hybrides pour certains domaines, car les blockchains publiques ne proposent pour l'heure aucune solution viable aux problématiques suivantes auxquelles elles se confrontent depuis 2015 sur un plan informatique :

(i) Le temps de réponse par transaction d'une blockchain est-il suffisant (de l'ordre de la milliseconde comme pour un serveur ou bien de plusieurs secondes ou minutes, comme pour une blockchain publique) ?

(ii) Le coût par transaction est-il raisonnable (quasiment nul pour un serveur mais très important sur une blockchain publique) ?

(iii) La blockchain accepte-t-elle une capacité de charge suffisante en cas de forte sollicitation du réseau par ses utilisateurs (un système de redondance est-il envisagé) ?

(iv) L'effort nécessaire pour que ledit système informatique soit conforme aux règles de droit est-il possible et dans quelles mesures ?

En octobre 2022, Google a lancé une nouvelle solution appelée « *Blockchain Node Engine* »[354] qui propose un service d'hébergement de nœuds blockchains entièrement géré et destiné aux organisations souhaitant développer des cas d'utilisation sectoriels (partiellement décentralisés). Bien que cette solution puisse intéresser des organisations telles que l'ABF ou l'EBSI précitées, elle semble contradictoire avec l'objectif de souveraineté européenne et de ses Règlements (Data Act, eIDAS, étudiés plus loin). En pratique, les entreprises du Web 3.0 qui ont besoin de nœuds dédiés peuvent relayer des transactions, déployer des contrats intelligents et lire ou écrire des données issues d'une blockchain, avec la fiabilité, les performances et la sécurité qu'elles attendent de l'infrastructure de calcul et de réseau rattaché au service Google Cloud. Ethereum[355] sera la première blockchain publique prise en charge par ce nouveau service et permettra aux développeurs de fournir des nœuds Ethereum clés en main et entièrement gérés avec un accès sécurisé à la blockchain. Remarquons qu'une autre société américaine, Amazon, propose un service concurrent depuis 2019[356]. A long terme, nous supposons que certaines blockchains publiques, telles que Bitcoin ou encore Ethereum, auront les capacités techniques d'héberger certains cas d'usage du secteur de l'identité numérique (v. INAS). Ainsi, la technologie blockchain devrait globalement continuer à se développer puis à prospérer, face à un environnement qui

[354] ZAVERY Amit, TROMANS James, « Introducing Blockchain Node Engine: fully managed node-hosting for Web3 development », 27 octobre 2022, in *Google Cloud Blog*. Disponible à l'adresse suivante
[355] V. Annexe 6, Focus 2.
[356] « Amazon Managed Blockchain Pricing », in *Amazon Web Services (AWS)*, Inc. Consulté le 27 octobre 2022, à l'adresse suivante

se digitalise progressivement et dans lequel les notions de dépendance et de confiance numérique concernent de plus en plus d'entreprises, d'institutions et de citoyens. Cependant, depuis 2021, de nombreuses préoccupations ressurgissent concernant la consommation énergétique des blockchains. Si les blockchains privées et hybrides consomment moins d'énergie que les blockchains publiques tel que Bitcoin, car elles ont des nœuds de validation connus et identifiés ce qui évite les calculs mathématiques nécessaires pour vérifier l'authenticité d'un acteur et valider une transaction, il est important de ne pas méjuger les blockchains publiques sans examiner attentivement les impacts énergétiques réels de leurs activités informatiques[357]. Ces impacts peuvent être plus complexes et surprenants qu'il n'y paraît. Finalement, cette étude évoque seulement certains cas d'usage relatif à la technologie blockchain et à l'identité numérique. Elle n'ambitionne pas de fournir une analyse segmentée par cas d'usage, mais plutôt de fournir une vision transversale de certaines de ses applications au regard des nombreux enjeux liés à l'identité numérique centralisée et décentralisée.

2.3.1.1.a Les crypto-actifs

Certains scientifiques comme le célèbre économiste américain Milton Friedman avaient anticipé l'ère des devises virtuelles dès 1999[358]. Désignés par le terme de crypto-monnaies ou de crypto-actifs, et par le terme d'actifs numériques dans notre droit positif[359], ces mots presque courants aujourd'hui regroupent une multitude de jetons virtuels, c'est-à-dire des *tokens* adossés à des blockchains ouvertes. Initialement, ces objets virtuels ont été créés pour protéger les infrastructures blockchains contre les attaques de spammeurs qui cherchaient à les surcharger en effectuant de multiples transactions. Cependant, en raison de leur valeur fluctuante, influencée par des facteurs tels que l'offre et la demande de jetons, l'infrastructure informatique sous-jacente et les campagnes mercatiques massives, ces jetons numériques sont progressivement devenus des objets d'utilisation particulièrement spéculatifs. En d'autres termes, comme l'explique le fondateur de la blockchain Ethereum, Vitalik Buterin déjà cité : « *la crypto économie consiste à essayer de réduire les risques liés à la confiance sociale en créant des systèmes dans lesquels nous introduisons des incitations économiques explicites pour les bons comportements et des pénalités économiques pour les mauvais comportements* »[360] tandis que

[357] V. Annexe 6, Focus 1.
[358] KRYPTOSPHERE®, « Milton Friedman avait prédit l'air des crypto-monnaies en 1999 ! », 2018, consulté en ligne le 13 janvier 2022.
[359] Loi n° 2019-486 du 22 mai 2019, dite PACTE, relative à la croissance et à la transformation des entreprises, pour une définition des actifs numériques, *v.* art. L.54-10-1 du CMF : « 1° Les jetons mentionnés à l'article L. 552-2, à l'exclusion de ceux remplissant les caractéristiques des instruments financiers mentionnés à l'article L. 211-1 et des bons de caisse mentionnés à l'article L. 223-1 ; 2° Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement ».
[360] « Governance, Part 2: plutocracy is still bad », 28 mars 2018, in *vitalik.ca*. Consulté le 1er avril 2022, à l'adresse suivante

d'autres évoquent la tyrannie des crypto-actifs[361]. Comme le suggère un regroupement de juristes spécialisés sur le sujet, le terme de crypto-actifs (écrit ici avec un tiret) est privilégié tout au long de cette recherche[362]. Dès lors, si ces multiples dénominations et leurs difficultés d'appréhension semblent montrer le potentiel applicatif de ce secteur, les actifs numériques sont introduits dans l'article L.54-10-1 du Code monétaire et financier : « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* »[363]. Il semble ainsi que les actifs numériques soient une catégorie d'actifs distincte des autres instruments financiers existants. En droit communautaire, un crypto-actif est qualifié par l'article 3(1)(2) du Règlement MiCA (étudié dans un chapitre ultérieur) en cours d'adoption, comme « *une représentation numérique d'une valeur ou d'un droit qui utilise la cryptographie pour sa sécurité et qui se présente sous la forme d'une pièce ou d'un jeton ou de tout autre support numérique qui peut être transféré et stocké électroniquement, en utilisant une technologie de registre électronique distribuée ou toute autre technologie similaire* »[364]. Jusqu'à 2019, les crypto-actifs étaient presque exclusivement perçus par les législateurs nationaux comme des instruments de fraudes, de blanchiment d'argent et de financement du terrorisme. Ce n'est qu'après que Facebook ait tenté sans succès d'émettre son propre crypto-actif stable, appelé à l'origine le « *Libra* », que le législateur européen a décidé de considérer sérieusement cet univers 3.0[365]. Si la France est en retard en matière d'adoption des crypto-actifs, aussi bien par les institutionnels que par le grand public comme le révèle en 2022 une étude internationale[366], il n'en demeure pas moins que le législateur français a fait preuve dès 2019 d'une importante capacité d'anticipation et d'innovation juridique les concernant au point d'en inspirer le droit communautaire à partir de 2020. Dans les faits, dès 2018, c'est la doctrine juridique suisse qui a établi une taxonomie précise et initiale spécifiquement dédiée aux différents types de crypto-actifs (voir ci-dessous)[367]. Très largement reprise par les régulateurs du monde entier, cette doctrine de l'Autorité fédérale de surveillance des marchés financiers suisses (FINMA)[368] a

[361] LARMAGNAC-MATHERON Octave, philosophe, « La tyrannie des cryptomonnaies », publié le 11 janvier 2022, in *Philosophie magazine*, disponible à l'adresse suivante
[362] BOUILLET-CORDONNIER Ghislaine et al. « La Finance Numérique, Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs », Ed. EFE, 2021, « Le terme actif numérique inséré dans le règlement général de l'AMF est à bannir au profit de celui de crypto-actifs. […] le terme [actif numérique] est source de confusion », p.146 (n°395), et « […] la notion de crypto-actifs est devenue hétérogène, regroupant des réalités très diverses. Ainsi, la définition légale qui en découle, précédemment évoquée, est devenue floue », et v. aussi « Monnaies, banques et finance : vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et Monétaire », in *Rapport de l'Assemblée nationale*, *op. cit*., p.11.
[363] Art. L 54-10-1 du CMF, Légifrance consulté le 28 juillet 2021 et *v*. également *infra*, II, Titre 2, 2.4
[364] RADLEY-GARDNER Oliver, BEALE Hugh, ZIMMERMANN Reinhard (dir.), librement traduit de l'anglais, Fundamental Texts On European Private Law : Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, en ligne, Hart Publishing, 2016, consulté le 4 mars 2022, p.59 et *v. infra*, I, Titre 2, 2.5
[365] V. infra, II, Titre 2, 2.4
[366] Bitstamp, « Crypto Pulse Report », 2022, pp.7-11. Disponible à l'adresse suivante
[367] BOUILLET-CORDONNIER Ghislaine, LANGLOIS-BERTHELOT Thibault, « Tour d'horizon du droit financier Suisse », en ligne, *op. cit*. Ed. EFE, 2021.
[368] Acronyme de Swiss Financial Market Supervisory Authority. V. Dictionnaire des acronymes

ultérieurement infusé dans de nombreux cadres législatifs, notamment en Europe et aux États-Unis. Cette nomenclature distingue[369] :

(i) Les jetons de paiement (« *payment tokens* »)

Cette première typologie de jetons caractérise les actifs numériques qui défraient régulièrement la chronique. Ils peuvent être définis comme de nouveaux moyens de réserve de valeur, d'échanges et de paiements rapides, sécurisés et sans intermédiaires ni frontières. Ils permettent l'achat de biens ou de services, mais ne confèrent pas de droit spécifique vis-à-vis d'un tiers émetteur : ils ne sont pas caractérisés comme des valeurs mobilières. Aux États-Unis, ce type de jetons (bitcoins, ethers) sera massivement adopté par les commerçants dans les cinq prochaines années d'après un rapport émanant de la société Deloitte en collaboration avec la société Paypal[370].

(ii) Les jetons d'utilité (« *utility tokens* »)

Ce type de jeton propose un accès a posteriori, en cas de levée de fonds en crypto-actifs pour développer un bien ou un service, à un produit ou à un service spécifique (accès à une application 3.0 et/ou à un bien physique). Ces jetons peuvent supposément être utilisés par les premiers investisseurs pour bénéficier d'avantages et de contreparties (comme des remises, des droits de vote) très avantageuses. Ce type de jeton d'utilité a pour vocation d'être utilisé au sein de l'écosystème et du projet développé par l'entreprise émettrice.

(iii) Les jetons d'investissement (« *security tokens – STO* »)

Les jetons d'investissement représentent une nouvelle classe d'actifs financiers auxquels sont notamment attachés des droits aux bénéfices. Ils reposent généralement sur des actifs tangibles ou encore intangibles. Par conséquent, les offres de jetons d'investissements sont en partie facilement sujettes à régulation, puisqu'ils représentent le prolongement numérique d'actes juridiques (attribution de parts de sociétés, de droits de vote). Les jetons d'investissement reproduisent numériquement, et avec les avantages intrinsèques précités de la technologie blockchain, des titres négociables ou non (actions, obligations, produits dérivés, parts sociales, participations à l'intéressement, intérêts) sur le marché primaire ou encore secondaire. Par conséquent, le droit suisse considère les jetons d'investissement comme des valeurs mobilières.

En pratique, de nombreuses entreprises du secteur technologique de la blockchain utilisent un ou plusieurs jetons pouvant caractériser à la fois des jetons de paiements, d'utilités et d'investissements. Dans ces cas, la qualification et l'encadrement juridique de ces derniers deviennent plus complexes à

[369] FINMA, « Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO) », 16 février 2018, p.7, disponible à l'adresse suivante

[370] CASTRO TANCO Claudina, « Merchants getting ready for crypto Merchant Adoption of Digital Currency Payments Survey Prepared in collaboration with PayPal », traduction libre de l'anglais « Environ 85 % des commerçants interrogés s'attendent à ce que les paiements en crypto-actifs soient omniprésents parmi les fournisseurs de leurs entreprises », pp.5-8, disponible en ligne à l'adresse suivante

interpréter pour les régulateurs. Les crypto-actifs sont révolutionnaires parce qu'ils permettent entre autres de transformer l'ordre établi, parfois de le bouleverser[371]. Comme cette étude le suggère pour le bitcoin[372], ces actifs cryptographiques permettent à leurs propriétaires de nouer ou de renouer avec une relative liberté financière, grâce à des mécanismes algorithmiques et mathématiques transparents. Cette confiance financière 3.0 est fondée sur l'idée selon laquelle lorsque chaque transaction est vérifiable sur une blockchain publique, il devient simple de faire confiance aux personnes et de s'engager dans des interactions *phygitales*. Ce nouveau souffle d'émancipation implique une nouvelle conception plus décentralisée et pair à pair de nos interactions sociales. Si ce nouveau courant culturel et mouvement social comporte certains risques (pertes des fonds, escroqueries) et certaines limites (gestion relativement complexe des clés cryptographiques), il s'agit pourtant d'effacer certains réflexes conservateurs pour tenter de comprendre et d'encadrer cette technologie qui est souvent comparée à l'avènement d'Internet. Il semble que le marché finira probablement par convaincre et faire évoluer les mentalités, un constat d'ores et déjà visible. L'évolution de la monnaie physique, vers une monnaie cryptographique serait ainsi un besoin sous-jacent à Internet. S'il faut admettre que la stratégie française en matière d'encadrement et d'adoption des crypto-actifs est politiquement, juridiquement et économiquement conservatrice, notamment en raison d'un lobby bancaire souvent défavorable à cette nouvelle classe d'actifs[373], il convient de ne pas transposer ce constat aux acteurs du marché de l'identité numérique décentralisée, car les rouages de ce secteur ne sont pas fondamentalement financiers. Bien que près de 70% des applications de la technologie blockchain concernaient en 2019 des cas d'usage financiers[374], d'autres cas d'usage émergent progressivement comme le souligne en 2021 l'un des huit co-fondateurs[375] de la blockchain Ethereum « *il est temps d'aller au-delà des applications de la finance* »[376]. Comme cela est étudié plus loin, l'identité décentralisée deviendra à terme aussi importante pour la monnaie numérique que pour l'identité numérique. En d'autres termes, il n'y aura plus besoin de multiples applications et portefeuilles numériques pour gérer les attributs (clés cryptographiques) de son identité, de ses relations et de son argent (cryptographique)[377]. Ainsi, la culture des crypto-actifs[378]

[371] MALABOU Catherine, « Les cryptomonnaies remettent en cause l'idée même d'Etat », philosophe et signataire de « la déclaration d'indépendance des cryptomonnaies », publié le 6 octobre 2020, in *Philosophie Magazine*.
[372] V. Annexe 3, Focus 4 à 6.
[373] PERSON Pierre, ancien député, 8 juin 2022, « on sous-estime le poids du lobby bancaire », « Il ne faut pas sous-estimer, en France, la force du lobby bancaire. Or, force est de constater qu'une partie de la haute fonction publique entretient des liens resserrés avec le secteur bancaire français. Il ne s'agit pas là de liens d'intérêts économiques directs ou individuels, mais surtout d'une incapacité à imaginer un monde différent lorsque toute une carrière s'est faite entre ces deux environnements. Il ne s'agit pas là de complotisme, que j'exècre. […] Ces derniers ne sont pas foncièrement opposés aux cryptos, mais cette logique décentralisée est contraire à leur construction intellectuelle », consulté le 9 juin 2022, à l'adresse suivante. Pour illustrer d'autres propos *v.* également « Droit de la finance numérique, blockchain, aspects fiscaux », EFE Edition, 2021, pp.147-151 (n°397-402) ⟨hal-03473371⟩.
[374] *Op. cit., v.* données publiques issues du site internet blockchainforgood.fr.
[375] La blockchain publique Ethereum et son écosystème a été initiée par huit co-fondateur dont Vitalik Buterin est le contributeur le plus emblématique à ce jour. Notons que ces personnes sont clairement connues et identifiées contrairement au(x) fondateur(s) de la blockchain publique Bitcoin.
[376] BUTERIN Vitalik, sur *Cryptoast*, en ligne, 2021, consulté le 4 août 2021.
[377] « L'argent n'avait pas d'odeur mais à présent il a une trace, et elle est indélébile », *op. cit.* GARAPON Antoine, LASSEGUE Jean, « Justice digitale ».
[378] « Pas vos clés [cryptographiques], pas votre argent [cryptographique] », librement traduit de l'expression anglophone très populaire dans l'univers des cryptos-actifs « not your keys, not your coins ».

repose sur l'autonomie financière et la gestion autonome des actifs financiers, et nous supposons que l'éthique et la culture de l'autonomie identitaire revendiquée par l'identité numérique auto-souveraine pourraient s'exprimer par le mantra « pas propriétaire de vos identifiants (DID), pas propriétaire de votre identité »[379]. S'il est aujourd'hui possible de distinguer les portefeuilles de crypto-actifs[380], des portefeuilles d'identité numérique décentralisée (PIND) étudiés au deuxième titre de notre étude, il est probable qu'à moyen terme ces deux types d'applications et de portefeuilles numériques fusionnent pour ne devenir plus qu'un. Notons qu'en matière de services sur crypto-actifs, l'application d'ici peu à l'échelle de l'UE du Règlement MiCA[381] aura pour effet d'imposer une nouvelle règle juridique, la « *travel rule* »[382], dont certaines exigences (juridiques et informatiques) pourraient constituer les standards de l'identité décentralisée, que tout désigne comme une solution adéquate en la matière. Le Règlement MiCA émane du fait que les crypto-actifs n'étaient pas couverts par la règlementation financière de l'Union européenne, cette absence de règles applicables aux services liés à ces actifs pouvant exposer les consommateurs et les investisseurs à certains risques. Il vise à soutenir l'innovation et la concurrence loyale en créant un cadre pour l'émission et la fourniture de services liés aux crypto-actifs. Par ailleurs, le sujet des crypto-actifs « stable », nommé des « *stablecoins* » étudiés plus loin, représente un défi juridique supplémentaire tant pour leurs consommateurs et utilisateurs que pour la Commission européenne et ses Etats membres dont la souveraineté monétaire peut être questionnée[383].

2.3.1.1.b La signature électronique et cryptographique

Une signature électronique peut être définie comme un ensemble de méthodes et de constructions informatiques, mathématiques et logicielles[384] qui visent à attester de l'intégrité d'un document ou objet numérique tout en authentifiant son auteur[385]. Grâce à la signature électronique, il est aujourd'hui possible de signer des actes juridiques en ligne et d'effectuer des transactions (crypto)financières,

[379] Ce mantra est librement inspiré du précédent et il permet de comprendre l'importance pour les personnes de contrôler leurs identifiants numériques (DID).
[380] Un portefeuille de crypto-actifs représente une application mobile permettant l'interaction (achat, vente, envoi, réception) avec un ou plusieurs crypto-actifs selon les fonctionnalités de l'application. V. Annexe 3.
[381] Proposition de Règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs (MiCA), modifiant la Directive (UE) 2019/1937.
[382] COMPANI Sarah, « Règlement MiCA : les prémices d'un nouveau paradigme financier européen », 8 décembre 2021, « […] tout fournisseur de service sur crypto-actif sera tenu d'identifier l'émetteur et le destinataire effectif de chaque transaction, De nombreuses questions d'interopérabilité des mécanismes d'échange d'information se posent et il n'est pas impossible qu'un standard d'échange d'information international spécifique aux transferts sur blockchain voit le jour dans les années qui viennent, notamment dans le cadre des réflexions en rapport à la mise en œuvre de la travel rule », in *Village de la Justice*. Consulté en ligne le 7 mars 2022, v. également *infra*, I, Titre 2, 2.5.1
[383] V. *infra*, II, Titre 2, 2.4
[384] « Lexique de termes juridiques 2017-2018 », « […] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », consulté en ligne le 28 octobre 2021, p.1904.
[385] Le Décret n° 2022-1620 du 23 décembre 2022 (JO du 24) a modifié l'Article R123-5 du Code de commerce concernant l'exigence d'un certficat qualité de signature électronique notamment pour les formalités de modification et de radiation au RCS : « l'identifiant du déclarant par un moyen d'identification électronique correspond à un niveau de garantie substantiel ou élevé figurant au sein du schéma d'identification électronique notifié en vertu de l'article 9 du Règlement (UE) n°919/2014 du 23 juillet 2014 sur l'identification électronique (…) associée à une signature électronique simple, vaut signature électronique avancée reposant sur un certificat qualité ».

quelquefois sans dévoiler son identité civile[386]. A cet égard, une distinction est à faire entre d'une part la signature électronique qui fait référence à une signature manuscrite dématérialisée au sens des dispositions du Code civil (initialement liée à l'identité pivot d'une personne)[387], et d'autre part la signature cryptographique pseudo-anonyme, étudiée plus loin et qui ne dévoile pas nécessairement l'identité pivot et civile de son signataire. Le cas évoqué ci-après implique que la personne qui signe n'a pas besoin de révéler son identité civile, mais il est essentiel que son identifiant et sa signature cryptographique soient liés de façon certaine pour permettre son identification par le destinataire. Depuis de nombreuses années déjà se développent massivement des systèmes de signature électronique reposant sur des algorithmes de chiffrement asymétrique, initialement apparu dès 1975[388]. Chaque utilisateur dispose de deux clés de chiffrement (deux suites de chiffres et de lettres) générées aléatoirement à l'aide d'algorithmes mathématiques, il s'agit d'une clé publique et d'une clé privée. Elles sont associées et dérivées l'une de l'autre[389] de façon unique et elles sont propres à chaque utilisateur. La clé qui permet d'effectuer des opérations sensibles (déchiffrement d'un message chiffré, signature électronique d'un message chiffré) est appelée la clé privée. L'autre clé, publique, est utilisée pour effectuer des opérations publiques, c'est-à-dire des opérations de vérification du chiffrement d'un message ou encore de sa signature par son émetteur. De cette façon, un message chiffré grâce à une clé privée issue d'un tel système ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. Toute clé publique est un élément qui peut être partagé et connu de tous, tandis que la clé privée doit rester secrète et ne jamais être partagée à un tiers (au risque de se faire usurper son identité). Lorsque ce type d'algorithme est utilisé pour générer une signature électronique, ces deux clés sont utilisées pour vérifier l'authenticité et l'intégrité de chaque message. Cette fonctionnalité native de la signature cryptographique est présente au sein de tout système blockchain et repose sur un pseudo-anonymat[390] qui est étudié plus loin, ainsi que sur une décentralisation informatique[391] plus ou moins importante selon les finalités poursuivies par ces infrastructures. Toutes les solutions de signature électronique 2.0[392] n'utilisent pas nécessairement des mécanismes de cryptographie asymétrique. Appliqués à la technologie blockchain, ces différents mécanismes cryptographiques et d'identification en ligne permettent de garantir une authenticité ainsi qu'une intégrité des jeux de données ou des documents auxquels sont associées des signatures électroniques. Ici, la cryptographie asymétrique garantit l'origine et la personne à l'initiative de la signature électronique d'un document. Le registre d'une blockchain permet de vérifier l'existence d'une

[386] Ce pseudo-anonymat permet une signature électronique compatible avec les règles du RGPD, *v. infra*, I, Titre 2, 1.4.1
[387] Art. 1366 du Code civil dans sa version en vigueur depuis le 1er octobre 2016, qui dispose : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».
[388] V. « Chiffrement asymétrique », 31 mai 2022, in *IONOS Digitalguide*. Disponible à l'adresse suivante
[389] Par essence ce mécanisme fonctionne tel qu'une *clé privée* est dérivée d'une *clé publique maître* accessible à tous : ce système permet ainsi de prouver à la fois sa capacité à signer (clé privée) et l'appartenance à un schéma de dérivation de clé (publique). Par exemple, il est possible de fournir des identités numériques à un groupe de personne identifié par leur *clé publique maître*.
[390] V. *infra*, I, Titre 2, 1.4.1
[391] V. *infra*, I, Titre 2, 2.1.3
[392] Il est fait référence aux services de signature électronique déjà utilisés par les juristes, comme HelloSign, DocuSign, Dropbox Sign, etc.

preuve pseudonyme de cette signature, grâce à la transaction dans laquelle son empreinte numérique est ancrée. Ce double mécanisme de clés permet au propriétaire d'une clé privée de signer numériquement une demande de transaction afin de prouver qu'il en est à l'origine, et à une entité vérificatrice de constater l'authenticité et la titularité de ladite signature inscrite directement sur une blockchain qui peut être de type ouverte ou fermée. Ainsi, la technologie blockchain fournit un moyen de signature électronique intrinsèque qui peut être par ailleurs associé ou non à d'autres mécanismes d'identification ou de signature électronique provenant de système d'identité numérique centralisé et/ou décentralisé.

En droit communautaire, le cadre règlementaire s'appliquant à la signature électronique relève du Règlement eIDAS (étudié au deuxième titre de cette recherche) partiellement entré en vigueur en 2016[393]. Il dispose que « *l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée* » ce qui lui assure une recevabilité en justice, au même titre qu'une signature manuscrite. Pour proposer un encadrement pratique de la diversité des besoins contractuels, le Règlement eIDAS distingue trois niveaux de signature électronique : la signature électronique simple[394], avancée[395] et qualifiée[396]. À la lumière de ces trois niveaux de signature numérique possibles, il est considéré qu'une signature numérique sur blockchain s'assimile à une signature simple dont la recevabilité juridique en termes de preuve est possible[397]. De plus, les articles 25 et 27[398] du Règlement précité réaffirment que toute signature électronique à une valeur légale au sein des pays de l'UE, ce principe incluant de facto la technologie blockchain, dont la fiabilité technique est présumée importante (seulement pour le cas des blockchains hybrides ou privées au sens d'eIDAS-2[399] qui est étudié plus loin). En France, le cadre juridique ne prévoit pas une reconnaissance juridique soit des dispositions légales spécifiques à la signature électronique reposant sur une blockchain. Le caractère de force probante est accordé aux écrits électroniques dès lors que les personnes dont ils émanent sont identifiées et que l'écrit est établi et

[393] Règlement (UE) No 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, consulté le 28 juillet 2021. V. également *infra*, II, Titre 1, 2.1.1.1

[394] *Ibid.* Art. 3-10 : « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ».

[395] *Ibid.* Art. 26 : « Une signature électronique avancée doit être liée au signataire de manière univoque ; permettre d'identifier le signataire ; avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ».

[396] *Ibid.* Art. 3-10 : « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ».

[397] A ce titre, le site « monjuridique.infogreffe.fr » propose un Registre des mouvements de titres dématérialisés reposant sur une blockchain privée, consulté le 11 avril 2022, *v.* l'adresse suivante et v. également *infra*, I, Titre 2, 2.8

[398] *Ibid.* Considérant (27), « ce règlement devrait être neutre du point de vue de la technologie. Les effets juridiques qu'il confère devraient pouvoir être obtenus par tout moyen technique, pour autant que les exigences posées par le présent règlement soient satisfaites ».

[399] V. *infra*, II, Titre 1, 2.1.1.1.a

conservé dans des conditions de nature à assurer son intégrité[400]. Si en pratique il serait possible de considérer qu'une signature numérique sur blockchain (clé publique/clé privée) représente une association technique minimale et donc un moyen d'identification suffisant en tant que tel, cette considération peut toutefois relever certaines complications : (i) lorsque la partie contre laquelle un tier entend prouver des obligations ne souhaite pas divulguer sa clé publique ou encore (ii) si une blockchain publique ne bénéficie pas de la présomption de fiabilité mentionnée. Au regard de ces éléments, deux types de situations nous semblent envisageables, le premier offrant une présomption de fiabilité et le second n'offrant aucune certitude :

(i) Un tiers de confiance qualifié intervient afin de proposer une fonction de signature électronique sécurisée et reliée à une blockchain de type privé ou consortium afin d'assurer une présomption de fiabilité.

(ii) Un utilisateur sans l'aide d'un tiers de confiance déciderait seul de la gestion de bout en bout de son identité numérique. L'identité numérique décentralisée ou auto-souveraine serait par exemple considérée comme un moyen de preuve simple, c'est-à-dire laissé à la libre appréciation souveraine du juge, sans bénéficier d'une présomption de fiabilité et en attendant l'application de la proposition d'amendement du Règlement eIDAS[401].

En fin de compte, la reconnaissance de l'identité numérique décentralisée (IND)[402] et de la technologie blockchain en tant que preuve juridique fiable ne sera possible que si le Règlement eIDAS-2 le permet. Cette question est abordée en détail dans une section spécifique. La reconnaissance de ces mécanismes de signature électronique 3.0, conformément aux textes en vigueur, nécessite la convergence de multiples facteurs en commençant par l'interopérabilité informatique (présumée native) de ces solutions, jusqu'à leur reconnaissance politique et juridique à l'échelle nationale voire communautaire. Avec l'arrivée de ces solutions, les tiers certificateurs pourront simplement se connecter à chaque service d'authentification substantiel ou forte basé sur une solution d'identité numérique décentralisée. Ils seront alors en mesure de récupérer en ligne l'identité légale d'une personne et de la certifier pour finalement procéder à une signature électronique de type avancée.

[400] Nous notons ici l'impérieuse nécessité d'assurer la pérennité des supports (identifiants numériques), et de leurs mécanismes de vérification. Ici, une blockchain (privée ou de consortium) pourrait permettre de respecter les caractères de conservations et d'intégrité édictés.
[401] V. *infra*, II, Titre 1, 2.1.1.1
[402] V. *infra*, II, Titre 1, 1.1

2.3.1.1.c Réseau et stockage distribué en pair à pair (P2P)

Le « *peer-to-peer* » (ci-après « pair à pair » ou « P2P »), est un type d'architecture de réseau dans lequel les ordinateurs ou les dispositifs se connectent directement les uns aux autres sans avoir recours à un serveur central. Cela signifie que chaque dispositif du réseau joue à la fois le rôle de client et de serveur, ce qui permet aux utilisateurs de partager directement des ressources et des informations entre eux. Cela diffère d'une architecture et relation informatique dite client-serveur, conventionnelle, dans laquelle tous les dispositifs du réseau sont soit des clients qui demandent des informations à un serveur, soit des serveurs qui fournissent des informations aux clients. Les réseaux P2P sont souvent utilisés pour le partage de fichiers et d'autres types de collaboration en ligne. Ils sont notamment utilisés par de nombreuses blockchains. Encore aujourd'hui, le concept de stockage de données sur une blockchain est régulièrement évoqué[403]. Pourtant, stocker des données sur une blockchain publique est généralement coûteux (environ 100 dollars par gigaoctet de stockage selon les périodes[404]). Sur le plan informatique, il convient pour cette démonstration de distinguer le stockage de données sur un système distribué versus un stockage sur un registre décentralisé (blockchain). Le premier processus implique de fragmenter (diviser en plusieurs empreintes numériques) les informations à partager, puis de les distribuer et de les répartir sur les ordinateurs des utilisateurs, qui peuvent ensuite les reconstituer automatiquement en pair à pair (sans intermédiaires) pour obtenir des données complètes tels que des documents, des images ou des vidéos. Le second système, quant à lui, ne permet pas de stocker des données d'un volume important en raison d'un coût économique prohibitif. Contrairement à une idée reçue du grand public, une blockchain n'est pas une technologie de stockage d'information car seules des preuves cryptographiques simples et limitées en taille peuvent y être ancrées, contrairement aux réseaux de stockage distribués. Ces logiciels et mécanismes de partage des données directement entre les ordinateurs des utilisateurs ne sont pas nouveaux, ils existent depuis les débuts d'Internet. Ils soulèvent de nombreuses problématiques sur le plan juridique, tant en matière de responsabilité notamment, que de propriété intellectuelle, car certains de ces logiciels ou protocoles sont non seulement distribués, mais entièrement décentralisés, grâce à une technologie blockchain[405].

Si la technologie blockchain et les technologies de registres distribués reposent sur des concepts similaires en tant que réseaux informatiquement distribués (sans autorité centrale), cette similitude ne doit pas entraîner de confusion : tandis que la blockchain partage un registre de transactions continues entre tous ses nœuds[406], un registre distribué se distingue en étant un système de partage de fichiers pair à pair qui séquence des informations en une multitude d'empreintes numériques nommées, des

[403] « Les protocoles d'application basés sur la blockchain fonctionnent comme le protocole BitTorrent à bien des égards, bien qu'ils ne s'appuient pas sur des trackers centralisés ou des tables de hachage distribuées pour coordonner l'activité sur le réseau », *op. cit.* « Blockchain and the Law », in *Harvard University Press*. Ed. Kindle. Emplacement 976 sur 7004.
[404] OMAAR Jamila, « Forever Isn't Free », in *IPDB Blog* [en ligne], publié le 19 juillet 2017, consulté le 29 juillet 2021.
[405] Il est fait référence au projet Ordinnals qui permet d'ancrer de manière complètement pair-à-pair et décentralisée des informations de toutes natures directement au sein des blocs de la blockchain Bitcoin.
[406] V. Annexe 3 & 6

« *hash* »[407], permettant aux utilisateurs de rechercher puis de réifier ces informations sur la base de ses empreintes numériques spécifiques. Ces deux applications technologiques sont informatiquement complémentaires et pourtant distinctes. Appliqué à notre recherche, le stockage distribué peut être utilisé pour stocker des fichiers tandis que leurs identifiants uniques (*hash*) sont conservés sur une blockchain. Un exemple concret de logiciel de stockage distribué est « Internet Protocol Files System - IPFS »[408]. D'autres méthodes plus ou moins similaires, récentes et complexes, permettent de parceller sous la forme de clé de chiffrement des informations ou même des documents. Ces informations sont distribuées et hébergées sur différents *clouds souverains* (serveurs) et nécessitent une réification des clés qui sont détenues par différentes parties afin de procéder à une lecture complète desdites informations. Ces méthodes de stockage et de parcellement informatique sont particulièrement efficaces afin de mettre en conformité les données au regard du RGPD européen ou encore du *Patriot Act américain*[409] qui sont étudiés plus loin. Pour assurer la conformité règlementaire d'une application reliée à une blockchain, il convient idéalement d'héberger et de stocker sur cette dernière uniquement des preuves et des références *pseudo-anonymes* (définies plus loin) qui seront ultérieurement utiles lors du processus de vérification d'une identité. Une solution actuellement privilégiée par de nombreuses blockchains privées et hybrides consiste à héberger des données sensibles sur des serveurs distribués (ou centralisés) identifiés comme étant de confiance et encadrés auprès de tiers certifiés. Pour rappel, un réseau décentralisé est composé de nœuds autonomes qui travaillent néanmoins ensemble pour atteindre un objectif commun, sans qu'il y ait un ou quelques nœuds centraux qui exerce un pouvoir (informatique) plus important sur les autres[410]. Chaque nœud peut prendre des décisions indépendantes et les données sont stockées localement. Un réseau distribué est également composé de plusieurs nœuds qui travaillent ensemble pour atteindre un objectif commun, c'est-à-dire avec un processus de synchronisation pour garantir la cohérence des données qui sont stockées dans des emplacements géographiques certes différents, mais toujours de façon synchrone et interconnectée. Finalement, tandis que les bases de données ont complété et remplacé le papier, le stockage distribué couplé à la technologie blockchain va renforcer, voire se substituer progressivement aux bases de données centralisées. Comme cela est évoqué dans les prochaines parties, l'identité numérique décentralisée (IND)[411] est basée sur une relation directe et pair à pair entre les personnes et les services en ligne. Cette utilisation possible à l'échelle industrielle de

[407] « Le hachage est la transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine. Le hachage est notamment employé pour indexer et récupérer les éléments d'une base de données. Il est en effet plus rapide de trouver l'élément d'après la clé de hachage réduite plutôt qu'à l'aide de la valeur d'origine. Cette fonction est également utilisée dans de nombreux algorithmes de chiffrement. », in *LeMagIT*, « Hachage (hashing) ». Consulté le 12 juin 2022, à l'adresse suivante. Pour comprendre concrètement cette méthode qui utilise l'algorithme SHA-256, vous pouvez introduire n'importe quel type d'entrée sur ce site et obtenir une nouvelle donnée de sortie « *hachée* » d'une longueur fixe. Le moindre changement à votre *donnée d'entrée* entraînera un changement complet de votre donnée en sortie : l'entrée du terme « Droit » sort le *hash* « 664a0432f64f145190913228c4d7357ed74247e93df343f935e8e83f2ba358b6 » ; l'entrée du terme « droit » sort un nouveau *hash* complètement différent « a6993f8f3f26eb9a2f2d232636bc47c0a0a3a819a098063e4c95127a25a460e1 ». Ici, une simple majuscule démontre le caractère unique de chaque *hash* issu d'une donnée initialement entrée, v. également Annexes 3 et 6

[408] Pour plus d'informations consultez le site internet suivant www.ipfs.io

[409] V. *infra*, I, Titre 2, 1.5

[410] V. Annexes 3 et 6

[411] V. *infra*, II, Titre 1, 1.1

serveurs distribués et/ou de technologies blockchains, permettrait aux personnes de se rapprocher d'un modèle d'interaction sociale et identitaire pair à pair (P2P), similaire à celui que nous vivons dans monde réel et physique. De cette façon, aucune entité ne contrôlerait ou ne détiendrait de données d'identité autrement qu'accompagnée d'une transparente totale et d'un consentement systématique de chaque interaction en ligne. A cet égard, un nouveau protocole informatique P2P a fait son apparition début 2020 : le protocole « Nostr » (« Notes and Other Stuff Transmitted by Relays »)[412]. Nostr est un protocole simple et ouvert qui permet de créer des médias sociaux en ligne interopérable, décentralisés et résistants à la censure (aucun ciblage algorithmique ou contrôle de l'information). Il s'agit d'un protocole qui ne dépend pas d'un serveur central et qui est conçu pour être facilement accessible grâce à une clé publique et privée, dans le but de créer un réseau social mondial P2P et résistant à la censure. Dans sa forme la plus fondamentale, il permet aux internautes d'échanger des messages signés par l'intermédiaire d'un réseau de relais, qui sont des serveurs que tout internaute peut faire fonctionner. Depuis son lancement, la communauté des utilisateurs de bitcoins a rapidement adoptée ce protocole et diverses plateformes ont fait leur apparition pour compter plus de 200 000 utilisateurs en avril 2023[413]. Nostr s'inclut donc dans la continuité du Web 2.0, tout en formant une nouvelle brique du Web 3.0 et en s'adossant avec pertinence aux actifs numériques comme le bitcoin.

2.3.1.1.d Appréhension informatique et juridique des contrats intelligents (AEC)

Plus connue du grand public sous son appellation anglophone de « *smart contract* » et généralement sujet à une traduction littérale en français par le terme de « *contrat intelligent* », cette nouvelle application sous-jacente à la technologie blockchain devient populaire lors de son émergence informatique en 2015[414], son concept ayant fait son apparition plus tôt au milieu des années 1990[415]. Depuis le 15 janvier 2021, les contrats intelligents ont été renommés en tant qu'« *automate exécuteur de clauses - AEC* » par la Commission d'enrichissement de la langue française déjà mentionnée[416]. Cette récente traduction vise à promouvoir l'utilisation de la langue française en appliquant une traduction nouvelle pour un concept et terme anglophone plus ancien. Mais cette traduction est complexe et peu intuitive, voilà pourquoi cette étude utilise pour une meilleure compréhension le terme de « *contrat intelligent* »[417], ou bien l'abréviation AEC suggérée par la Commission d'enrichissement de la langue

[412] Pour plus d'informations sur ce protocole *v.* l'adresse Github du projet ou bien l'adresse suivante.
[413] Pour plus d'informations et de statistiques en temps réel consultez le lien suivant. Pour consultez un profil de réseau social utilisant Nostr, visitez le lien suivant.
[414] Lorsque la blockchain Ethereum permet pour la première fois d'effectuer un nouveau type de transaction native sur sa blockchain, permettant le déploiement et l'exécution de contrat intelligent (« *Contract deployment transactions* »).
[415] Le concept de « *smart contract* » est connu depuis des décennies et a été initié par le cryptographe et informaticien Nick Szabo au milieu des années 1990. Selon lui, un contrat intelligent est un protocole de transaction informatisé qui exécute les termes d'un contrat. Ses objectifs sont de satisfaire les contractants selon des conditions contractuelles communes et prédéfinies.
[416] Commission d'enrichissement de la langue française, janvier 2021, *v.* Vocabulaire des actifs numériques. Texte 108-B.
[417] Même si l'utilisation de ce terme est trompeuse car un *smart contract* n'est en réalité ni *intelligent* au sens d'une intelligence artificielle, ni nécessairement un contrat en droit au sens du droit commun. V. également « Les smart contracts, étude de droit des contrats à l'aune de la blockchain », LEVENEUR Claire, Thèse Université Paris-Panthéon-Assas, 2 décembre 2022.

française. Sur le plan sémantique, le terme « *intelligent* » est trompeur, car il semble faire référence à une relative indépendance, voire autonomie, en termes de prise de décision, ce qui n'est pas le cas puisqu'un AEC nécessite pour l'instant une supervision humaine via l'implication d'un développeur. Par ces contrats intelligents, il semble ainsi que la technologie blockchain devienne d'autant plus porteuse de normes (cryptographiques et sociales), conçues par sa communauté, mais dont la juridicité est remise en cause par une partie des juristes. Avec la technologie blockchain, toute la chaîne de valeur contractuelle serait ainsi progressivement façonnée par le code. Souvent considérées comme des objets juridiques non identifiés, les AEC font partie intégrante de cette hypothèse. Afin de resituer ce concept, il s'agit de comprendre qu'avec la naissance d'autres technologies blockchains (soit après celle de Bitcoin), de nouvelles fonctionnalités et applications innovantes sont apparues[418], parfois en faisant l'objet d'une adoption croissante dans les écosystèmes informatiques, économiques et juridiques[419]. L'idée fondatrice de ces programmes automatisés est de se libérer des grandes plateformes numériques 2.0 et plus généralement de tous tiers de confiance lors de la réalisation d'échanges socio-numériques de différentes fonctions (financière, contractuelle, politique)[420]. En février 2022, la Commission européenne propose dans sa proposition de « Loi sur les données » (*v.* pages suivantes) une première définition légale d'un contrat intelligent : un « *programme informatique stocké dans un système de registre électronique, le résultat de l'exécution du programme étant enregistré dans le registre électronique* »[421].

En langage informatique, il est possible de définir un contrat intelligent comme un programme informatique autonome et distribué, utilisant la technologie blockchain et dont les fonctionnalités et la complexité peuvent varier. Ce dernier est nécessairement créé et programmé par un développeur, directement au sein d'une blockchain et grâce à une interface dédiée[422], accessible à tous dans le cadre de blockchains ouvertes. Son idée principale est de déterminer des interactions et des relations entre des parties (droits et obligations) grâce à un programme informatique qui les administrera automatiquement dès sa publication sur une blockchain (dans une transaction)[423]. Si conceptuellement, un contrat n'est qu'un cadre théorique qui délimite les conditions d'une transaction donnée entre des parties, un contrat intelligent porte les principes de dématérialisation, d'autonomie et de prévisibilité, c'est-à-dire d'une confiance 3.0 par conception supposée. Cela signifie qu'il peut contribuer à faciliter, vérifier et faire respecter l'exécution d'un contrat virtuellement et légalement formé. L'utilisation de contrats intelligents

[418] *Op. cit.*, « Blockchain and the Law », Harvard University Press. Emplacement 875 sur 7004.
[419] SCHREPEL Thibault, « Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach », in *European commission*. 2021. Disponible à l'adresse suivante
[420] Selon une étude de PWC en 2022, « 37% des acteurs blockchain utilisent Ethereum dans le monde », « Blockchain & crypto : comment les entreprises en tirent bénéfice ? », disponible à l'adresse suivante. Cette étude est à mettre en perspective avec l'Annexe 6.
[421] Proposition de Règlement du Parlement et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (« Règlement sur les données ») (2022/0047 (COD), *v.* Art. 2 considérant (16), p.47. Ce texte est disponible en ligne. Le *Data Governance Act*, quant à lui, a été adopté en mai 2022 et sera applicable en septembre 2023.
[422] L'écriture d'un tel programme informatique nécessite des connaissances approfondies en programmation traditionnelle ou encore spécifique à un protocole blockchain donné.
[423] V. Annexe 3

pourrait ainsi contribuer à rendre les transactions contractuelles plus sûres, plus transparentes et plus efficaces. Cependant, toutes les blockchains ne sont pas en mesure de prendre en charge l'exécution de contrats intelligents. Seules celles disposant d'un protocole approprié peuvent stocker et exécuter de tels programmes[424]. Une fois ces programmes rédigés puis compilés afin d'optimiser leur exécution sur une blockchain (stockage et bande passante limités), ils s'exécutent automatiquement selon les conditions et les règles informatiques qui les composent. Ces lignes de code peuvent ainsi être conformes à des règles de droit, dès lors que le développeur possède des directives spécifiques en la matière ou des compétences juridiques. Les principales caractéristiques d'un contrat intelligent résident entre autres dans son caractère supposé immuable grâce à sa technologie sous-jacente : la blockchain[425]. Son autonomie de fonctionnement et d'interaction est également une source de gain de temps, en fonction des multiples paramètres qui peuvent être définis en son sein. Un contrat intelligent peut en théorie être implémenté dans toutes sortes de services qui impliquent des programmes informatiques tout en pouvant permettre d'échanger de la valeur. Avec un AEC, la transparence et l'efficacité d'un échange peuvent être contrôlées par des mécanismes numériques et cryptographiques (une interaction de valeur étant ici possible grâce à une valorisation et contrepartie en crypto-actifs).

Une fois rédigé et enregistré sur une blockchain généralement ouverte, un contrat intelligent devient donc public (le code de ce programme est lisible et vérifiable sur cette blockchain)[426]. Cela signifie que toute personne peut librement consulter ses transactions (transferts de crypto-actifs, jeton de droits de vote, ancrage de liens hypertextes ou documents[427]) effectuées automatiquement et quasi instantanément sur la blockchain sur laquelle l'AEC repose. L'automatisation est certaine, la rapidité d'execution est supposée latente, et les coûts de déploiement et de transactions sont en principe diminués en comparaison à l'intervention de tiers de confiance traditionnels (notaires, avocats par exemple). En modifiant les habitudes financières et contractuelles conventionnelles, il semble que les AEC puissent représenter un nouvel outil au service des procédures contractuelles et du droit commun des contrats. La sécurité informatique et l'automatisation peuvent ainsi apporter plus de sécurité et d'efficience juridiques aux relations contractuelles. Par exemple, en cas d'inexécution d'une obligation contractuelle,

[424] Par exemple, la blockchain Bitcoin ne permet pas pour l'instant d'effectuer des contrats intelligents aussi complexes que ceux existants sur la blockchain Ethereum, en raison de leurs différences de protocoles, de langage de programmation ainsi que de vision conceptuelle à long terme. Bitcoin privilégie un réseau simple et robuste, qui permet néanmoins le déploiement de certains programmes autonomes basiques et assimilables à des contrats intelligents : les « *Discreet Log Contract - DLC* ». Ces derniers permettent par exemple aux parties de réaliser des paris en utilisant la blockchain Bitcoin et l'actif bitcoin (BTC). Afin d'établir un contrat, deux parties séquestrent des fonds dans une adresse partagée ou séquestre (multisignature). Ces fonds ne peuvent être dépensés que lorsqu'un tiers de confiance (nommé un oracle) publie et envoie les informations demandées à un instant précis. Par cet exemple pratique, nous constatons que la blockchain Bitcoin accueillera probablement l'équivalent d'AEC sur son infrastructure à moyen terme, ceci au regard des multiples protocoles en cours de développement, comme *Lightning, Taproot, Taro,* étudiés dans l'Annexe 3 (Focus 3), et d'autres protocoles à ce jour inexistants. V. également Annexe 3.

[425] LEVENEUR Claire, « Les smart contracts, étude de droit des contrats à l'aune de la blockchain », 2 décembre 2022, in *Theses.fr*, Université Paris-Panthéon-Assas, pp.3-5.

[426] LASSEGUE Jean, GARAPON Antoine, « Dans la blockchain, les termes encodés du contrat (qui ne sont plus des mots) font immédiatement ce qu'ils disent en exécutant leur programme », *op. cit.* in « Justice digitale », p.162.

[427] V. Annexe 3, Focus 3.

cette dernière est directement enregistrée et visible au sein du contrat intelligent, ce qui explique la valeur probatoire cryptographique et sociale que les utilisateurs d'une blockchain accordent aux AEC. La publicité des contrats intelligents renforce aussi leur capacité d'audit, désormais possible numériquement à tout instant, par les parties intéressées autant que par des tiers. Les lignes de code informatique d'un AEC peuvent ainsi spécifier à la fois les obligations à respecter par les parties impliquées et les étapes d'exécution en temps réel de leurs obligations. Dans ces programmes décentralisés, il est possible de commenter chaque ligne de code et ses effets informatiques, une pratique qui doit être transposée en droit et encouragée pour favoriser une meilleure appréhension juridique de ces programmes. Ces caractéristiques et cette transparence par conception favorisent une forme d'équité contractuelle pour les parties contractantes. Aujourd'hui déjà et a fortiori demain, un contrat intelligent permettra à des acteurs autonomes de développer des programmes entièrement personnalisés et d'une grande complexité, aux impacts d'ores et déjà inédits pour certaines interactions sociales, notamment financières[428]. Si les conditions stipulées dans un contrat intelligent sont automatiquement exécutées et vérifiables grâce à la technologie blockchain, cette autonomie et liberté de conception permet aussi de programmer des règles et conditions nécessaires à la bonne protection contractuelle des parties. De façon générique, il est possible de distinguer trois principales formes de contrats intelligents d'après le rapport d'un groupe de travail composé de juristes et de scientifiques[429] :

(i) Le contrat intelligent en langage naturel : il permet d'exécuter automatiquement tout ou partie des obligations contractuelles déjà existantes en langage naturel (contrat classique). Il ne sert pas à enregistrer les obligations contractuelles, mais plutôt à fournir un support numérique aux parties pour exécuter leurs obligations respectives.

(ii) Le contrat intelligent hybride : dans lequel certaines obligations contractuelles sont enregistrées en langage naturel et d'autres sont enregistrées et programmées directement dans le contrat intelligent sous la forme de conditions et de règles. Certains services permettent d'ores et déjà de faire la passerelle entre l'univers du code informatique et celui des codes juridiques[430].

(iii) Le contrat intelligent (im)pur : il n'existe pas de version en langage naturel de l'accord et de ses conditions ce qui signifie qu'il n'existe d'obligations contractuelles que de façon latente, puisqu'enregistrées dans le code et exécutées par celui-ci sans contrat en langage naturel. Ce dernier type est massivement utilisé aujourd'hui, par exemple au sein des organisations

[428] Il est fait référence à la Finance Décentralisée (« Decentralized Finance ») qui permet aux internautes de bénéficier de taux d'intérêt variables et risqués, mais inédits en comparaison à ceux proposés par des institutions financières traditionnelles.
[429] The LawTech Delivery Panel & UK Jurisdiction Taskforce, 2019, « Legal statement on cryptoassets and smart contracts », consulté en ligne le 12 janvier 2021.
[430] Le site internet OpenLaw permet depuis 2019 de rédiger des contrats en langage naturel puis de les automatiser sur la blockchain Ethereum depuis une interface dédiée, consultez openlaw.io

autonomes décentralisées (DAO) ou pour la finance décentralisée (Defi) évoquées plus loin, souvent avec une intention de se soustraire à la législation en vigueur.

Forts de ces distinctions non exhaustives de type de contrats intelligents, il semble que l'avenir probable de ces programmes informatiques 3.0 soit, en langage naturel à court terme, hybride à moyen terme et (im)pur à long terme. En matière de cybersécurité, les contrats intelligents principalement issus de la blockchain Ethereum[431] sont des programmes développés dans de nouveaux langages informatiques, dont des failles de programmation défraient régulièrement la chronique (pertes et vols de fonds en crypto-actifs)[432]. Toutefois, cette incertitude technique des contrats intelligents ne doit pas être confondue avec la robustesse théorique des blockchains publiques (v. Annexe 7). Si le piratage d'un AEC signifie que l'écosystème de la blockchain Ethereum est vulnérable, cette insécurité de l'application décentralisée ne doit pas être confondue avec l'insécurité moindre de son protocole principal qui semble plus éprouvé depuis 2015 (v. Annexe 6). A cet égard, pour favoriser et garantir une sécurité informatique et juridique minimale pour les AEC issus de tiers de confiance, cette recherche soutient que la loi n° 2022-309 du 3 mars 2022[433] pour la mise en place d'un « *Cyber Score* »[434] devrait inclure avec pertinence les contrats intelligents, au même titre que les plateformes en ligne ou encore les systèmes de messageries. Sur le plan juridique, parce que de nombreux contrats intelligents assurent la fourniture d'une prestation de service en ligne entre un professionnel et un particulier, ils doivent se conformer aux obligations légales applicables à tout contrat conclu par voie électronique. Il convient de constater que les contrats intelligents réunissent plus ou moins bien certaines conditions de fond et de forme à la formation de contrats légalement formés (entre professionnels et entre professionnels et particuliers) :

[431] « A deep dive into the 5 popular smart contract development platforms and their comparison », in *CoinTelegraph*, 19 mai 2022, disponible à l'adresse suivante, *v.* également Annexe 6, Focus 2.
[432] « À la fin du mois d'avril 2021, les principaux vols, piratages et fraudes de cryptomonnaies ont totalisé 432 millions de dollars », 11 août 2021, *v.* « Cryptocurrency Crime and Anti-Money Laundering Report », in *CipherTrace*. Disponible à l'adresse suivante
[433] Loi n°2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, JORF n°0053 du 04/03/22, modifiant les dispositions de l'Article L. 111-7-3 du Code de la consommation qui dispose désormais « Les opérateurs de plateformes en ligne (…) et les personnes qui fournissent des services de communications interpersonnelles non fondés sur la numérotation (…) réalisent un audit de cybersécurité, dont les résultats sont présentés au consommateur (…) portant sur la sécurisation et la localisation des données qu'ils hébergent, directement ou par l'intermédiaire d'un tiers (…) L'audit mentionné est effectué par des prestataires d'audit qualifiés par l'Agence nationale de la sécurité des systèmes d'information ».
[434] La mise en place d'un *Cyber Score* a pour objectif de lutter contre les menaces et les failles de sécurité. Sont concernés tous les grands opérateurs du numérique à destination du public tels que les plateformes en ligne, logiciels de visioconférences, systèmes de messageries. Les startups et petites entreprises ne sont pas encore concernées. Un décret est attendu pour préciser les seuils, le périmètre et la durée de validité du Cyber Score. Les sanctions en cas de manquement pourront atteindre 375 000 € pour une personne morale. L'objectif du Cyber Score est de renforcer la protection des acteurs (TPE, PME, grand public) en favorisant les solutions sécurisées et responsables. L'audit à l'origine de la détermination du score sera mené par l'ANSSI selon plusieurs indicateurs (localisation des données, sécurité et types de chiffrement, nombre de condamnations RGPD, et nombre de failles logicielles mises à jour). Il servira d'indicateur de comparaison entre les entreprises et deviendra un des critères de valorisation.

Types de contrats (*non exhaustifs*)	**Validité juridique d'un AEC en tant que contrat valablement formé**
Contrat négocié	Oui
Contrat authentique	Non
Contrat solennel	Non
Contrat réel	Oui ou non selon l'objet spécifique du contrat
Contrat d'adhésion	Oui

Pour le moment, les AEC semblent tout au mieux pouvoir prétendre à une qualification juridique de quasi-contrats. Citons les dispositions propres au contrats conclus par voie électronique, à savoir les dispositions des articles 1125 à 1127-4 du Code civil[435] concernant leur formation et conclusion à distance. Il n'est pas certain que la conclusion de contrats intelligents respecte systématiquement le droit positif, un paradoxe au regard de l'utilisation croissante et quotidienne notamment de plateformes d'échanges de crypto-actifs et de services financiers 3.0[436]. Ainsi, un amendement aux dispositions actuelles du Code civil concernant la formation des contrats pourrait permettre d'inclure de manière explicite les « *automates exécuteurs de clauses - AEC* ». La doctrine s'y emploie depuis 2018[437], mais il reste de nombreuses incertitudes juridiques ne serait-ce qu'en matière de responsabilité civile et/ou pénale. Est-ce le développeur ou la partie qui n'a pas respecté les conditions ? Sans doute et comme cela est souvent le cas pour une matière juridique, il s'agira d'une appréciation au cas par cas. Il doit être mentionné pour être complet dans la stratégie numérique européenne plusieurs textes communautaires essentiels à l'encadrement juridique des données impactant les contrats intelligents. Le Data Governance

[435] Articles 1112 à 1127-4 du Code civil, dans leur version en vigueur depuis le 1er octobre 2016, Sous-section 4 : dispositions propres au contrat conclu par voie électronique de la Section 1 : la conclusion du contrat.
[436] Il est fait référence au concept précité de « Finance Décentralisée » (« Decentralized Finance – DeFi »), qui regroupe de nombreuses plateformes et services financiers (*v.* plateforme/bourses de crypto-actifs nommée Uniswap) pseudo-décentralisées à destination des détenteurs de crypto-actifs.
[437] Maître GIUSTI Jérôme, « Les 'smart contracts' sont-ils des contrats ? », 31 mars 2018, in *Metalaw*, consulté le 11 juin 2022, à l'adresse suivante

Act (DGA)[438], un Règlement européen sur la gouvernance des données qui a été voté en mai 2022 pour une entrée en vigueur en septembre 2023, suivi d'une proposition législative pour un nouveau Règlement, le « Data Act (DA) »[439], rédigé au profit des entreprises avec un volet conséquent sur l'Internet des objets (IdO/IoT), venant s'inscrire aux côtés du « Digital Markets Act – DMA » qui a été voté le 19 octobre 2022, et du « Digital Services Act - DSA » voté le 27 octobre 2022. D'autre propositions de Règlements sont en cours de discussion, comme le Règlement « e-privacy » et un futur Règlement « IA » dédié à l'intelligence artificielle[440].

Le projet du DA ne mentionne pas spécifiquement l'industrie des crypto-actifs. Certains acteurs de cette industrie s'inquiètent des conséquences de son entrée en vigueur en septembre 2023 sur les contrats intelligents. En l'état actuel, il est prévu une « *présomption de conformité* » pour les contrats intelligents non financiers, dédiés à la gestion de données de personnes morales, physiques ou de machines (objets connectés). Selon l'article 30, le vendeur d'un contrat intelligent, ou la personne dont l'activité implique le déploiement de contrats intelligents pour des tiers dans le cadre d'un accord de mise à disposition de données, devrait réaliser une « *évaluation de conformité* » et délivrer une déclaration de conformité pour ces contrats. Cette personne devient alors responsable du respect de quatre exigences[441]. Si le champ d'application se trouve un jour élargi pour inclure les contrats intelligents (crypto)financiers, alors ces derniers ne pourront se conformer à de telles exigences. Une telle extension entraînerait ainsi des conséquences similaires à la tentative d'interdiction de la *Preuve de travail* rejetée *in extremis* du Règlement MiCA, comme étudié plus loin[442]. En pratique, cette *présomption de conformité* sera accordée aux contrats intelligents à vocation non financière (gestion de données issues de machines), mais elle ne s'applique pas aux contrats intelligents (crypto)financiers massivement utilisés actuellement. Ces règles visent à créer une forme de standardisation des contrats intelligents avec une nouvelle classe d'AEC centralisés, contrôlés et hybrides, dont le caractère immuable des transactions est écarté. L'impact réel de ces règles reste à déterminer à travers de futurs actes d'exécution dédiés. Cette disposition semble ainsi faire écho à la *présomption de fiabilité* qui est également accordée sous certaines conditions aux « *registres électroniques* » (blockchains)[443] au sens du Règlement eIDAS-2.

---

[438] Règlement (EU) 2022/868 du Parlement Européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (Règlement sur la gouvernance) et modifiant le Règlement (UE) 2019/1724 sur la gouvernance des données, v. le Livre blanc « Gouvernance des données : organisation et stratégie à adopter en 2023 », in *DataValue consulting*, téléchargeable sur le site *dataconsulting.com*

[439] Proposition (CE) de Règlement du Parlement Européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (Règlement sur les données), 2022/0047(COD), 23 février 2022, *v.* disponible à l'adresse suivante

[440] Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), COM/2021/206, disponible en ligne

[441] V. Art. 30 : « (…) robustesse, capacité d'interruption, contrôle des accès et audibilité (…) ».

[442] V, *infra*, I, Titre 2, 2.5

[443] Un second flou sémantique au sein du Data Act concerne la référence au terme de « *registre électronique* » (art. 2, 16 & 17), qui renvoi à « l'article 3 point 53 » du Règlement eIDAS. Pourtant, cette référence ne définit pas ce terme (inexistant dans eIDAS). Par extension, il est probable que le terme de « registre électronique » du Data Act fasse plutôt référence à celui « d'horodatage électronique » défini dans le point 33 (non pas « 53 » comme inscrit dans le Data Act). Cela peut être une source de confusion, car le Data Act mentionne le terme de registre électronique dans la définition d'un contrat intelligent, alors qu'il

Tentative de réappropriation technologique pour certains ou d'habillage technologique pour d'autres, il est encore tôt pour le savoir, et seuls les actes d'exécution mentionnés permettront de le déterminer[444].

Par conséquent, les contrats intelligents restent principalement utilisés en 2023 dans le cadre de relations et contrats (crypto)financiers, c'est-à-dire relatifs aux crypto-actifs. Toutefois, à mesure de l'adoption de son concept et de sa technologie blockchain sous-jacente, d'autres cas d'usage apparaissent, notamment relatifs aux attributs d'identité numérique. Notons que lorsque plusieurs contrats intelligents sont liés les uns aux autres (l'un pour gérer des transactions financières, un autre gérant des droits de vote, etc.), ils forment le concept « *d'organisation autonome décentralisée - DAO* »[445] qui est étudié plus loin, de sorte que leurs bénéficiaires et utilisateurs puissent répliquer le fonctionnement d'une personne morale, mais de façon transparente, accessible et dématérialisée[446]. Finalement, les contrats intelligents ne doivent pas être considérés isolément, car leur potentiel applicatif reste partiellement méconnu, comme le démontre leur réappropriation par les jetons non fongibles (NFT)[447] entre 2020 et 2022. Nous soutenons que dans un avenir proche les AEC seront un pilier de la gestion de l'identité numérique auto-souveraine, étudiée au titre deuxième de cette étude. Une majorité des blockchains privées et consortiums sont compatibles avec la création et la gestion d'AEC, car elles sont issues de la version publique de la blockchain Ethereum qui a vu naître ce concept de programme autonome et décentralisé. Si les contrats intelligents défient partiellement les règles de droit par du code informatique, mais aussi en diminuant le rôle du juge pour trancher un litige, les conditions de formation et d'exécution des AEC relèvent sur le plan juridique du droit commun des contrats, comme semblent progressivement le rappeler de plus en plus de juristes[448].

---

s'agit stricto sensu d'une référence à la notion d'horodatage électronique au sein d'eIDAS, et non pas comme cela est possible, une référence à la notion de « registre distribué » dont dispose le Règlement MiCA (*v.* art. 3, 1). Cela pourrait sembler plus cohérent, car les contrats intelligents ne peuvent exister informatiquement que sur un « *registre distribué* » (MiCA) et non pas sur un « horodatage électronique » au sens d'eIDAS et comme cela est actuellement rédigé dans le Data Act. Il semble ainsi que cette confusion mène à une forme de contresens sémantique au regard des sciences de l'informatique ainsi que la nécessite en droit de mettre le terme « registre/horodatage électronique » par « registre distribué ».

[444] Consultez le Chap. XI « Dispositions finales », disponible à l'adresse suivante

[445] V. *infra*, I, Titre 1, 2.3.1.1.f

[446] *Op., cit.* « (…) les mini-communautés créées par la blockchain prétendent s'institutionnaliser grâce à la technique », in « Justice digitale », p.152.

[447] Le terme de « JNF » a fait son entrée dans l'édition 2023 du Larousse, avec la définition suivante : « Fichier numérique non reproductible et infalsifiable représentant un actif unique, objet virtuel ou physique (œuvre d'art, tweet, morceau de musique, etc.), qui est répertorié dans une blockchain et auquel est associé un certificat digital d'authenticité et de propriété. ». Si cette définition est perfectible, notamment au regard de la notion d'unicité des actifs dont un JNF fait l'objet (bien souvent ni uniques ni rares), notons qu'elle demeure particulièrement proche de la réalité informatique et pratique des usages faits de ces objets numériques en 2022. *v.* également *infra*, I, Titre 1, 2.3.1.1.f

[448] V. *infra*, I, Titre 2, 2.7.1

2.3.1.1.e Les contrats ricardiens au service d'une contractualisation 3.0 renforcée

Le programmateur en informatique Ian Grigg a dressé le constat suivant « *si pour certains les problèmes ont des contrats pour les résoudre, nos problèmes sont les contrats* ». Ce constat l'a conduit à créer le concept de « contrats Ricardiens », également connus sous le nom de « Ricardians contracts » en anglais[449]. En 1995, il a inventé ce nouveau concept et l'a initialement appelé « Ian Grigg Ricardian contract ». Ce nom a été choisi en hommage à David Ricardo, un économiste libéral anglais célèbre et grand contributeur de la théorie internationale du commerce. En 2016, Oliver Hart et Bengt Holmström ont reçu le prix Nobel d'économie pour leur travail sur l'incomplétude des contrats et ses conséquences sur l'économie. Cependant, Ian Grigg a trouvé une solution à la complexité des contrats bien avant l'attribution du prix Nobel. Les contrats sont souvent imparfaits et incomplets en raison des risques imprévus qui peuvent survenir avant ou après leur signature. Ian Grigg a proposé que la programmation et l'exécution automatique de certaines clauses permettent de réduire considérablement le problème de complexité et d'efficacité associé aux contrats traditionnels. Contrairement à ces derniers, une exécution contractuelle automatique pourrait améliorer la clarté et l'efficacité tout en économisant un temps précieux pour les parties concernées. L'invention du « contrat Ricardien » remonte à 1995, mais le terme n'a été utilisé pour la première fois dans une publication académique qu'en 1998[450]. Ce n'est qu'en 2004 qu'une publication spécifiquement dédiée au sujet a détaillé l'origine du problème et la solution proposée par Ian Grigg[451]. En plus de la création du concept de contrat Ricardien, Ian Grigg est également connu dans le monde de la blockchain pour son travail sur les monnaies cryptographiques dans les années 2000, notamment avec sa startup DigiCash[452]. En substance, un contrat Ricardien est un concept novateur qui permet de lier un contrat papier à sa version numérique programmée afin de rendre automatique l'exécution de certaines de ses clauses. Il est complémentaire au contrat intelligent hybride mentionné précédemment. Ce contrat est juridiquement contraignant et peut être lu par des ordinateurs aussi bien que par des professionnels du droit. Il se compose d'un document rempli et signé par les parties, qui existe sous deux formes : l'une sous forme de code lisible uniquement par les ordinateurs, et l'autre sous forme de texte lisible par l'Homme. Le contrat Ricardien est présenté sous la forme d'un texte comportant plusieurs paramètres à remplir, qui s'auto-exécutent une fois validés. Cette approche astucieuse lui a valu d'être appelé « contrat judicieux » (« Wise contract »), car elle permet à la fois la lecture, la compréhension et l'exécution du contrat.

Le contrat ricardien peut être défini comme un modèle de contrat accessible à tous, qui permet de générer un document (i) lisible par l'Homme, (ii) exécutable par un ordinateur, (iii) signé numériquement[453],

[449] KRYPTOSPHERE®, « Les Ricardian contracts, l'avenir des smart contracts ? » in *Cryptoast*, en ligne, publié le 5 septembre 2020.
[450] GRIGG Ian, « Financial Cryptography in 7 Layers », 1998-2000, disponible à l'adresse suivante
[451] *Op. cit.* « The Ricardian Contract », consulté le 29 juillet 2021.
[452] V. *infra*, I, Titre 2, 1.4.1
[453] Concernant la signature du contrat, une fois les paramètres remplis, la signature se fait à l'aide d'une *clé privée* ou utilisant d'autres protocoles similaires (type PGP). Cette signature constitue une preuve de l'intention d'une partie.

(iv) contenant les clés privées des parties ou des serveurs informatiques impliqués, et (v) pouvant posséder un identifiant unique[454]. Cette invention vise à surmonter la barrière qui sépare le monde des machines de celui des Hommes. Traditionnellement, les contrats existent sous forme papier ou numérique, mais sont exclusivement lus par des humains. Les programmes informatiques, en revanche, ne sont exécutables que par des ordinateurs. Leur séparation crée un écart où la complexité peut se nicher. Le contrat Ricardien crée ainsi une passerelle inédite entre l'Homme et la machine pour combler cet écart. Dans l'histoire des sciences informatiques, le contrat ricardien peut être considéré comme un précurseur du contrat intelligent. En effet, dès les années 2000, Ian Grigg avait déjà compris l'importance d'automatiser l'exécution de certaines clauses de contrats numériques, ce qui est aujourd'hui une caractéristique clé des contrats intelligents. Ainsi, en créant le contrat ricardien, il répondait à cette problématique en créant un document unique qui pouvait être à la fois juridiquement valable et exécutable de manière transparente et incorruptible sur une blockchain publique, privée ou hybride. Initialement, Ian Grigg avait conçu le contrat ricardien pour le secteur financier et plus précisément pour l'émission de produits financiers complexes. Cependant, dès 2019[455], la plateforme de vente en ligne OpenBazaar a adopté cette nouvelle forme de contrat, témoignant ainsi de la diversité des cas d'utilisation possibles pour ce système informatique et contractuel ancien et pourtant toujours pertinent. En principe, un contrat ricardien doit être stocké chez l'une des parties ou une tierce partie pour être conservé numériquement puis exécuté via une interface. La blockchain ou des serveurs P2P évoqués précédemment proposent à cet égard leur complémentarité, intérêt et pertinence. Le contrat peut alors être stocké et exécuté sur un registre électronique distribué ou décentralisé[456] avec les divers avantages que cela peut impliquer (conformité, sécurité, transparence, intégrité de la donnée). Comme nous l'avons expliqué, un contrat ricardien est en premier lieu un contrat juridiquement valable, et en second lieu, qui s'auto-exécute. Lorsqu'un contrat intelligent ne peut être qu'un moyen d'exécution d'un contrat sur une blockchain (le contrat légalement formé étant un document distinct), le contrat Ricardien est à la fois un contrat et un mode d'exécution sur une blockchain et/ou sur un serveur centralisé. Un contrat intelligent ne peut prévoir l'issue de nombreuses situations qui peuvent survenir dans un contrat, les contrats étant imparfaits par nature. En effet, un contrat intelligent peut prévoir l'arrêt de son exécution, mais pas l'issue définitive d'une situation. En cas d'échec de l'automatisation de certaines de ses clauses, un contrat ricardien prévoit par conception une issue légalement approuvée par les parties, comme le renvoi devant un arbitre ou un juge. A ce titre, il est possible d'imaginer que des AEC ou contrats ricardiens

[454] Il s'agit tout simplement du *hash* du contrat une fois que celui a été signé numériquement par les parties. Le *hash* étant une suite de chiffres et de lettres d'une longueur donnée résultant du passage d'un fichier dans une fonction de hachage. Quels que soient le format et la taille du fichier, le *hash* sera toujours de la même longueur, mais ne sera jamais le même. Une simple modification d'une seule lettre dans un texte de milliers de pages entraînera une modification radicale du hash, permettant *in fine* d'attester de l'intégrité dudit contrat.

[455] LOPAMUDRA Mandal, « Ricardian contract : Bridging the Gap Between Smart Contracts and Traditional Contracts », Master Thesis, International Business Law, juin 2019, p.10, disponible en ligne à l'adresse suivante

[456] Ici, une distinction est importante à faire entre un *registre distribué* qui permet le stockage de données et un *registre décentralisé (blockchain),* qui ne permet que de stocker des preuves de données et non l'entièreté de ces dernières (pour des raisons informatiques comme un coût de stockage prohibitif lorsqu'effectué sur une blockchain décentralisée).

disposent de clauses d'arbitrages prévoyant le recours à un règlement décentralisé des différends (v. « Kleros »). En résumé, les contrats ricardiens offrent une sécurité supérieure à celle des contrats papier grâce à leur signature cryptographique complexe à usurper et contrefaire. Ils permettent également d'automatiser tout ou partie du contrat, ce qui peut entraîner un gain de temps considérable et une économie de coûts humains et financiers. Cependant, selon Ian Grigg, il n'est pas toujours bénéfique d'automatiser toutes les clauses d'un contrat, car certaines sont trop complexes et imprévisibles. Par conséquent, il est probable que seuls les contrats peu complexes et répétitifs seront entièrement automatisés, tandis que les autres seront des contrats hybrides qui visent à satisfaire aux exigences juridiques des parties. En outre, selon Ian Grigg, les professionnels concernés peuvent ne pas avoir besoin ou ne pas être intéressés par les contrats numériques, qu'ils soient « intelligents » ou « ricardiens », et le rôle des juristes ne peut être totalement remplacé par ces contrats.

2.3.1.1.f Les organisations autonomes décentralisées (DAO)

Comme l'expliquait déjà en 2016 la docteure et auteure Primavera De Filippi : « *si les blockchains s'améliorent en termes de vitesse, de performance, de fonctionnalité et d'accessibilité, la technologie pourrait, à plus long terme, commencer à structurer des organisations qui concurrencent les sociétés traditionnelles et d'autres entités juridiques* (…) ». En 2022, une organisation autonome décentralisée, traduit de l'anglais « *Decentralized Autonomous Organization - DAO* », peut être simplement définie comme une communauté en ligne structurée sur un protocole blockchain[457]. Il s'agit d'un nouveau type d'organisation apparu en 2016 qui fonctionne à l'aide de contrats intelligents sur une blockchain. Cela signifie qu'il s'agit d'une entité numérique qui fonctionne automatiquement, avec ou sans intervention humaine, selon un ensemble de règles encodées dans des AEC. Ces règles déterminent la façon dont l'organisation est gérée, comment les décisions sont prises et comment cette organisation interagit avec d'autres entités sur la blockchain. La promesse des DAO est de contribuer à transformer la gouvernance d'Internet et plus précisément de ses services en ligne, notamment en proposant de les co-construire en les impliquant avec leurs utilisateurs dans la chaîne des prises de décision, c'est-à-dire dans leur gouvernance. En d'autres termes, une DAO est une organisation numérique qui reproduit sur une blockchain les actions et interactions propres à toute organisation, comme le droit de vote, les transferts financiers, les services de messagerie. En conséquence, une DAO est une entité virtuelle (généralement sans structure ni statut juridique) dans laquelle toutes les interactions sont effectuées au moyen de contrats intelligents sur une blockchain. Il existe ainsi autant de DAO que de multiples possibilités d'environnements et contextes virtuels, à la disposition de détenteurs de crypto-actifs qui souhaitent fonder ou rejoindre une DAO. Le caractère autonome d'une DAO signifie que certaines de ses

[457] « Elle [DAO] permet de fonder des groupes par des contrats mais sans contrat politique initial ni statuts (…) », *op. cit.* « Justice digitale », p.148.

interactions peuvent être programmées et automatisées en fonction des règles de leurs fondateurs et communautés. Son caractère décentralisé suppose qu'aucun intermédiaire ne peut la censurer ou empêcher son bon fonctionnement[458], un constat régulièrement remis en cause dans les faits en raison d'une nécessité intrinsèque de tiers de confiance au cœur de la création de ces entités en réalité profondément sociale et donc hiérarchisée et centralisée. Comme pour les contrats intelligents, une approche ainsi mesurée au cas par cas du caractère ou non informatiquement décentralisé d'une DAO semble pertinente, car cela implique une qualification juridique bien différente selon les situations et juridictions. En principe, toute DAO est décentralisée, ce qui signifie qu'elles ne sont pas contrôlées par une seule personne ou un seul groupe, mais plutôt par tous les membres qui participent à son fonctionnement (utilisateurs, développeurs et entrepreneurs). Cela leur permet de fonctionner de manière transparente et démocratique (tous les membres ayant par exemple une voix égale dans la façon dont l'organisation est gérée). Sur le plan sémantique, le terme « autonome » inscrit dans l'acronyme DAO est aussi trompeur que le terme d'intelligent attribué aux AEC. Il s'agit plutôt d'un système automatisé et non pas techniquement indépendant et autonome. Un constat similaire est possible en ce qui concerne l'utilisation du terme « décentralisée », car une DAO est souvent contrôlée par un groupe plus ou moins important d'acteurs, tels que des particuliers ou des entreprises (voir ci-dessous).

Il est important de noter que le pouvoir de gouvernance au sein de ces communautés numériques est partagé entre les membres grâce à des contrats intelligents qui visent à créer une communauté en ligne libre et indépendante. En théorie, chaque décision et règle d'une communauté numérique décentralisée est soumise à l'appréciation collective de ses autres membres (droit de vote, échanges de crypto-actifs, messagerie privée, processus de revue par les pairs, etc.). Bien que les DAO existent sur Ethereum depuis 2016, ces premières expériences informatiques et sociales représentaient des projets scientifiques grandeur nature (expérimentations), plutôt que des produits commercialisables et accessibles au grand public. Toutefois, depuis décembre 2020, les DAO sont devenus une nécessité pratique au sein de la crypto- économie et une inquiétude pour certains juristes. Le premier vecteur quasi industriel du déploiement de ce concept technologique a été mis en pratique par des protocoles de « *Finance Décentralisée - DeFi* » qui pour se développer (parfois pour échapper aux règlementations financières)[459], ont remis un contrôle plus ou moins important de leur(s) protocole(s) entre les mains de

[458] *Ibid.* « Les decentralized autonomous organisations [DAO] ne sont plus localisables sur un serveur donné, et ne sont la propriété de personne ».

[459] Toutefois, dans cette nébuleuse de la *finance décentralisée*, nous considérons que le législateur peut toujours trouver une entité ou un responsable à qui s'adresser et par conséquent qui peut être régulé. A ce titre, la Commission européenne a émis un appel à projets d'une durée de 15 mois le 5 octobre 2022 - à hauteur de 250 millions d'euros – afin d'encadrer ce nouveau segment de marché de la technologie blockchain. Il s'agit notamment de « développer, déployer et tester une solution technologique pour la supervision embarquée de l'activité de la finance décentralisée (DeFi). Le projet cherchera à profiter de la nature ouverte des données de transaction sur la blockchain Ethereum, qui est la plus grande plateforme de règlement des protocoles DeFi. Il sera principalement axé sur la collecte automatisée de données de surveillance directement à partir de la blockchain afin de tester les capacités technologiques de surveillance de l'activité DeFi en temps réel. », traduction libre de l'anglais, in *TED - Tenders Electronic Daily*. Consulté le 19 octobre 2022, à l'adresse suivante

leur(s) communauté(s) et d'utilisateurs. Ce fonctionnement très plébiscité entre 2020 et 2022 fonctionne de telle sorte que ces utilisateurs votent grâce à des jetons d'utilité et de gouvernance qu'ils acquièrent directement sur leurs adresses personnelles, elles-mêmes enregistrées et liées à ces DAO, de façon à influencer le développement de ces projets aux promesses parfois douteuses. En élargissant le propos, la création d'une DAO sur une blockchain permet à une entité de profiter des mêmes avantages inhérents à la technologie blockchain, tels que la décentralisation des interactions, la sécurité, la rapidité, la transparence et l'immutabilité[460]. Sur le plan social et politique, de nombreux acteurs de la crypto-économie suggèrent qu'une DAO se rapproche d'un système démocratique pur, similaire à ceux de la Grèce antique. Si les DAO permettent effectivement de créer une nouvelle multitude décentralisée de communautés numériques, cette assertion semble utopique ne serait-ce qu'au regard (i) de la formation d'une DAO et (ii) de leurs effets pour ses utilisateurs.

(i) Lors de sa formation, une DAO implique la création puis la répartition et distribution de son capital de jetons numériques, au bénéfice de ses utilisateurs. Cette émission de jetons est ainsi soumise à une centralisation initiale par quelques acteurs ou entités, qui dans la majorité des cas représentent les bénéficiaires effectifs et majoritaires de cette DAO. En principe, plus une personne possède de jetons, plus elle possède de pouvoir de décision (à l'image de la détention de parts sociales au sein d'une société commerciale par exemple). La détention capitalistique étant au cœur de ce système de gouvernance centralisé, il convient de ne pas la confondre avec son protocole blockchain (qui est lui informatiquement décentralisé[461]), comme cela peut souvent être le cas en dehors de cet écosystème.

(ii) Les systèmes de gouvernance des DAO sont donc nombreux, et tous informatiquement et socialement centralisés. Les utilisateurs ayant une faible participation à la gouvernance et possédant moins de jetons peuvent subir des conséquences inattendues, notamment le risque de manipulation par des utilisateurs ayant une plus grande quantité de jetons. Les petits porteurs pourraient ainsi subir des pertes financières importantes. De plus, en cas d'escroqueries, de vols ou d'erreurs, les responsabilités sont complexes

En outre, un nouveau rapport publié par la Commission européenne propose quatre mesures pour encadrer cet écosystème : (i) réglementer les personnes morales (dispositions macro-prudentielles, etc.), (ii) introduire un cadre volontaire pour la supervision de la DeFi, (iii) créer un observatoire public qui émet des avis sur la base des données issues de blockchains publiques (« *supervision intégrée* ») et enfin (iv) construire une approche pour la supervision/régulation des *oracles* (un oracle est un tiers de confiance utilisé pour transférer des informations de confiance vers une blockchain). FISMA: Directorate-General for Financial Stability, Financial Services and Capital Markets Union. 2022. « Decentralized finance: information frictions and public policies: approaching the regulation and supervision of decentralized finance ». Consulté le 24 octobre 2022, à l'adresse suivante

[460] À titre d'illustration, voici une DAO basée sur la blockchain Ethereum pour mieux comprendre les explications précédentes. Cette DAO a été utilisé à des fins d'expérimentation entre 2019 et 2021. En naviguant sur son interface, il est possible de voir qu'elle permet à ses utilisateurs de voter, de déposer ou retirer des crypto-actifs (ethers) ou encore d'échanger des messages directement via la blockchain Ethereum.

[461] V. Annexe 7.

à définir et les responsables à identifier en raison d'un pseudo-anonymat[462] étudié au titre suivant de cette étude, ce que démontre la juriste Primavera De Filippi : « *toute action à l'encontre des promoteurs ou des détenteurs de jetons peut dissuader l'intérêt mais ne mettra pas nécessairement fin à ces organisations.* (...) *En effet, même avec une ordonnance du tribunal, les mécanismes traditionnels d'application de la loi peuvent avoir du mal à atteindre les actifs contrôlés par une organisation décentralisée* »[463]. De plus, le fait que chaque DAO fonctionne de manière unique et que ses jetons numériques puissent être classés dans une ou plusieurs des catégories d'une ou plusieurs (crypto)taxonomie et de juridictions, en fonction de leur nature, de leur objectif ou de leurs caractéristiques, complexifie toute qualification juridique. A ce jour, la majorité des DAO ne sont pas légalement enregistrées, excepté dans l'Etat du Wyoming qui a été le premier Etat à créer un régime juridique ad hoc dédié à ces organisations décentralisées[464]. Finalement, comme l'admet partiellement en 2022 le co-fondateur d'Ethereum, Vitalik Buterin : « *d'un point de vue réaliste, nous n'avons probablement besoin que d'un petit nombre de DAO qui ressemblent plus à des constructions issues des sciences politiques plutôt qu'à des DAO au fonctionnement similaire à la gouvernance des entreprises. Mais ce sont les plus importantes* »[465].

Par conséquent, afin de répondre à une partie de ces défis numériques et juridiques, un récent rapport de l'Assemblée nationale[466] propose de reconnaître les DAO comme une entité légale dotée d'une personnalité juridique. Cette proposition, que cette recherche soutient, a pour objectif d'adopter un cadre juridique *ad hoc* pour ces entités numériques, notamment en leur imposant (i) de se conformer aux obligations réglementaires en vigueur en France (enregistrement en tant que PSAN[467]), (ii) d'identifier l'identité des détenteurs et bénéficiaires de jetons numériques et (iii) de mettre en place des garanties

[462] V. *infra*, I, Titre 2, 1.4.1
[463] *Op. cit.*, De FILIPPI Primavera. « Blockchain and the Law », emplacement 2835 sur 7004.
[464] L'Etat américain du *Wyoming* a légalement reconnu les DAO qui sont dès lors considérées comme une société à responsabilité limitée avec des dispositions spéciales permettant à la société d'être dirigée ou gérée de manière algorithmique (tout ou en partie) par des *contrats intelligents*. Ce projet de loi crée un supplément à la loi sur les sociétés à responsabilité limitée du Wyoming afin de fournir une loi contrôlant la création et la gestion d'une DAO. Les dispositions de la loi sur les sociétés à responsabilité limitée s'appliquent à une DAO, sauf si elles sont spécifiquement modifiées par le supplément. Ce projet de loi établit des exigences de base pour les DAO gérées par des membres ou par des algorithmes et fournit des définitions et des règlements pour la formation des DAO, les articles d'organisation, les accords d'exploitation, les contrats intelligents, la gestion, les normes de conduite, les intérêts des membres, les droits de vote, le retrait des membres et la dissolution. Sixty-sixth legislature of the state of Wyoming, 2021, « SF0038 - Decentralized autonomous organizations », in *www.wyoleg.gov*. consulté le 12 juin 2022, à l'adresse suivante
[465] BUTERIN Vitalik, « DAOs are not corporations: where decentralization in autonomous organizations matters », 2022, Consulté le 20 septembre 2022, à l'adresse suivante
[466] « Proposition 22 : (i) Permettre aux DAO d'obtenir la personnalité juridique afin de reconnaitre leur existence juridique et leur donner le pouvoir de nouer des relations contractuelles contrairement à d'autres personnes morales. (ii) Développer un cadre règlementaire afin de prendre en compte leur gouvernance, d'assurer leur stabilité financière notamment afin de protéger leurs membres et de garantir leur sécurité informatique. », *op. cit.*, « Monnaies, banques et finance : vers une nouvelle ère crypto : un enjeu de souveraineté et de compétitivité économique, financière et monétaire », Rapport de l'Assemblée Nationale, rapporté par l'ancien député de Paris M. Pierre PERSON, 2022, p.194.
[467] BOUILLET-CORDONIER Ghislaine et al., « La Finance Numérique - Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs », p.146, *op. cit.* Disponible à l'adresse suivante

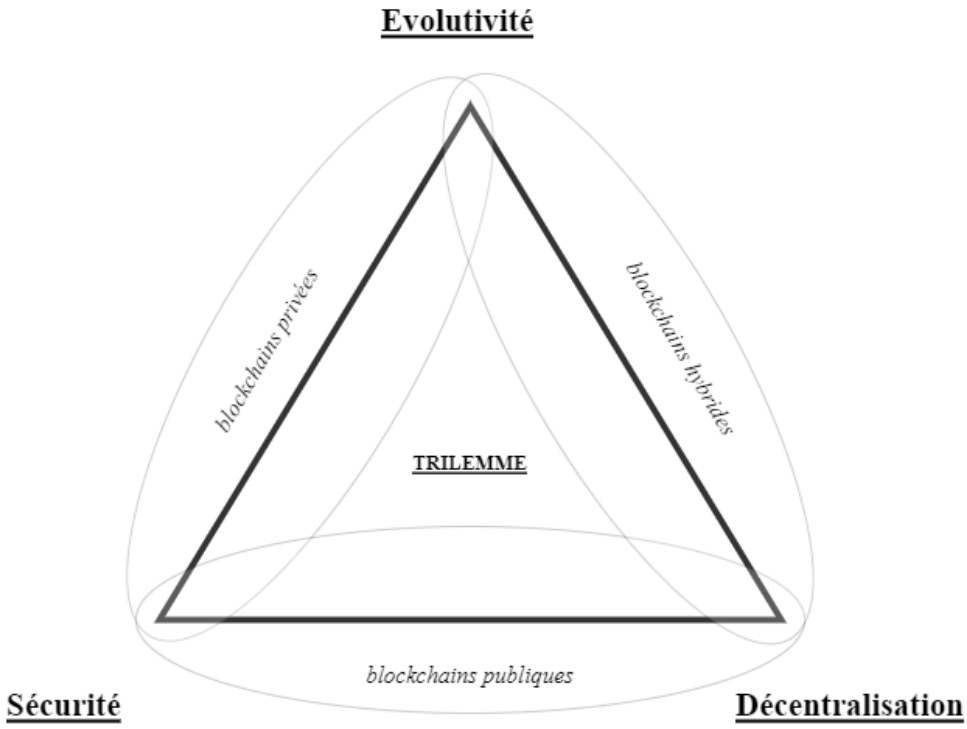
pécuniaires (réserves de sécurité) comme sur les marchés financiers traditionnels. Effectivement, un juge pourrait actuellement considérer qu'une DAO constitue de facto une société, ou bien que les règles de la fiducie prévues dans notre droit positif trouvent pleinement application. Notons qu'au Royaume-Uni, il a été demandé à la Commission juridique (« *Law Commission* ») d'entreprendre une étude de 15 mois à partir de l'été 2022 afin d'explorer et de décrire le traitement actuel des DAO, notamment pour identifier la façon dont elles devraient être traitées dans la loi, et clarifier leur statut et faciliter leur adoption[468]. En somme, les DAO représentent un nouvel outil 3.0 supposé au service des utilisateurs et de communautés en ligne, s'inscrivant dans la continuité de l'évolution du Web2.0 (incluant les blogs et les réseaux sociaux). La réflexion juridique et la jurisprudence autour des DAO façonneront l'évolution des usages des crypto-actifs qui y sont associés et plus largement de la finance décentralisée[469]. Du point de vue juridique, une zone floue subsiste, et chaque législateur national semble à juste titre laisser l'innovation s'exprimer à travers ces nouveaux véhicules socio-numériques de l'identité numérique. Si ces communautés numériques 3.0 permettront l'émergence de nouveaux modèles à vocation humaniste et pourtant au fonctionnement capitalistique, nul doute qu'elles pourront, selon leur degré de décentralisation, finalités et encadrement(s) juridique(s)[470], bénéficier aux internautes, tant en termes d'expérience utilisateur que d'exercice augmenté de leurs droits et de leurs obligations et responsabilités individuelles et collectives. Pour cela, les DAO doivent s'inscrire dans la continuité des systèmes sociaux et juridiques existants afin de limiter le phénomène d'arbitrage juridique qui consiste à choisir la législation la moins contraignante pour opérer avec un minimum de contraintes légales.

[468] « Decentralised Autonomous Organisations (DAOs) » | Law Commission, 2022, disponible à l'adresse suivante

[469] L'ACPR et la Banque de France ont publié en avril 2023 un rapport en faveur de la construction d'un cadre règlementaire applicable au secteur de la *finance décentralisée*, ou plutôt de la « *Finance désintermédiée* » (une distinction sémantique récente en écho au concept de degré de décentralisation qu'étudie cette recherche). Les mesures visant à réguler la DeFi se concentrent sur cinq axes clés. Tout d'abord ce rapport propose d'homologuer les infrastructures blockchains en imposant des normes minimales de protection et de sécurité. Deuxièmement, le contrôle des intermédiaires qui facilitent l'accès des utilisateurs aux services de la DeFi devrait être renforcé d'après ce rapport. Troisièmement, une évaluation objective des compétences financières des utilisateurs et de leur appétence au risque doit être imposée. Bien que ces mesures semblent bénéfiques pour les internautes, la mise en œuvre de telles propositions renforcera inévitablement une centralisation de ces solutions 3.0, par exemple soumis à une certification obligatoire concernant les contrats intelligents sur lesquels elles reposent. Si ces propositions ne sont pour le moment que théoriques, car s'accompagnent d'un sondage essentiel à destination des acteurs de ces écosystèmes, nul doute que le droit risque à nouveau d'introduire des règles de droit extrêmement contraignantes pour ces protocoles, écosystèmes et utilisateurs pourtant simplement à la recherche de plus de liberté, de pseudo-anonymat et d'alternative financière en ligne. v. ACPR, Banque de France. « Finance 'décentralisée' ou 'désintermédiée' : quelle réponse réglementaire ? », 2023, disponible à l'adresse suivante

[470] « Il s'agira de protéger les citoyens tout en conservant à l'esprit l'impérieuse nécessité de soutenir l'innovation et la compétitivité dans une logique de décentralisation. », *op. cit.* Rapport de l'Assemblée nationale, p. 193.

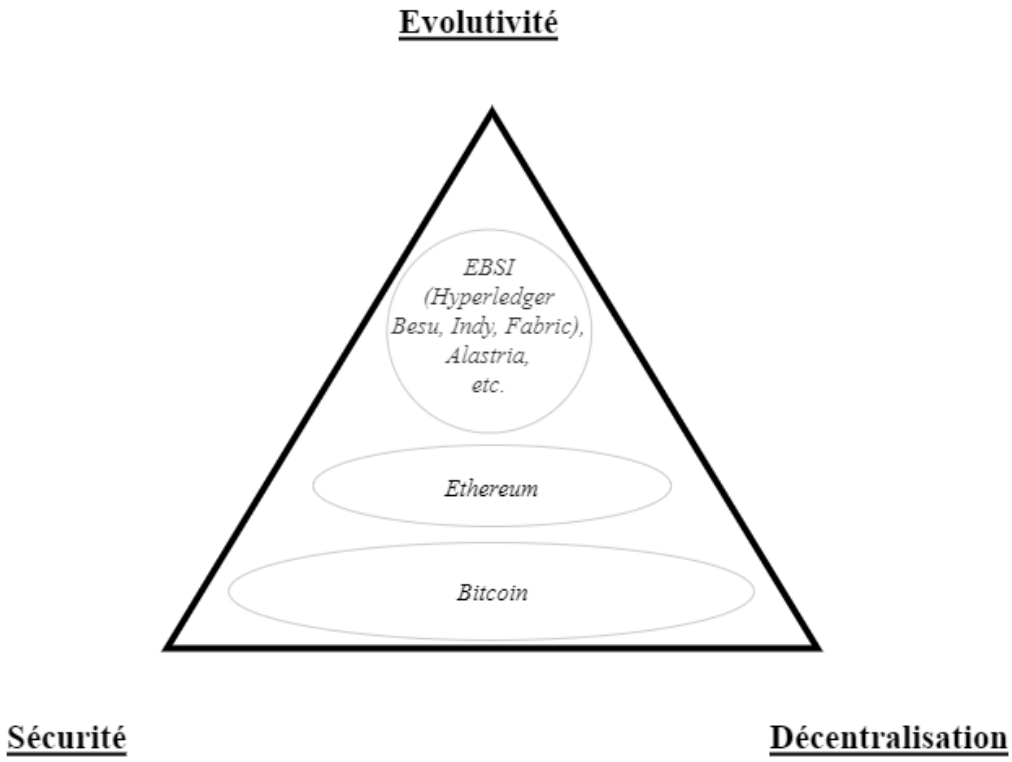
2.3.2 Le triangle d'incompatibilité des technologies blockchains



Le schéma présenté ci-dessus illustre une théorie informatique récente et renommée dans le domaine de la technologie blockchain, présentée pour la première fois en 2017 par Vitalik Buterin. La loi du « trilemme d'incompatibilité » s'applique à toute infrastructure blockchain, et énonce que cette dernière ne peut simultanément concilier trois aspects : (i) une évolutivité informatique, autrement dit la capacité à 'mettre à l'échelle' et faire évoluer l'infrastructure, (ii) une sécurité informatique, et (iii) une décentralisation informatique. Dans le schéma présenté, la sécurité et la décentralisation sont les deux piliers fondamentaux de la technologie blockchain, tandis que l'évolutivité en représente le défi majeur. Ainsi, comment atteindre un nombre suffisant d'ordinateurs pour assurer l'immutabilité du registre des transactions, tout en garantissant une rapidité de traitement des transactions sur le réseau ? En d'autres termes, ce trilemme informatique dispose qu'une blockchain et son écosystème ne peuvent idéalement avoir que deux choix techniques ou situations possibles à la fois[471]. En effet, comme le démontre la seconde version de ce schéma ci-dessous, une blockchain ne peut atteindre ou tendre que vers deux éléments parmi la décentralisation, l'évolutivité ou la sécurité (seul un côté du triangle illustré peut être atteint et nécessairement au détriment des deux autres). Fort de ce constat, les compromis sont donc inévitables face à ce trilemme consistant à parvenir à une évolutivité, sécurité et décentralisation informatique de manière simultanée. Par conséquent, une entité qui souhaite utiliser une blockchain doit

[471] (i) Une blockchain très sécurisée et évolutive (rapide), mais peu décentralisée ; (ii) Une blockchain très sécurisée et décentralisée, mais lente pour valider les transactions du registre ; (iii) Une blockchain évolutive et décentralisée au détriment de sa sécurité.

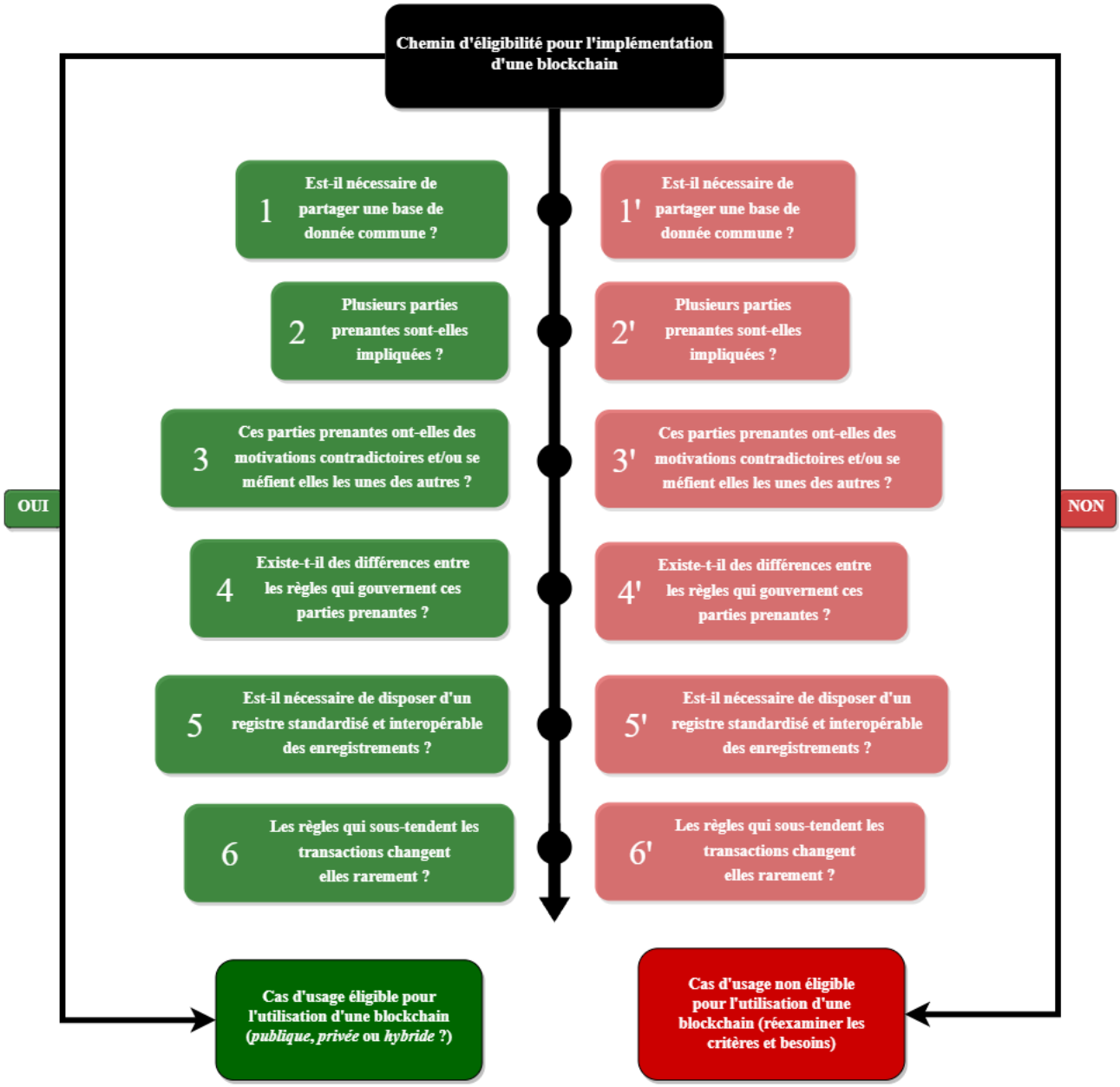
se positionner sur ce schéma, comme l'illustrent ces zones circulaires positionnant certaines des blockchains publiques (Bitcoin, Ethereum)[472], privées (Quorum, Corda)[473] et hybrides (Hyperledger Besu, Indy, Fabric)[474], les plus (re)connues à ce jour. Sur ce second schéma, chaque blockchain possède un positionnement spécifique et qui correspond à ses paramètres et fonctionnalités informatiques intrinsèques, généralement définis lors de la conception de son protocole[475]. Comme cela est mentionné et même avec un progrès technique continu, ce trilemme théorique ne pourra jamais être résolu par une blockchain pour des raisons matérielles et informatiques. Il convient finalement de souligner que sur ce schéma, la blockchain Bitcoin possède un haut degré de décentralisation et de sécurité, c'est-à-dire de résilience informatique (*v.* Annexe 3).



[472] Remarquons que si Ethereum est une blockchain publique, sa décentralisation informatique est à ce jour inférieure à celle de Bitcoin, ce qui signifie que son positionnement sur le schéma serait au-dessus et plus à gauche que celui de la blockchain Bitcoin. Si atteindre une *décentralisation pure* ou *totale* n'est pas une fin en soi, cela permet de protéger le protocole et toutes ses transactions antérieures contre toute tentative d'altération.
[473] Ces deux projets permettent aux entreprises de créer leurs propres *blockchains privées*, cf. site internet de Quorum et Corda
[474] Ce projet permet la création de *blockchains hybrides* grâce à des suites de protocoles *open source* (y compris d'autres blockchains publiques comme Ethereum).
[475] Nombre de nœuds, mécanisme de consensus (*v.* Annexes 3 puis 6), temps de validation entre chaque bloc, etc.

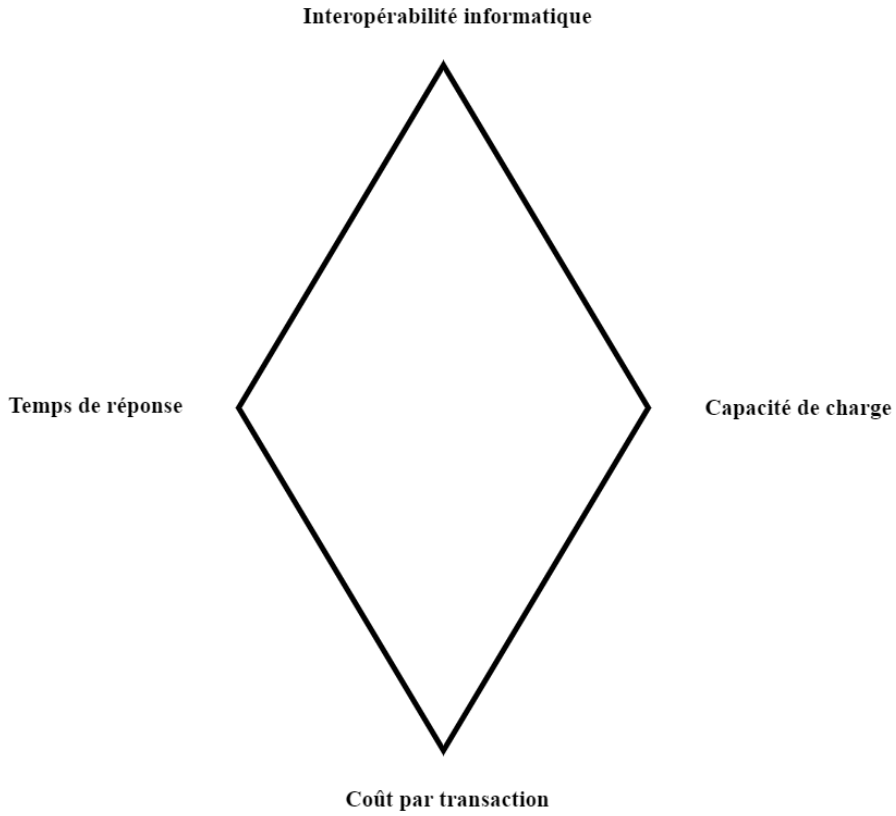
2.3.3 Chemin d’éligibilité et modèle d’affaire en losange des technologies blockchains

Il est essentiel pour une organisation de déterminer si l'utilisation d'un registre (semi)décentralisé est nécessaire ou non pour répondre aux besoins de son marché et de ses produits. Pour aider à cette réflexion, un processus de questionnement simplifié et non exhaustif désigné en tant que « chemin d'éligibilité d'une blockchain » est proposé afin de déterminer si l'utilisation d'une de ces variantes technologiques est pertinente pour une organisation.



Dans la continuité du triangle d'incompatibilité exposé au paragraphe précédent, ces quelques recherches théoriques proposent d’étendre ce même concept aux différents modèles d'affaires possibles pour une infrastructure blockchain, selon le point de vue d’une entreprise et de ses besoins en la matière. En effet, il semble possible de s’inspirer du triangle d'incompatibilité pour proposer un nouveau «

modèle d'affaires en losange » qui permet d'inclure de nouvelles notions au regard des facteurs clés de succès (FCS)[476] qu'une infrastructure blockchain doit respecter pour qu'une entreprise industrielle puisse l'implémenter et l'utiliser. Ce modèle théorique permet aux organisations et tout particulièrement aux entreprises, d'une part d'identifier leurs besoins récurrents pour de nombreux services en ligne, et d'autres part d'observer comment différentes blockchains peuvent se positionner au centre de ce schéma.



La première extrémité haute de ce losange fait référence à « l'interopérabilité », c'est-à-dire à la capacité d'une blockchain à communiquer informatiquement avec un ou plusieurs autres systèmes informatiques 2.0 et/ou 3.0 (grâce à des normes et standards techniques communs ou équivalents). La seconde extrémité opposée (« *coût par transaction* ») représente les ressources nécessaires au fonctionnement et à la validation de chacune des transactions de l'infrastructure blockchain en place (ce coût varie selon les types de blockchains et de leurs paramètres sous-jacents). La troisième extrémité à gauche désigne « *le temps de réponse* » informatiquement possible entre chaque transaction à la suite d'une demande pour obtenir une information inscrite sur ladite blockchain. Pour rappel, ce délai de réponse peut varier de quelques millisecondes pour un serveur centralisé, à plusieurs minutes pour une blockchain publique

[476] VERSTRAETE Thierry, « Les facteurs clés de succès sont les éléments ou les variables déterminantes qui contribuent à la réussite d'un projet, d'une entreprise ou d'une activité », « Faut-il toujours appeler les facteurs clés de succès : facteurs clés de succès ? », disponible à l'adresse suivante, p. 2, consulté le 18 mai 2021.

comme Bitcoin[477]. Enfin, la dernière extrémité à droite du losange (« *capacité de charge* ») fait référence à la capacité d'une blockchain à répondre à une forte augmentation de la demande de transactions dans un temps limité (certaines blockchains mettent ainsi en place des systèmes dits de « *seconde couche informatique* »[478] dédié). Remarquons que ces systèmes informatiques interconnectés à une blockchain permettent parfois d'améliorer la conformité juridique des blockchains auxquelles elles sont rattachées[479].

Au regard du chemin d'éligibilité précédent, il apparait que tout acteur qui souhaite utiliser ou interagir avec une blockchain doit répondre à un certain nombre de questions essentielles. Tout d'abord (i), il s'agit de comprendre et d'identifier quel type de blockchain et de gouvernance sont techniquement pertinents (blockchain publique, privée ou hybride) et (ii) en fonction de quel cas d'usage et secteur. Ensuite (iii), une étude d'impact juridique[480] est systématiquement recommandée afin d'identifier quelles sont les lois applicables ou susceptibles de l'être concernant ladite technologie/application 3.0. En fonction de la législation (iv), il convient d'inclure, dès le début du développement de l'infrastructure ou des applications, des exigences minimales et obligatoires selon le droit applicable (v). Poursuivant les idées et les parties précédentes, il est judicieux de présenter dans un tableau quatre scénarios envisageables quant aux conditions et aux probabilités d'adoption pour chaque type de blockchain :

[477] Entre chaque bloc de transactions un temps de validation d'environ 10 minutes est imposé en moyenne, ce délai étant propre à Bitcoin en permettant de renforcer sa sécurité informatique tout en lui conférant une importante prévisibilité (en anglais son protocole est ainsi surnommé la « Timechain »).
[478] V. Annexe 3, Focus 4. Les systèmes de seconde couche peuvent être attachés directement (« Layer 2 »), ou indirectement (« Sidechain »), à la blockchain et au protocole principal, avec des modalités informatiques qui peuvent varier en complexité et en similitude. En somme, un *Layer 2* repose sur la sécurité d'un réseau blockchain déjà existant, tandis qu'une *Sidechain* repose sur son propre modèle de sécurité informatique.
[479] « Les informations présentes sur une chaîne latérale [Layer 2] peuvent être facilement supprimées, ce qui permet aussi d'organiser un droit à l'oubli que n'autorise pas la logique initiale de la blockchain. », *op. cit*. BOUSQUET Marc, « Tout savoir sur le Bitcoin et les cryptomonnaies », in *Dossiers Science Hors-Série*, édition du Sens, ISSN : 2802-1843, novembre 2022, p.39.
[480] Une telle analyse peut contribuer à répondre à diverses questions, notamment : comment assurer la conformité légale et règlementaire de la blockchain ? Quelles données seront capturées et échangées ? Qui aura accès à ces informations ? Quels niveaux de confidentialité et de sécurité des données sont souhaités pour la solution ? Comment sera géré le flux de données et d'informations ?

CONDITIONS ET PROBABILITÉ D'ADOPTION PAR TYPE DE BLOCKCHAIN	**<u>Scénario 1 :</u>** ***Échec** des **blockchains publiques***	**<u>Scénario 2 :</u>** ***Échec** des **blockchains privées/hybrides***	**<u>Scénario 3 :</u>** ***Cohabitation** des blockchains **sans interopérabilité***	**<u>Scénario 4 :</u>** ***Cohabitation** des blockchains **avec interopérabilité***
Horizon(s) temporel(s)	Long terme	Court ou moyen terme	Court ou moyen terme	Long terme
Probabilité	Faible	Moyenne	Faible / Moyenne	Moyenne / Elevée
Conditions de réalisation (cumulatives)	- Rejet politique - Rejet juridique - Rejet social - Rejet économique et commercial	- Rejet économique et commercial - Rejet politique - Rejet social - Rejet informatique	- Rejet informatique - Rejet économique et commercial	- Acceptation politique - Acceptation juridique - Acceptation sociale - Acceptation économique et commerciale - Acceptation informatique
Explications et pistes de réflexion	A long terme, il semble exister une faible probabilité que les blockchains publiques disparaissent au profit de celles privées/consortium, en raison de rejets successivement politiques, sociaux, juridiques, économiques et commerciaux.	A court ou moyen terme, il semble exister une probabilité moyenne que les promesses économiques, commerciales, politiques, sociales et informatiques des blockchains privées et consortiums échouent au profit de celles publiques.	A court ou moyen terme, il semble exister une probabilité faible ou moyenne que les blockchains publiques, privées et hybrides cohabitent sans être interopérables entre elles, car cela implique le rejet d'une recherche d'interopérabilité informatique (opposé aux pratiques actuelles du marché) ainsi qu'une segmentation économique et commerciale de chaque blockchain	A long terme, il semble qu'il existe une probabilité moyenne ou importante que les blockchains publiques, privées et hybrides cohabitent sur des marchés et des usages multiples, de façon complémentaire et interopérable. Cela repose sur une acceptation politique, sociale, économique et commerciale ainsi qu'informatique, plus ou moins longue selon les

			pour des marchés et usages cloisonnés (ce qui est rare et s'applique à une minorité de marchés).	situations observées.

Titre 2 : Un droit stable face à une constante mutation technologique et sociale

Chapitre 1 : Le droit à l'ère d'une société numérique, entre promesses et défis

Au XIXè siècle, l'industrialisation et les progrès technologiques suscitaient des critiques en raison des impacts économiques, sociaux, politiques et environnementaux de leurs activités. Il s'agit d'enjeux toujours d'actualité pour toutes nouvelles technologies, y compris celles du numérique. Au début des années 2000, l'informatique était considérée comme une solution technique sans conséquence environnementale puisqu'elle était immatérielle et transfrontalière et en plus du fait qu'elle n'était fournie que par une poignée d'acteurs en avance technologique (masquant ainsi certains coûts sociaux dont écologique pour la société). Il semble donc important de distinguer le progrès technologique du progrès social, car chaque avancée technologique ne garantit pas systématiquement un réel progrès social pour la société. La transparence numérique doit être vérifiable afin de recréer une confiance numérique avec des preuves tangibles au bénéfice des citoyens. L'identité numérique décentralisée, étudiée plus loin en deuxième partie de cette étude, ainsi que les blockchains publiques, peuvent être une source de progrès majeur avec des effets économiques et sociétaux bénéfiques pour les individus, à condition de maîtriser leurs effets écologiques par exemple avec une approche « Low Tech »[481]. Chaque nouvelle technologie numérique représente un progrès technique, mais il est essentiel de l'évaluer de manière objective au regard des règles de droit elles-mêmes calquées sur les besoins de la société.

1.1 La démocratie au regard des nouvelles technologies

La démocratie est perçue comme l'émanation d'une volonté collective généralement exprimée par des processus de votes et d'élections. Cette vision collective de la société se trouve confrontée à l'individualisme croissant des individus dont les intérêts personnels sont parfois en contradiction avec une vision collective. L'accroissement des revendications personnelles[482] peut toutefois permettre, avec les possibilités du numérique, d'acquérir un nouveau pouvoir collectif qui peut être transposé au sein de l'univers physique (lanceur d'alerte, vote anonyme en ligne, etc.). L'interconnexion sociale inédite que permet le numérique vient aussi bouleverser certains processus sociaux traditionnels par la possibilité

[481] V. Annexe 3, Focus 6.
[482] *Op. cit.* Présentation dans cette courbe du nombre d'apparition du terme « identité » dans la littérature depuis 1800 à 2019, disponible à l'adresse suivante

d'une émancipation numérique des personnes et de leur identité (droits et libertés fondamentales, données, opinions). L'image utopique, mais largement répandue, d'une démocratie participative et directe comme dans la Grèce antique peut devenir difficilement applicable au contexte actuel en raison d'une croissance rapide de la population mondiale couplé à la hausse de revendications identitaires et politiques. Il semble que la démocratie[483] repose étroitement sur la liberté d'expression des différents groupes qui composent une société, ainsi que sur la légitimité du pouvoir en place et la présence de contre-pouvoirs œuvrant en principe pour l'intérêt général. Cela permet à la population de s'autogouverner en protégeant les valeurs fondamentales essentielles pour le bien commun[484].

Les nouvelles technologies blockchains et l'identité numérique décentralisée précitée, faisant l'objet d'une étude détaillée au titre deuxième de l'étude, apparaissent comme des contre-pouvoirs au service de certaines libertés fondamentales. Ces nouvelles technologies permettent en effet de former des biens communs numériques tels le bitcoin et l'Ethereum[485] au service d'une société numérique un peu plus dirigée par les internautes qui peuvent désormais questionner le rôle de certains acteurs institutionnels. Par exemple, le droit bancaire et financier repose sur le besoin d'intermédiation dont le Web 3.0 peut se passer. Ces nouvelles technologies permettent de fait une formidable libéralisation d'actes de toutes les communautés, sans aucune frontière, pouvant se structurer en ligne pour transmettre et revendiquer leurs messages et valeurs. Ces nouvelles possibilités permettraient, en théorie, de renouer avec une démocratie plus directe. La numérisation et la décentralisation des interactions font ainsi miroiter aux internautes de nouveaux modèles sociaux en ligne, avec moins d'Etats et d'intermédiaires de confiance, partiellement remis en question. Ces nouvelles technologies redessinent par conséquent le contrat social de Jean-Jacques Rousseau[486], en conférant un nouveau pouvoir d'influence individuel aux personnes, en quête de leur autonomie personnelle, désormais bien au-delà du pouvoir politique et social des urnes. Dès lors, si le numérique peut favoriser l'exercice de la démocratie, il peut tout autant l'affecter et engendrer des comportements antidémocratiques. Il est fait référence à des actions illégales perpétrées et diffusées à distance par des internautes pseudo-anonymes, comme la diffusion massive de fausses informations, la psychométrie comportementale[487], les « *deep fake* »[488] ou les rumeurs numériques. Pour les opérateurs de la sphère numérique, qu'il s'agisse de grandes entreprises technologiques ou d'Etats, la possibilité technique d'une surveillance généralisée des populations peut progressivement l'emporter sur un Etat de droit et ses valeurs démocratiques, particulièrement en période de transitions politiques

[483] Terme issu du grec « *dêmos* » pour « *peuple* », « *daíomai* » pour « *distribuer* » et « *kratein* » pour « *commander* ».
[484] MAALOUF Amin, « Ce qui est sacré, dans la démocratie, ce sont les valeurs [la dignité humaine], pas les mécanismes [politiques]. », *op. it.* « *Les identités meurtrières* », p.178.
[485] V. Annexe 3 et Annexe 6.
[486] ROUSSEAU Jean-Jacques, « Du contrat social - ou principes du droit politique », disponible à l'adresse suivante
[487] Il s'agit de l'étude psychologique des comportements numériques des internautes. Cette nouvelle matière, largement utilisée par *Cambridge Analytica*, est aujourd'hui considérée comme une nouvelle arme numérique par la Commission européenne. Ces plateformes originellement créées pour nous connecter deviennent aujourd'hui des outils au service de la géopolitique.
[488] Il s'agit de l'animation d'une photo ou d'une vidéo grâce à l'intelligence artificielle pour exprimer des propos ou comportements qui ne proviennent pas de la personne physique ciblée, *v.* en ce sens la récente photo du Pape, « Cette photo du Pape en doudoune qui affole le web est un fake créé par l'IA », 28 mars 2023, in *journaldugeek.com.*

majeures. S'exprimant lors d'une conférence au CERN en 2019, le père fondateur d'Internet Sir Tim Berners-Lee se questionne *« où se trouve l'équilibre entre laisser les entreprises technologiques faire ce qu'il faut et les réglementer ? Où se trouve l'équilibre entre la liberté d'expression et les discours de haine ?* (…) » et poursuit « *oups ! Le web n'est pas le web que nous voulions à tous égards »*[489]. Il semble que ce dilemme entre liberté numérique et dépendance informatique s'intensifie de jour en jour, par exemple au regard de l'adoption prochaine d'un euro numérique parfois jugé controversé et source d'inquiétudes au sens de certains experts du numérique.

Si la décentralisation d'Internet que permet la technologie blockchain, couplée au contrôle de ses données que permet l'identité décentralisée que nous évoquons plus loin, reflète la mise en place d'une possible démocratie numérique directe[490], il faut considérer que cette utopie numérique ne doit pas faire oublier que la démocratie représentative reste une solution réaliste et plutôt équilibrée au regard de la complexité de la société. Ces technologies sont souvent considérées de manière ambivalente, parce que d'un côté, perçues comme des moyens novateurs d'implication et de participation démocratique sans précédent en ligne, et d'un autre côté, considérées comme des outils qui enfreignent les règles collectives et qui ne profitent qu'à des personnes individualistes. Pour maintenir des fondements démocratiques, il faut veiller à ce que la règle de droit institue des droits et devoirs pour chaque citoyen. L'informatique ne possédant pas en théorie d'autres règles que celles imposées par les communautés de développeurs, il convient de se demander si la loi façonne l'informatique ou si c'est l'informatique qui façonne la loi[491]. En effet, l'auteure scientifique et numéricienne Aurélie Jean rappelle « *il demeure vrai que les algorithmes et leurs protagonistes influencent indirectement (ou pas) la loi, tant la discipline est complexe, les législateurs sont démunis en termes de compétences dans le domaine, et les géants de la tech puissants* »[492]. De manière concrète, les blockchains publiques semblent augmenter la liberté d'information, d'expression et de communication des citoyens, comme cela a été observé par exemple avec la création, au début d'Internet, d'une version numérique inédite du Journal officiel de la République française (JORF) et de services publics en ligne. La liberté de la presse et la liberté d'entreprendre se trouvent par conséquent renforcées par l'utilisation d'une blockchain publique, surtout dans les pays où l'exercice de la démocratie est restreint, parfois inexistant. D'après cette démonstration, les blockchains publiques ont le potentiel de révolutionner les pays en voie de développement en offrant des solutions innovantes pour résoudre les problèmes de corruption, de transparence et d'inclusion financières. Dans ces pays, la corruption est endémique et ce sont les personnes les plus vulnérables qui sont les plus touchées. Les blockchains publiques peuvent offrir une solution en permettant, grâce à une traçabilité de transactions de diverses natures (financières, organisationnelles, contractuelles) de former en ligne et

[489] Associated Press, « Father of World Wide Web Tim Berners-Lee says what his creation has become isn't the web we wanted », in *dailymail.co.uk*, 2019, consulté à l'adresse suivante
[490] La technologie blockchain en tant que registre numérique infalsifiable des données et l'identité décentralisée en tant que preuve suffisante de citoyenneté.
[491] LESSIG Lawrence, « Code is Law: on liberty in cyberspace », in *Harvard Magazine*, 2000, *op. cit.*
[492] JEAN Aurélie, « Les algorithmes font-ils la loi ? », in *Humensis*, 2021, position de lecture dans le livre : 94%.

en toute confiance une alternative au service de l'expression démocratique. Par conséquent, la digitalisation des interactions sociales implique un changement dans l'exercice de certains droits et libertés fondamentales. Il faut soutenir cette évolution pour permettre une extension plus efficace des droits en ligne tout en restant fidèles aux règles cryptographiques et aux règles de droit, notamment le Règlement RGPD[493] et le Règlement eIDAS[494] qui sont étudiés plus loin. Par principe, rien ne devrait être plus important dans une démocratie que l'émancipation personnelle de ses citoyens. Dans une démocratie représentative, l'Etat doit former ses citoyens à l'utilisation de technologies émancipatrices telles que l'identité décentralisée ou l'utilisation de crypto-actifs par exemple. Si le citoyen est condamné à être ou à devenir un cybercitoyen, il lui appartient cependant d'en choisir les conditions, c'est-à-dire de décider en toute transparence et confiance, de l'utilisation des nouvelles technologies mises à sa disposition.

1.1.1 Le cyberespace comme lieu de souveraineté et d'autonomie juridique

Cette étude fait état d'une asymétrie entre l'exercice des droits des personnes dans le monde réel et l'exercice de ces mêmes droits dans le monde virtuel. Cette forme de distance et de latence incompressible entre l'exercice des nouvelles technologies et l'exercice du droit semble progressivement s'immiscer dans la vie numérique des personnes pendant un laps de temps propre à chaque situation d'identification *phygitale*. En réalité, il s'agit d'une course sans fin, car les technologies évoluent, disruptent puis distancent sans cesse le droit[495]. La notion de cyberespace est en effet un concept complexe à définir. Il peut être défini comme un espace de communication immatériel créé par une interconnexion mondiale entre des ordinateurs. Lieu de rencontres économiques, culturelles et plus largement sociales, il représente un nouvel espace virtuel parfois perçu par certains internautes comme un territoire numérique[496] qui garantirait un espace informationnel empreint de liberté, de transparence, de partage, d'égalité ou de progrès. En réalité, il semble que les frontières de cette toile Internet ne soient pas physiques, mais surtout idéologiques et donc infinies, chaque personne pouvant se trouver à plusieurs endroits en même temps et de façon instantanée afin de réaliser des tâches aussi diverses que variées, avec une liberté de navigation totale, une sorte de liberté de circulation numérique. L'utilisation d'Internet et de ses nouvelles technologies nous amène à revisiter le concept de souveraineté numérique avec une acceptation contemporaine[497]. Plutôt que d'essayer de proposer une définition générale de la

[493] V. *infra*, II, Titre I, chap 2. 1.1
[494] V. *infra*, II, Titre 1, 2.1.1.1
[495] V. Annexe 4.
[496] Ce nouvel eldorado et territoire numérique fait depuis sa création l'objet de nombreuses références géographiques, pour le décrire « naviguer sur le web », « ports internet », « l'information transitent par des canaux », etc.
[497] BELLANGER Pierre, *La Souveraineté Numérique, op. cit.* 2014.

notion de souveraineté à l'ère numérique, il semble plutôt pertinent d'évoquer les perspectives suivantes :

(i) Initialement, la souveraineté d'un État se définit comme sa capacité à être autonome en matière de gestion de sa population et de son territoire. Bien que cette capacité de contrôle s'étende également à la sphère numérique, elle prend plus de temps à être établie en raison de l'évolution constante des écosystèmes numériques disruptifs qui revendiquent leur propre autonomie et souveraineté informatique, économique et politique. La souveraineté étatique au sens juridique peine ainsi à s'imposer dans la sphère numérique et tend vers une souveraineté collective et nationale visant à assurer la protection des internautes-citoyens face à des opportunités numériques parfois génératrices de risques à court et moyen termes. Dans la partie suivante, il est mentionné que la souveraineté numérique est également associée aux grandes entreprises technologiques, dont les pouvoirs économiques, techniques, sociaux et juridiques sont en constante augmentation, influençant la société à la fois de manière positive et négative.

(ii) En ce qui concerne les entreprises, la souveraineté se réfère principalement à leur capacité à être indépendantes et à avoir une marge de manœuvre stratégique en raison de leur taille et de changements permanents des contextes sociaux.

(iii) Pour les citoyens et internautes, la souveraineté s'apparente à une liberté personnelle ou collective, d'action et de choix. Cette capacité individualiste à influencer son environnement proche reste toutefois limitée face aux définitions précédentes, chaque internaute en ligne a conscience que sa maîtrise personnelle et par extension sa souveraineté numérique sont restreintes et dépendent de fournisseurs de services numériques. En dépit de ce fatalisme que combattent les systèmes décentralisés, certains services en ligne favorisent tout de même cette capacité à s'autodéfinir en ligne (jeux vidéo, messageries chiffrées). Ainsi, regroupés en communautés, les internautes peuvent créer de nouvelles conditions pour favoriser l'émergence d'une souveraineté numérique pour leur communauté. Cette souveraineté est ainsi contextualisée, mais tend à croître en principe dans la limite pratique du respect des règles de droit protégeant les internautes. Dans les faits, cette souveraineté individuelle est largement subordonnée à un degré de maîtrise et de compréhension suffisant des systèmes numériques, ce qui est aujourd'hui le cas seulement pour une minorité d'internautes.

Finalement, la pluralité de définitions possibles pour le concept de souveraineté fait qu'elle ne peut être seulement circonscrite à son acceptation étatique, autoritaire ou juridique. Il s'agit d'appréhender cette notion sous un angle individuel, celui de l'existence numérique et de sa maîtrise pour l'autodétermination numérique des personnes et dans sa globalité. En réalité, il semble que la société

soit en train de se diriger vers une forme de concurrence entre plusieurs définitions complémentaires du concept de souveraineté numérique. Il est probable que la définition traditionnelle persiste en raison d'un Etat de droit dans les pays développés, mais il ne fait pas de doute que les acteurs économiques vont lutter pour défendre leurs modèles commerciaux. Toutefois, cette même lutte ne doit pas compromettre la définition citoyenne de souveraineté numérique que nous soutenons au profit des internautes, et particulièrement au profit de ceux vivant dans un Etat de droit perçu comme faible dans certains pays en voie de développement.

1.2 Le temps court de l'innovation face au temps long de la régulation

Les acteurs économiques souhaitent, selon leurs besoins et leurs situations, que le droit s'applique soit dans un temps expéditif à leur profit, soit dans un temps plus long. L'innovation technologique est un processus en apparence court grâce aux révolutions techniques et sociales qu'elle peut rapidement engendrer[498]. Du fait qu'une donnée est toujours accompagnée d'autres données ou métadonnées, il convient de la considérer comme étant fluide plutôt que statique. C'est cette fluidité intrinsèque à l'informatique qui est ainsi à l'origine des difficultés d'appréhension des notions d'espace et de temps, spécifiques en informatique, et que les juristes rencontrent parfois avec difficulté[499]. Mais il semble que toute innovation technologique requiert aussi un temps long préalable, souvent invisible pour les néophytes, qui se cantonne pendant un certain temps à un cercle restreint de technophiles avisés[500]. Comme cela a été mentionné dans les parties précédentes, Internet est en réalité le fruit de plusieurs décennies de développement informatique et social, un constat similaire pouvant être attribué aux développements des téléphones mobiles ou encore de l'identité numérique comme évoqué. Dès lors, si le temps de l'innovation et le temps de la régulation passent nécessairement tous deux par un temps long, comment expliquer l'écart de perception et de ressenti temporel entre l'évolution perçue comme rapide des nouvelles technologies et celle perçue comme longue en termes de législation applicable ? Une explication possible serait que la nature complexe et en constante évolution de l'innovation ne peut être pleinement comprise et accessible qu'à un petit groupe de personnes, principalement des développeurs[501]. Bien que les développements informatiques open source soient disponibles publiquement, cette restriction sociale liée aux compétences spécifiques impose une barrière technique qui ne peut être franchie que par certains événements[502] qui peuvent conduire à une diffusion rapide et

[498] LASSEGUE Jean, GARAPON Antoine, « S'agissant du temps, le numérique détruit la durée vécue : (…) il contracte le temps d'un échange à presque rien […] », 11 avril 2018, « Justice digital », PUF, p.120.
[499] *Ibid.* « L'innovation se dit toujours au service du droit mais elle est aussi au service du business car (…) les deux sont inséparables […] », p.99.
[500] V. *supra*, II, Titre 2, 1.3.1
[501] De FILIPPI Primavera, WRIGHT Aaron, « Même si le code des contrats intelligents est disponible publiquement sur Internet pour que tout le monde puisse l'examiner, seul un petit nombre de personnes est capable de vérifier ce code », « Blockchain and the law : the rule of code », 9 avril 2018, in *Harvard University Press*. Emplacement 2759 sur 7004.
[502] Par exemple lorsque de grandes entreprises technologiques décident de s'emparer d'une nouvelle technologie, d'en adopter les standards et d'en promouvoir les mérites, *v. infra*, II, Titre 1, 1.3.1

massive de l'innovation dans la sphère publique et sociale, créant ainsi une adoption exponentielle qui se nourrit d'elle-même. À cet égard, le citoyen et l'internaute ne perçoivent pas ces temporalités comme longues, mais plutôt comme fulgurantes, en accord avec la « *loi de Fraisse* »[503] du psychologue français Paul Fraisse connu pour ses travaux sur la perception du temps. Ainsi, ce n'est pas l'innovation qui est fulgurante, mais plutôt son adoption sociale, en raison d'une circulation de l'information désormais phénoménale via notamment les réseaux sociaux numériques[504]. En droit, l'information n'a pourtant pas pour vocation à circuler rapidement, mais plutôt à faire respecter les textes et les procédures dont les conditions sont dûment identifiées et encadrées, aux fins d'assurer une équité et une transparence devant la loi. Ce temps long de la régulation est le fruit de discussions publiques, convergentes et contradictoires, afin d'essayer d'appréhender au mieux l'encadrement de nouveaux phénomènes technologiques impactant la société. Ce premier processus de récolte et d'échange d'informations semble ainsi plus long et fastidieux[505], face au fonctionnement silencieux et en apparence plus rapide de l'innovation. Si les métiers de juristes et de développeurs sont à cet égard des métiers-passions, force est de constater que l'émotion n'est pas gérée de la même façon dans ces deux écosystèmes : être juriste revient à se concentrer sur les règles de droit à établir, tandis que les développeurs laissent libre cours à leurs émotions personnelles lorsqu'ils programment des règles informatiques, dont seuls les utilisateurs finaux seront des juges partiaux. Ces quelques constats n'ont pas pour objet de démontrer que la lenteur de la régulation est néfaste à l'innovation, bien au contraire, il s'agit de comprendre pourquoi des différences structurelles existent et comment elles peuvent être articulées ensemble malgré leur persistance. En définitive, il s'agit de considérer que le temps (long) n'est pas une durée (fixe). En d'autres termes, la régulation doit laisser le temps à l'innovation de faire son œuvre avec un encadrement juridique minimum en raison de règles de droit[506] à mettre en place, avant éventuellement de fixer dans un second temps, une régulation adaptée dans une durée clairement définie. Ainsi, les temps de l'innovation se chevauchent sans se confronter, grâce à une distanciation de leur temporalité respective « (…) *si la loi est souvent conservatrice du fait de son établissement souvent en décalage avec les pratiques sociales et économiques, elle se doit d'anticiper au mieux les scénarios et les changements technologiques, médicaux ou encore sociétaux pour pouvoir perdurer. Force est de souligner que le RGPD est apparu dix ans après la création de Google* »[507]. Finalement, si l'innovation est indéniablement source de bouleversement pour le droit, il s'agit pour les juristes de tenter d'identifier

[503] Cette loi du nom du psychologue français qui l'énonce, suppose que plus une tâche à accomplir nous passionne et procure du plaisir, plus la notion de temps nous semble courte, « Plus une tâche a d'unité, plus elle risque de paraître intéressante. L'unité renforce la motivation (...). Plus une tâche a une unité, plus elle paraît courte », FRAISSE Paul, « Psychologie du temps », 1975, Ed. PUF.
[504] WOITIER Chloé, « Elon Musk et des centaines d'experts réclament une pause dans l'IA, évoquant 'des risques majeurs pour l'humanité' », 29 mars 2023, AFP Agence, in *Le Figaro*.
[505] JEAN Aurélie, « Les lois s'inscrivent par définition dans les temps longs. La loi est même généralement perçue comme conservatrice dans la mesure où les textes arrivent bien souvent en décalage, pour ne pas dire en retard, avec les pratiques sociales », version en ligne in *decitre.fr*, Ed. Humensis, 2021, position de lecture dans le livre : 8%.
[506] *Ibid.* « Comme le RGPD a réussi à le faire, faisons du temps un allié et non une menace par une législation qui autorise tout en encadrant strictement et en réprimant sévèrement », Position de lecture dans le livre : 66%.
[507] *Ibid.* Position de lecture dans le livre : 65%.

puis d'anticiper à quel moment une adoption massive par la société est susceptible d'advenir, ce qui implique se former aux technologies 2.0 puis 3.0. Les crypto-actifs (blockchains publiques) sont par exemple en phase d'atteindre ce point d'adoption pivot, tandis que les blockchains privées et hybrides ne l'ont pas encore atteint au même titre que l'identité décentralisée comme cela est exposé plus loin.

1.3 La protection des libertés en ligne : droit au respect de la vie privée et intégrité numérique

Il y a huit ans déjà, le fondateur et Président du média Skyrock expliquait dans un livre que « *la captation indolore de nos vies privées en contrepartie de services, si séduisants soient-ils au départ, est aujourd'hui une gratuité fallacieuse dont le prix futur n'est même pas quantifiable tant il impactera nos vies* »[508]. Ce constat tend toutefois à être progressivement remis en question par les internautes et le législateur depuis l'adoption de diverses lois dédiées à la protection des données. Le droit au respect de la vie privée est un droit fondamental qui doit s'exercer au profit de tout internaute. Il est essentiel à son autonomie et plus généralement à la protection de la dignité humaine[509]. Il permet à d'autres libertés fondamentales de s'y rattacher (liberté de culte, d'expression, etc.). Par principe « *ce qui est illégal hors ligne doit également être illégal en ligne. Les valeurs et les règles éthiques européennes ainsi que les normes sociales et environnementales doivent s'appliquer également dans l'espace numérique* »[510]. La technologie a toujours été intimement liée aux droits des personnes. Pour illustration, nos capacités à protéger la vie privée sont aujourd'hui plus importantes que jamais grâce à divers outils numériques[511] et cryptographiques dont le ZKP[512] étudié au titre deuxième de notre recherche, bien que les capacités de surveillance soient proportionnellement égales voire plus importantes qu'auparavant, selon les pays et doctrines sociales et culturelles retenues. Il est désormais possible d'identifier de manière unique les individus parmi les masses de flux de données dans l'univers numérique, ce qui peut compromettre leur capacité de prise de décision et d'utilisation de manière consciente ou inconsciente. Certaines organisations, entreprises et gouvernements, ont la capacité de surveiller chaque conversation, chaque relation commerciale et chaque lieu visité. Ces capacités, latentes ou exercées, peuvent avoir des effets négatifs sur les individus, les groupes et plus généralement la société, car elles peuvent freiner l'action des citoyens, exclure et discriminer des personnes physiques. Autrement dit, ces organisations ont le pouvoir d'influencer la façon dont les individus pensent et gèrent leurs relations avec les marchés et les différentes branches d'un État de droit, parfois sans que les personnes concernées n'en soient

[508] BELLANGER Pierre, « La Souveraineté Numérique », 2014, *op. cit.* Emplacement 2315 et 2331 sur 3565.
[509] V. Art. 6 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 : « Tous les citoyens étant égaux (…) sont également admissibles à toutes dignités (…) ».
[510] *Op. cit.*, CE, traduction libre de l'anglais, « Communication shaping europes digital future », *op. cit.*, consulté en ligne le 20 décembre 2021, p.6.
[511] Mooc Inria, ICN–SNT–Python, 2019-2021, « [...] les technologies de l'information et de la communication (Tic) ne sont pas définitivement et indubitablement des menaces pour la vie privée. On peut effectivement aussi concevoir des nouvelles techniques visant à protéger la vie privée et résoudre le genre de hiatus évoqué avec le big data », in *Informatique et culture scientifique du numérique*, p.67.
[512] V. *infra*, II, Titre 1, 2.2.6.1

véritablement conscientes[513]. L'adoption croissante de services et de technologies centralisés conduit progressivement à une perte de contrôle et à une certaine ignorance en raison de la surveillance généralisée dont les internautes peuvent être victimes. Ces derniers ont souvent peu de connaissances en informatique pour remettre en question les fondements de cette surveillance. L'une des composantes essentielles du droit à la vie privée est le droit à la protection des données personnelles et certains instruments internationaux prévoient des dispositions juridiques spécifiques à cet effet[514]. Le droit au respect de la vie privée est souvent considéré comme intangible ce qui peut amener certaines personnes à penser que leur vie privée n'est pas importante, car elles n'auraient rien à cacher, mais cela reviendrait à dire qu'elles ne considèrent pas d'autres droits tels que ceux portant sur la liberté d'expression ou la liberté de la presse simplement parce qu'elles n'ont rien à dire ou à écrire.

D'après l'auteur et philosophe français Gaspard Koenig[515], la disparition programmée du libre arbitre dans la sphère numérique ferait l'objet d'un consensus théorique. Dans le même temps les travaux du célèbre économiste et psychologue américano-israélien Daniel Kahneman selon lesquels l'individu est constamment confronté à ses propres illusions et biais cognitifs, couplés aux travaux sur l'influence comportementale (« *Nudge* »[516]) de l'économiste Richard Thaler, ainsi qu'aux recherches de l'auteur et psychologue français en neuropsychologie Stanislas Dehaene sur la neuroscience, tendent à confirmer que l'identité des personnes en ligne est altérée, voire aliénée, par les grandes entreprises du numérique. Du point de vue des internautes, ce n'est plus seulement l'État qui pourrait être considéré comme l'ennemi du respect des droits à la vie privée et à la liberté en ligne[517], mais également et surtout certaines grandes entreprises technologiques. Les outils numériques sophistiqués des grandes entreprises technologiques privées contribuent à un effacement des individualités des personnes, ce qui signifie que plus les individus perdent leur singularité, moins ils sont capables de revendiquer une identité libre et démocratique. Face à ces manipulations de données et transposition des identités, il ne s'agit pas de condamner et d'éviter les nouvelles technologies mais de se les approprier. Le rôle de l'État est de rendre l'individu autonome, c'est-à-dire de lui fournir les moyens techniques pour se réapproprier ses données et identités numériques. Ainsi, la vie privée doit être sécurisée par défaut et par conception, grâce à de nouvelles technologies et mécanismes plus respectueux et moins gourmands en données personnelles. Cette protection technologique et juridique doit être garantie par les grandes entreprises technologiques ainsi que par les États, qui ne sont pas encore assez incités à le faire par les citoyens et les internautes

[513] Le Monde AFP, « Espionnage de journalistes et d'opposants : l'affaire 'Pegasus' provoque l'indignation », 4 novembre 2022, in *LeMonde.fr*
[514] V. notamment : art. 14 de la CNU sur les travailleurs migrants, art. 16 de la CNU sur les droits de l'enfant, art. 10 de la Charte africaine des droits et du bien-être de l'enfant, art. 4 des principes de l'Union africaine sur la liberté d'expression (droit d'accès à l'information), art. 11 de la Convention américaine relative aux droits de l'homme, art. 5 de la Déclaration américaine des droits et devoirs de l'homme, art. 16 et 21 de la Charte arabe des droits de l'homme, art. 21 de la DDH, art. 8 de la CEDH.
[515] FERRY Luc, in *Le Figaro*, en ligne, publié le 23 octobre 2019, consulté le 18 novembre 2021.
[516] Le « Nudging » ou « Coup de pouce » en français consiste à inciter les personnes à prendre certaines décisions inconscientes, grâce à des mécanismes d'incitation psychologiques. L'objectif est de les amener dans une direction pour leur propre bien ou pour le bien collectif, selon certaines circonstances. ELIE Pauline, « Gare à la tyrannie des "coups de coude". Les "nudges" vous veulent-ils (vraiment) du bien ? », 2022, disponible à l'adresse suivante
[517] CEDH, « Surveillance de masse – fiche thématique », 2022, disponible à l'adresse suivante

eux-mêmes. Actuellement, l'informatique et la recherche juridique sont largement considérées comme des matières indépendantes l'une de l'autre. Cette situation crée une incertitude juridique pour les entités qui cherchent à traiter des ensembles de données pseudo-anonymes (évoquées dans la partie suivante), et peut même entraîner une confusion terminologique généralisée pour le grand public qui bénéficie pourtant de cette protection et de ces mécanismes qui lui sont ainsi hors de portée. En réalité, le Règlement général sur la protection des données (RGPD) déjà évoqué, ne semble pas entièrement répondre aux attentes en matière de protection des données personnelles. La confidentialité devrait être un droit garanti et facilement accessible lors de l'utilisation de sites web, et non une action que les utilisateurs doivent rechercher à exercer à travers des procédures longues et parfois coûteuses. Depuis 2021, plusieurs juristes suisses proposent l'adoption d'un nouveau droit à l'intégrité numérique[518]. Leur ambition est de développer un nouveau droit fondamental à l'intégrité numérique, c'est-à-dire quelques principes généraux et impersonnels que chacun puisse comprendre et faire respecter. Il s'agit, en plus de l'intégrité mentale et physique de la personne humaine d'inclure et de garantir une nouvelle dimension numérique qui serait issue de cette protection initialement physique. Par exemple, lors d'un vote en présentiel, une personne peut difficilement être influencée en raison du caractère public dans lequel le vote se déroule (diverses procédures assurent précisément l'intégrité du vote de chaque citoyen, exemple de l'isoloir). A l'inverse, lors d'un vote en ligne et lorsqu'une personne est seule devant son écran, il suffit que d'autres pages internet de Facebook ou Twitter par exemple soient apparentes pour qu'une éventuelle influence directe ou indirecte subvienne et viole l'intégrité numérique du votant. Dans cet exemple, garantir une intégrité numérique à un votant permet de garantir à cette même personne sa libre auto-détermination en ligne. A cet égard et comme le proposent les juristes, l'article 3 al. 1 de la Charte des droits fondamentaux de l'UE[519], pourrait être amendée ainsi : « *Toute personne a droit au respect de son intégrité physique, mentale et numérique* » (ici ajouté et souligné). En réalité, si le droit à la vie privée n'est pas respecté, tous les autres droits d'une personne peuvent être menacés. Les vies étant de plus en plus numériques, le droit à la vie privée pourrait être étendu et à tout le moins comprendre toutes les actions d'une vie devenue aujourd'hui numérique.

1.3.1 Pour un pseudo-anonymat contextuel et un anonymat résiduel dans le Web 3.0

Sur Internet, le chiffrement de bout en bout est nécessaire et essentiel afin d'assurer une navigation confidentielle des internautes. Sans ces mécanismes de chiffrement, les fournisseurs de services sont en mesure de reconstituer, de catégoriser et de commercialiser les choix et les comportements en ligne des

[518] GUILLAUME Florence, MAHON Pascal, ROUSSEL Alexis., « Réelle innovation ou simple évolution du droit ? le droit à l'intégrité numérique », Université de Neuchâtel, Éd. Helbing, Lichtenhahn, 2020, p.180.
[519] V. Art. 3 de la Charte des droits fondamentaux de l'Union européenne : « toute personne a droit à son intégrité physique et mentale », consulté le 11 avril 2022, à l'adresse suivante

internautes[520]. Si tous les services en ligne étaient dignes de confiance pour préserver la confidentialité des informations de leurs utilisateurs, ces mécanismes de chiffrement ne seraient pas nécessaires. Mais ils le sont devenus au fil du développement d'Internet et de ses services en ligne et données qu'il héberge. Effectivement, si « *l'une des libertés fondamentales apportées par internet réside* (…) *dans cette capacité à défaire le poids de responsabilité que fait peser l'assignation automatique du droit d'expression à une identité attestée* »[521], force est de constater que certains internautes abusent de cette confidentialité en ligne, c'est-à-dire de l'anonymat que confèrent ces méthodes de chiffrement. En effet, parce que leurs contenus sont chiffrés et leurs identités plus ou moins temporairement masquées, certains internautes entrent dans l'illégalité par leurs actes ou comportements en ligne, et il n'existe aucun moyen de les distinguer de tous les autres contenus chiffrés et légitimes qui circulent dans la masse des systèmes informatiques. Le risque est ainsi de perdre cet outil de protection de la vie privée qu'est la cryptographie, au nom d'une lutte contre une minorité d'acteurs malveillants en ligne. Il s'agit ainsi de trouver des mécanismes cryptographiques qui permettent de séparer les contenus nuisibles des contenus licites, sans pour autant empiéter sur la confidentialité des utilisateurs. Le concept d'*anonymat* est aujourd'hui largement dépendant de modèles sociaux, idéologiques, informatiques et culturels. Au Moyen-Age, il était une règle non dérogeable en littérature pour tous les auteurs religieux (notamment les moines copistes), dont la tâche principale se résumait uniquement à copier et à diffuser des ouvrages sans droit d'auteur, ni aucune appropriation personnelle. Avec le développement de l'imprimerie, les XVIIè et XVIIIè siècles représentent des périodes de révélation de l'identité individuelle et littéraire des auteurs, dont l'anonymat ne devient pas une condition, mais un refuge contre la censure politique, religieuse ou sociale. L'usage d'un pseudonyme pour préserver son anonymat pouvait être une pratique courante, revêtant pour certains écrivains, auteurs ou philosophes une façon de se dissimuler, comme le nom de Voltaire[522] pris par François-Marie Arouet en 1718 à la sortie de son emprisonnement de la Bastille, ou George Sand[523] prit par Aurore Dupin de Francueil son vrai nom patronymique. Ces dernières décennies et après de multiples scandales liés à des fuites, des vols ou manipulations des données, les jeunes générations d'internautes semblent progressivement à la recherche de nouvelles formes d'anonymat en ligne[524]. Mais l'avènement de la technologie numérique transforme le concept d'anonymat. Il est en effet relativement facile de rester anonyme dans le monde physique, ce qui est devenu presque impossible en ligne. Toute utilisation de matériel informatique et de navigation sur Internet laisse des traces numériques qui peuvent être récupérées, enregistrées ou exploitées, ce qui n'est pas le cas dans le monde physique au sein duquel il est pour l'instant plus simple de préserver l'anonymat

[520] Messages, photos, vidéos, navigation sur internet, etc.
[521] GAYON Jean et al., « L'Identité : dictionnaire encyclopédique », *op. cit*.
[522] « Voltaire, le jongleur de lettres (1/2) », in *Le Projet Voltaire*, 2015, consulté en ligne le 20 décembre 2021.
[523] Wikipedia, « George Sand », consulté en ligne le 20 décembre 2021.
[524] DUFOUR Fanny, 26 juin 2022, « (Re)devenir anonyme sur Internet, la nouvelle tendance des années 2020 ? », Clubic.com. Consulté le 27 juin 2022 à l'adresse suivante

et de revendiquer des idées de manière anonyme, par exemple lors d'une manifestation[525]. Dans l'univers numérique, il est dès lors plus exact de parler de *pseudo-anonymat* inhérent à toute identité devenue cryptographique (transactions grâce aux outils cryptographiques) ou numérique (adresse IP par exemple), tel un IBAN et BIC bancaire permettant par une suite de caractères alphanumériques d'identifier l'auteur de la transaction. Certains logiciels accordent aujourd'hui un *pseudo-anonymat* plus ou moins relatif, comme le logiciel de navigation Tor Browser qui permet aussi bien d'accroître la liberté d'information et d'expression dans des pays où la censure est quotidienne[526], que d'accéder dans certains cas à des marchés illicites sous couvert d'anonymat[527].

L'*anonymat* permet donc une totale dissimulation de l'identité, alors que le *pseudo-anonymat* ne permet au sein de l'univers numérique qu'une certaine forme de dissimulation en ligne. Il semble par conséquent plus approprié de considérer le concept de *pseudo-anonymat* plutôt que celui d'*anonymat* au sein de l'univers numérique. Bien que l'idée d'un anonymat complet représente aujourd'hui une utopie conceptuelle en informatique, cela toutefois ne signifie pas que quelques rares internautes avertis ne parviennent pas à vivre sans jamais être identifiés, comme certains pirates informatiques[528]. Près de 12.700 faux comptes[529] avec des images générées par des outils d'intelligence artificielle (IA) auraient été créés sur LinkedIn depuis le début d'année 2023, avec la création d'un « Bot » (logiciel) qui génère les likes et les demandes. Certains utilisateurs d'Internet peuvent par conséquent tirer avantage de leur anonymat provisoire sur les réseaux sociaux pour influencer certaines communautés en ligne en utilisant plusieurs comptes, adresses IP et identités numériques. Cette technique dite de l'« *astroturfing* », aussi désignée comme une « *attaque Sybil* » en informatique[530], vise à manipuler anonymement et en masse, à polariser et à augmenter une réputation ou une adhésion sur un réseau numérique. Ce phénomène a toujours existé sur les réseaux numériques et continuera probablement, car l'anonymat est nécessaire[531]

---

[525] Si l'anonymat social est prédominant dans notre monde physique lorsqu'une personne circule dans la rue, la multiplication des systèmes d'identification biométrique remet en question cet anonymat dans la sphère réelle, en raison d'une sollicitation possible à tout moment sous réserve du respect d'un cadre légal (accident, vols, terrorisme, etc.).

[526] Le New York Times utilise le logiciel Tor pour contourner la censure en ligne dans les pays où l'accès à l'information est limité ou interdit. Tor est un réseau décentralisé de relais (ordinateurs) qui permet de masquer l'adresse IP de l'utilisateur et de chiffrer le trafic, rendant ainsi la navigation sur Internet presque anonyme et sécurisé. En utilisant Tor, le New York Times peut fournir un accès plus sûr et plus privé à ses lecteurs dans les pays où la liberté de la presse est restreinte. Cela permet également aux journalistes et aux sources de communiquer de manière plus confidentielle sans craindre d'être surveillés ou censurés. En résumé, Tor est un outil essentiel pour les médias qui cherchent à garantir la liberté d'expression et à protéger les journalistes et les sources. Pour plus d'informations, consultez le Mémoire de recherche « Les méthodes de légalisation et de blanchiment des activités mafieuses », publié en juillet 2020, consulté en août 2021 et disponible à l'adresse suivante

[527] Les marchés illicites en ligne, également appelés *darknets*, sont des sites web cachés qui ne sont accessibles que via le réseau Tor susvisé. Le réseau Tor permet donc aux acheteurs et aux vendeurs de rester anonymes en masquant leur adresse IP et en chiffrant leur trafic. Les transactions sont souvent effectuées en utilisant des crypto-actifs pour éviter de laisser des traces. Bien que l'utilisation de Tor ne soit pas illégale en soi, ces plateformes illicites sont souvent associées à la vente de drogues, d'armes, de contrefaçons et d'autres produits illégaux. Il est important de noter que l'utilisation de Tor ne garantit pas un anonymat complet et que les autorités peuvent être en mesure de suivre les transactions et d'identifier les utilisateurs en utilisant des techniques de surveillance plus ou moins sophistiquées.

[528] PARGAMIN David, « Sur la piste des voleurs de cryptomonnaies », in *Challenge*, n°779, 23 mars 2023, p.46-47.

[529] BODNAR Bogdan, « ça y est, les premières arnaques générées par une IA sont en ligne », 23 février 2023, in *Numerama*, disponible à l'adresse suivante

[530] V. Annexe 6, Focus 1.

[531] BABEAU Olivier, déjà cité, Président de l'Institut Sapiens, « Face à la tyrannie de la transparence, retrouvons les vertus de l'opacité », publié le 4 mai 2021, in *Le FigaroVox*, Chroniques.

dans certains cas et vouloir l'éradiquer pourrait bien être non souhaitable aussi bien qu'utopique. Les réseaux sociaux représentent aussi une chance formidable de témoigner d'expériences personnelles sans craindre pour sa sécurité physique et personnelle grâce au pseudo-anonymat, renforcé aujourd'hui par certains réseaux sociaux tels Facebook, Twitter et Instagram qui proposent aujourd'hui à leurs abonnés[532] moyennant le paiement de 8 dollars par mois pour Twitter et 11,99 dollars pour Facebook de leur assurer l'authenticité de leurs messages et contenus. La *recherche de l'anonymat* en ligne peut être perçue comme une déviance par certains juristes « (...) *le chaos résulte de l'anonymat* »[533], tandis que la fin de l'anonymat en ligne signifierait une obligation pour tout internaute de revendiquer la paternité de ses propos.

Parce que l'anonymat en ligne favorise effectivement des comportements asociaux tels que le harcèlement, la diffamation, la calomnie, les moqueries, les injures, les discours haineux et l'usurpation d'identité, de nombreux gouvernements cherchent progressivement à y mettre fin. Pourtant, cette volonté politique semble paradoxale, car les termes *anonymat* et *pseudo-anonymat* créent une forme de confusion juridique et informatique pour le grand public. Chaque fois que l'anonymat est remis en question aux motifs précédents, cela semble être pour offrir des avantages à court terme aux internautes, telle une traçabilité élevée des transactions ou pour lutter contre le blanchiment d'argent et le financement du terrorisme. Une impossibilité de pouvoir être *pseudo-anonyme* signifie une identification numérique accrue, basée sur un soupçon de fraude généralisé mettant en péril des libertés fondamentales. Sur un plan psychologique, le *pseudo-anonymat* offre à une personne la possibilité de défendre ses positions (politiques, sociales, économiques) sous un pseudonyme qui protège son intégrité. Cela peut également permettre à l'auteur de reconnaître ses erreurs et de revenir dans les échanges en ligne sous un nouveau pseudo, libéré de tout jugement social grâce à son pseudo-anonymat voir anonymat. Cette liberté d'expression sans jugement ni attachement à une identité reconnaissable permet en théorie aux internautes d'être plus ouverts dans leur pensée. Toutefois, l'influence sociale peut à l'inverse inciter certains utilisateurs à se cramponner à leurs positions, ce qui peut les enfermer dans leur propre réflexion (fiction identitaire), créant ainsi le paradoxe des réseaux sociaux : à la fois émancipateurs et bourreaux sociaux.

Mais le *pseudo-anonymat* ne devrait-il pas être une question de contextualisation et de proportionnalité (comme le suggère l'illustration suivante) ? Chacun doit accepter que les citoyens et internautes puissent agir dans l'ombre de l'anonymat en ligne, comme le soutiennent certains juristes « *le grand soleil de l'identification perpétuelle* [fin de l'anonymat] *n'éclaire pas : il aveugle. Il n'illumine pas : il brûle* »[534]. Une société qui contrôle a priori tous les comportements des individus contribue à les enfermer

[532] « Les réseaux sociaux font payer la fin de l'anonymat », in *Challenges*, n°776 du 2 mars 2023, p.34.
[533] Plus précisément : « Il est désolant que ce vecteur de communication (courriel, tweets, clavardage, forums, etc.), si simple d'emploi, si vulgaire d'usage, premier moyen d'échange d'information et outil de lien social, soit devenu, grâce à l'anonymat électronique, le terrain privilégié des cybercriminels : il est temps de repenser le droit et de créer les moyens d'identification des acteurs œuvrant sur les réseaux », *op. cit.* BENSOUSSAN Avocats. « L'identité numérique 5.0 ». Lexing, p.47.
[534] NETTER Emmanuel. « L'identité à l'épreuve du numérique », in Larcier, 2020, p. 9, disponible à l'adresse suivante

préventivement dans des comportements liberticides, comme cela est le cas en Chine. Pour autant, il est utopique de penser qu'un Internet totalement anonyme soit viable, ne serait-ce qu'au regard du commerce en ligne qui nécessite par conception la récolte légitime de certaines données personnelles telles une adresse de livraison, un nom, un prénom, un âge, etc. Si l'anonymat assure en théorie une confidentialité pure en ligne, il ne permet pas toujours d'inspirer confiance, notamment lors de certaines transactions sociales qui requièrent une confiance tierce par une identification afin de garantir le processus et la validité d'échanges numériques.

D'un point de vue informatique, les blockchains publiques sont conçues pour offrir un anonymat par conception[535], mais l'historique complet de transactions en crypto-actifs par exemple demeure accessible publiquement en ligne[536]. Ces principes d'anonymat[537] et de décentralisation des échanges sont essentiels pour garantir le caractère incensurable d'une blockchain, c'est-à-dire l'immuabilité théorique de son registre de transactions. Si l'adresse d'un portefeuille de crypto-actifs est identifiée, il est possible de retracer l'historique complet des transactions de l'utilisateur, ce qui pourrait constituer un danger pour sa vie privée et son intégrité numérique. Cependant, ces mêmes caractéristiques peuvent être utilisées par des sociétés d'analyse spécialisées dans l'analyse de blockchains (en concertation avec les forces de l'ordre) pour identifier les parties impliquées dans une ou plusieurs transactions illicites, en examinant des informations auxiliaires telles que des messages sur un forum en ligne associés à des transactions[538]. Face à la volonté politique de permettre une identification systématique des utilisateurs de crypto-actifs pour retracer l'origine de leurs transactions[539] (par exemple lorsque des crypto-actifs sont « *teintés* »[540]), la question suivante se fait jour : cette volonté politique, légalement justifiée, d'identifier systématiquement les acteurs des blockchains publiques en mettant fin au pseudo-anonymat des transactions pourrait-elle mettre en danger leur existence ? Il semble en effet qu'il existe un risque vital pour les blockchains publiques d'être confrontées à ces mécanismes d'identifications systématiques des

[535] Une blockchain publique permet à n'importe quel internaute de devenir un utilisateur pseudo-anonyme (via une adresse et un identifiant numérique unique, nommé « clé publique ») ou encore grâce à un ordinateur validateur anonyme du réseau en achetant un ordinateur spécifique et dédié à la validation du réseau, nommé « ASIC ».

[536] V. Mempool - Bitcoin Explorer, 2022, pour consultez en temps réel la blockchain Bitcoin à l'adresse suivante

[537] L'anonymat joue un rôle essentiel dans la préservation de la décentralisation d'une blockchain en permettant aux utilisateurs de participer sans avoir à se soumettre à une autorité centrale. Il permet également d'éviter tout risque de surveillance et de censure. De plus, l'anonymat encourage l'adoption des blockchains publiques, car les utilisateurs se sentent en sécurité lors de la réalisation de transactions pseudo-anonymes. Enfin, l'anonymat des utilisateurs favorise la concurrence en permettant à de nouveaux acteurs de participer sans craindre d'être surveillés ou bloqués par des acteurs déjà établis.

[538] En 2022, un nouveau mécanisme judiciaire a vu le jour en réponse à un vol de crypto-actifs réalisé par des hackers : le cabinet d'avocats des plaignants a décidé d'envoyer les documents du tribunal judiciaire (sous la forme de NFT) directement sur les adresses pseudonymes des auteurs anonymes afin de leur notifier l'existence d'une enquête à leur encontre : « Cela nous donne un mécanisme pour au moins signifier un processus légal à une personne qui contrôle une adresse impliquée concernant un actif numérique qui a été affectée », a déclaré Andrew Balthazor du cabinet Holland & Knight. In *New Approach*, "Big law firm uses NFT to serve court papers on anonymous defendants", 17 juin 2022, in *Daily Business Review*. Consulté le 18 juin 2022, à l'adresse suivante

[539] KRYPTOSPHERE®, 27 juin 2022, « Contrairement aux idées reçues, Bitcoin n'est PAS anonyme ... », in *Cryptoast*, consulté le 28 juin 2022, à l'adresse suivante

[540] Proviens du terme anglais « *tainted coins* » qui désigne un jeton numérique soupçonné ou identifié comme étant impliqué dans une transaction illicite (blanchiment d'argent, réalisation d'une activité illicite, etc.). Pour plus d'informations *v. infra*, I, Titre 2, 1.4.1

parties prenantes de leurs écosystèmes[541] (utilisateurs, entreprises). Si les blockchains publiques sont conçues pour être décentralisées, transparentes et ouvertes, l'utilisation de *jetons teintés* (« *tainted coins* »)[542] attire l'attention des autorités et des régulateurs, bien que cette utilisation illégale de ces protocoles informatiques par certains utilisateurs demeure marginale. Les régulateurs peuvent en effet exiger que toutes les plateformes d'échanges de crypto-actifs et autres prestataires de services identifient et déclarent les utilisateurs qui effectuent des transactions avec ces jetons, ce qui peut compromettre la vie privée et l'anonymat d'autres utilisateurs légitimes sur ces blockchains. De plus, cette identification règlementaire de ces acteurs de l'écosystème peut également décourager l'innovation et le développement des blockchains publiques, car les startups et les développeurs peuvent hésiter à construire sur des protocoles où l'encadrement réglementaire serait trop contraignant.

Pour atténuer ce risque, certaines blockchains comme Bitcoin et Ethereum[543] - étudiée en Annexe - développent des technologies améliorant la confidentialité et permettant aux utilisateurs d'effectuer des transactions de manière anonyme ou pseudo-anonyme selon les situations, tout en respectant les exigences règlementaires. Pour trouver un équilibre entre la conformité règlementaire et la préservation de la nature décentralisée et pseudo-anonyme des blockchains publiques, il faudra du temps et un développement informatique continu. Ces propos remettent en question l'argument de l'anonymat proclamé des blockchains, aujourd'hui plus proche d'un *pseudo-anonymat* comme cela vient d'être expliqué et qui a été critiqué depuis les débuts de la technologie Bitcoin[544]. Une recherche de *pseudo-anonymat* pour les développeurs de ces protocoles restera dans cet écosystème une priorité[545]. Supprimer les principes d'anonymat des transactions et de décentralisation des blockchains publiques reviendraient aussi à freiner le développement et l'adoption massive des blockchains publiques et par effet de ruissellement de leurs écosystèmes blockchains privées et hybrides y compris. Par conséquent, le développement des mécanismes de *pseudo-anonymisation* susvisés respectant ces grands principes fondamentaux de la blockchain (pseudo-anonymat et décentralisation) ne peut être que bénéfique pour cette technologie et les identités numériques qu'elle héberge. Il est soutenu qu'un droit au *pseudo-anonymat* doit être préservé sur les blockchains publiques, y compris de façon marginale et accessoire à un anonymat qu'utilisent d'ores et déjà certains développeurs aux compétences uniques nommés des développeurs « cores » et par ailleurs indispensables pour les mises à jour des protocoles des blockchains

[541] V. Annexe 7.
[542] Pour plus d'informations v. *infra*, I, Titre 2, 1.4.1
[543] V. Annexe 6 Focus 2.
[544] « Le réseau est robuste dans sa simplicité non structurée. Les nœuds travaillent tous en même temps avec peu de coordination. Ils n'ont pas besoin d'être identifiés, puisque les messages ne sont pas acheminés vers un endroit particulier et ne doivent être délivrés que dans la mesure du possible. Les nœuds peuvent quitter et rejoindre le réseau à volonté, en acceptant la chaîne de preuve de travail comme preuve de ce qui s'est passé pendant leur absence. Ils votent avec leur CPU proof-of-work, exprimant leur acceptation des blocs valides en travaillant à leur extension et rejetant les blocs invalides en refusant d'y travailler. Toutes les règles et incitations nécessaires peuvent être appliquées avec ce mécanisme de consensus. », NAKAMOTO Satoshi, « Bitcoin Whitepaper, Bitcoin: A Peer-to-Peer Electronic Cash System », accessible en ligne à l'adresse suivante, p.3.
[545] « La blockchain a ainsi permis l'émergence d'entités sans visage, sans dirigeant, totalement autonomes. », *op. cit.* « Monnaies, banques et finance : vers une nouvelle ère crypto Un enjeu de souveraineté et de compétitivité économique, financière et Monétaire », p.30.

publics. A ce jour, l'un des secrets les mieux gardés d'Internet concerne l'identité du ou des créateurs du protocole Bitcoin[546], dont l'anonymat persiste depuis plus de 14 ans. Si avec les propos tenus précédemment il est impensable au 21e siècle de proposer un nouveau concept technologique de rupture, sans dévoiler l'identité de ses créateurs, l'origine mystérieuse du protocole Bitcoin infirme ce constat. Tout ce que nous savons avec certitude sur ce mystérieux créateur se résume à son pseudonyme : « Satoshi Nakamoto »[547]. Ce dernier aurait fini par se retrouver en contact avec l'influence du mouvement des « cypherpunks »[548], au point qu'il soit fort probable qu'il y ait été actif sous différents pseudonymes avant d'inventer puis de dévoiler le protocole Bitcoin sur la toile du Web[549]. Aujourd'hui, plusieurs scénarios sont présumés et plausibles concernant l'inactivité dont fait preuve ce(s) mystérieux personnage(s) depuis 2010 : retraite volontaire de son implication, décès, perte de ses clés cryptographiques (permettant l'accès à ses fonds en bitcoins)[550], observation silencieuse, arrestation gouvernementale, etc. Si le doute doit persister pour assurer la longévité de ce protocole informatique, il semblerait que le ou les individus à l'origine du personnage de Satoshi Nakamoto aient volontairement décidé de se retirer de la scène publique. Cette décision aurait pu être influencée par une invitation de l'ancien bras droit de Satoshi Nakamoto, Gavin Anderson, à présenter les prémices de Bitcoin à la CIA, une invitation qui avait été refusée par Satoshi Nakamoto. Depuis ce jour du 12 décembre 2010[551], il s'agit vraisemblablement de la dernière correspondance numérique vérifiée et publique émise par le pseudo de Satoshi Nakamoto[552] (une année plus tard, un courriel adressé à Gavin Andresen semblerait confirmer que l'anonymat était pour Satoshi un élément fondamental à ne pas compromettre)[553].

---

[546] Selon une étude récente : « 64 agents ont miné la plupart des bitcoins entre le lancement du bitcoin et le moment où il a atteint le même prix que le dollar américain. Nous avons exploité les fuites de données pour construire une carte de la blockchain début 2011, dans laquelle les bitcoins sont classés en fonction de l'agent qui les a minés », BLACKBURN Alyssa et al. « Cooperation among an anonymous group protected Bitcoin during failures of Decentralization », p. 64 sur 76, disponible à l'adresse suivante

[547] Le principal profil en ligne de ce pseudo et personnage est disponible à l'adresse suivante

[548] « Cypherpunk » est un mot-valise inventé par la célèbre auteure et pirate informatique Judith Milhon. Ce terme est issu de la rencontre entre les mots anglais « cypher » (« cipher » en français) en référence à un algorithme de chiffrement et « cyberpunk » qui désigne une science-fiction dystopique. Cette simple définition caractérise l'idéologie de ce groupe d'individus et d'activistes au service d'un Internet libre et respectueux de la vie privée des internautes (une idéologie aujourd'hui plus d'actualité que jamais). Nous constatons que le chiffrement est la pièce maîtresse de ce mouvement qui est le berceau de nombreux membres et participants au lancement de la blockchain Bitcoin : la mère des blockchains reposant sur une idéologie technologique en partie seulement devenue une réalité. Sur le plan politique, ce mouvement marque son opposition à la toute-puissance des États : « Nous les Cypherpunks sommes dédiés à construire un système anonyme. Nous défendons notre vie privée avec la cryptographie, un système anonyme de mail, des signatures numériques et la monnaie électronique ». Propos issus de l'article « À la découverte du mouvement cypherpunk à l'origine du Bitcoin », in *Cryptoast*, disponible en ligne

[549] À ce propos, Satoshi Nakamoto s'est inspiré de connaissances antérieures issues de travaux précédemment réalisés (*B-Money*, *DigiCash*, *Hashcash*) par d'autres experts informatiques (dont Jean-Jacques Quisquater) présents dans la « *Cryptography mailing list* » afin de les intégrer à sa proposition : *The Bitcoin Project*

[550] V. Annexe 3.

[551] « Added some DoS limits, removed safe mode (0.3.19) », 2010, in *bitcointalk.org*, consulté le 01/06/2022 à l'adresse suivante

[552] Excepté un message du 8 septembre 2014 qui aurait été posté par Satoshi Nakamoto d'après une investigation vidéo disponible à l'adresse suivante, Barely Sociable. 2020. « The Most Elusive Identity On The Internet - Pt. 2 » [Vidéo]. YouTube.

[553] La dernière correspondance de Satoshi, un courriel du 26 avril 2011 adressé à Gavin Andresen a donné lieu à une autre théorie sur les raisons de son départ brutal. Il a écrit : « J'aimerais que vous ne continuiez pas à parler de moi comme d'une mystérieuse figure de l'ombre, la presse ne fait que transformer cela sous le prisme d'un pirate de monnaie virtuelle. Peut-être que vous devriez plutôt parler du projet open source et donner plus de crédit à vos contributeurs et développeurs ; cela aide à les motiver », « Satoshi's Final Email to Gavin Andresen ». 26 juin 2011, in *Nakamotostudies.Org*. Consulté le 20 juin 2022, à l'adresse suivante

D'après le Professeur émérite en mathématiques et cryptographie Jean-Jacques Quisquater (cité dans le livre blanc et PDF officialisant Bitcoin)[554], l'ingénieur et docteur en informatique Adam Back et plusieurs autres personnes, tous rattachés publiquement ou non au mouvement des Cypherpunks, seraient à l'origine de la naissance de Bitcoin (peut-être en se partageant le pseudo « Satoshi Nakamoto »). Il semble en effet peu probable qu'une seule personne ait pu concevoir le protocole Bitcoin, car cela aurait nécessité de multiples compétences en matière de développement de logiciels, de cybersécurité, de gestion d'infrastructures informatiques, de théorie des jeux[555] et de connaissances économiques et financières très poussées pour l'époque. Si de multiples hypothèses existent concernant l'identité de cette mystérieuse genèse[556], force est de remarquer que ces tentatives de démasquement de l'identité de Satoshi Nakamoto restent à ce jour vaines, contre-indiquées par sa communauté[557], pour des motifs qui semblent plutôt légitimes à la lumière des propos précédents. En dépit des hypothèses entourant l'identité de Satoshi Nakamoto, il est indéniable que l'anonymat de ce pseudonyme a permis à Bitcoin de donner naissance à une nouvelle classe de technologies sans précédent sur Internet : la technologie blockchain[558]. En d'autres termes, si l'identité de Satoshi Nakamoto avait été révélée, le monde n'aurait peut-être jamais connu cette révolution de la confiance numérique que représente Bitcoin, ainsi que la technologie blockchain sous toutes ses formes, y compris privées et hybrides. En effet, l'identité de Satoshi Nakamoto aurait pu être influencée par des tiers ou même poursuivie ou stoppée par un gouvernement, notamment en raison des liens avérés à l'époque entre le bitcoin et le blanchiment de capitaux. Ce cas d'étude démontre que *l'anonymat* peut jouer un rôle important dans l'innovation des réseaux (sociaux) informatiques. Pour atteindre une décentralisation totale, l'entité ou la personne à l'origine du réseau généralement centralisé au début par quelques développeurs[559], doit

[554] Cela signifie que Jean-Jacques Quisquater a directement inspiré les travaux de Satoshi Nakamoto dès 1999, en plus d'avoir participé à l'organisation d'évènement à Londres pour le compte des *Cypherpunks*. Discussion privilégiée d'une heure avec Jacques Quisquater lors du *Forum International sur la Cybersécurité (FIC)* le 09/10/2021 à propos du protocole Bitcoin, de l'identité décentralisée ou encore de l'identité de Satoshi Nakamoto.

[555] V. Annexe 6, Focus 4, 5 et 6.

[556] De nombreuses personnalités affirment être Satoshi Nakamoto ou avoir démasqué son ou leurs identités, ce qui représente en effet un *sophisme* puisqu'il s'agit d'indices et non pas de preuves irréfutables. Suite à nos recherches, voici une liste sérieuse, mais non exhaustive, de candidats et personnes susceptibles d'être, à titre individuel et/ou collectif, Satoshi Nakamoto (remarquons que nombre de ces personnes sont rattachées au mouvement précité des *Cypherpunks*) : David Lee Chaum, Craig Wright, Paul Le Roux, Adam Back, Nick Szabo, Hal Finney, Tony Spilotro, Zooko Wilcox-O'Hearn, Len Sassaman, Gavin Andresen, Jed McCaleb, Shinichi Mochizuki, Neal King, Vladimir Oksman, Charles Bry, Wei Dai, Ian Grigg, Dave Kleiman. Pour plus d'informations, v. les sources suivantes : « Le mystère Satoshi : enquête sur l'inventeur du bitcoin », ARTE. 2021. YouTube. Disponible à l'adresse suivante ; MoneyRadar Crypto. 2022. « Satoshi et le mystère des Cypherpunks » [Vidéo]. YouTube. Disponible à l'adresse suivante ; Barely Sociable. 2020. « Bitcoin - Unmasking Satoshi Nakamoto ». YouTube. Disponible à l'adresse suivante ; Wikipedia contributors. 2022. « Satoshi Nakamoto », disponible à l'adresse suivante

[557] Révéler l'identité de Satoshi Nakamoto reviendrait à renouer et à conférer une responsabilité économique, juridique et sociale à cette personne. Cette nouvelle prise de responsabilité pourrait engendrer une perte de confiance et par effet domino une perte de valorisation de cet actif 3.0. La communauté ne souhaite ainsi pas donner suite à toute volonté de réponse face à cette curiosité légitime mais qui serait en réalité contreproductive pour tout l'écosystème blockchain.

[558] V. *infra*, I, Titre I, 2.3

[559] Tout réseau informatique naissant est par conception informatiquement centralisée, y compris Bitcoin à ses débuts. En effet, il a été démontré par des chercheurs que Satoshi Nakamoto faisait fonctionner environ 48 ordinateurs au début du lancement de Bitcoin, puis a progressivement réduit ce nombre, c'est-à-dire sa puissance de calcul à mesure que d'autres *mineurs* rejoignaient le réseau (car il considérait le réseau comme suffisamment robuste pour se permettre de se retirer à titre personnel). « Nous soupçonnons que Patoshi était composé d'au moins 48 ordinateurs, avec une machine pour la coordination et d'autres en attente en cas d'attaque, ce qui expliquerait la fourchette manquante de [10-18]. Dès que Satoshi a jugé le réseau

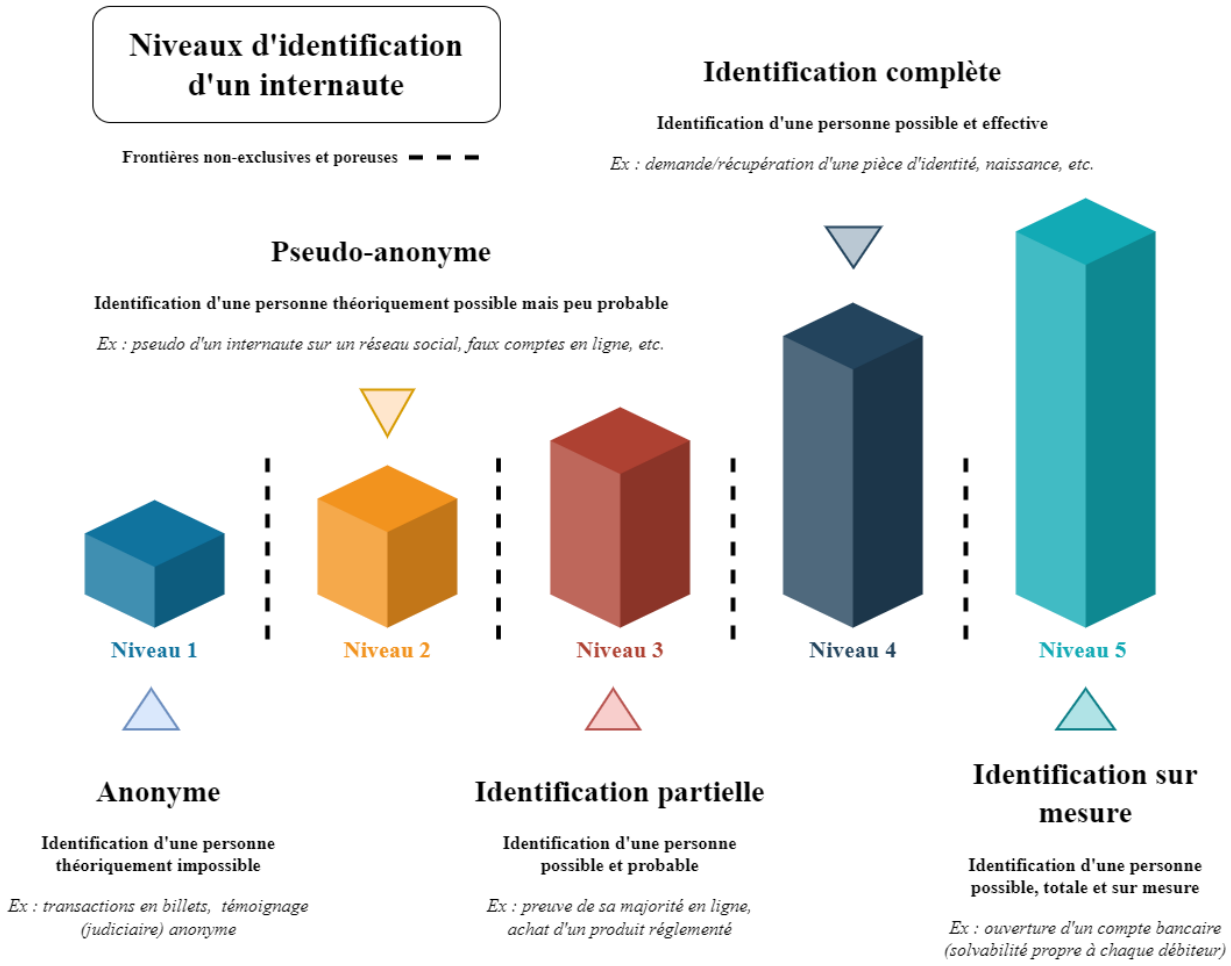
rester anonyme afin d'éviter tout risque d'intimidation du fondateur. A cet égard, il est souligné que la création d'un crypto-actif n'est pas illégale, les quelques 900 personnes ayant contribuées au développement du protocole Bitcoin depuis 2009[560] auraient été empêchées en cas de levée d'anonymat. Pour ce secteur des crypto-actifs[561], l'*anonymat* n'est pas considéré comme une exigence, mais plutôt comme une caractéristique historique essentielle et structurelle. Les acteurs financiers et institutionnels classiques considèrent ce marché comme opaque ou comme la source d'une perte de confiance significative par rapport à d'autres classes d'actifs financiers réputées plus transparentes. Mais un certain niveau d'*anonymat* minimum doit rester possible, car il est un moteur d'innovation pour ses bénéficiaires qui ont le choix de s'en saisir ou de s'en dessaisir à tout moment. Finalement, parce que garantir l'*anonymat* en ligne paraît techniquement utopique pour une majorité d'internautes, une solution intermédiaire qui est le *pseudo-anonymat* doit être privilégiée et de façon industrielle, c'est-à-dire par l'utilisation par exemple de notations et de scores de pseudo-anonymisation programmés (*v*. illustration suivante), comme le propose déjà une publication scientifique depuis 2021[562]. Pour résumer, l'*anonymat* en ligne est une question d'équilibre à rechercher entre une contextualisation systématique des besoins et les niveaux de *pseudo-anonymat* existants. La recherche d'*anonymat* ne doit finalement pas être proscrite, car c'est elle qui permet en réalité aux internautes de retenir des solutions *pseudo-anonymes* protectrices de leur vie privée. Les technologies blockchains et l'identité numérique décentralisée étudiées dans une deuxième partie de cette recherche joueront un rôle crucial dans la reconnaissance d'une nouvelle ère de confidentialité numérique où l'*anonymat* sera possible pour certaines solutions, tandis que le *pseudo-anonymat* demeurera courant pour certains attributs secondaires de l'identité numérique décentralisée, objet de cette étude.

suffisamment fort, il a réduit l'objectif de blocs par 10 minutes de Patoshi pour donner aux autres une meilleure chance de miner un bloc », librement traduit de l'anglais. Whale Alert, « The Satoshi Fortune », 2022, Medium

[560] Contributors to bitcoin/bitcoin. 30 août 2009. GitHub. Consulté le 14 octobre 2022, à l'adresse suivante

[561] En attestent les innombrables projets blockchains qui existent et possèdent à leur tête une fondation, une société ou même une icône (référence à la blockchain Ethereum) ; *v, supra*, I, Titre 1, 2.3.1.1.a

[562] KOLAIN Michael, GRAFENAUER Christian, EBERS Martin, traduction libre de l'anglais, « L'évaluation de l'anonymat que nous proposons dans ce document déterminera un ensemble de deux scores. Le score objectif d'anonymat (Objective Anonymity Score - OAS) détermine les risques résiduels de (ré)identification d'une personne physique selon des mesures statistiques objectives. Il sert d'outil pour mesurer les propriétés [...] d'un ensemble de données traité par le système informatique évalué sans tenir compte d'informations supplémentaires provenant d'autres sources. Le score d'anonymat subjectif (SAS) fournit un indicateur de l'anonymat relatif du traitement effectué par un responsable du traitement ou un sous-traitant : il prend en compte le coût et le temps nécessaires pour réussir à réidentifier l'ensemble de données en question en tenant compte de la main-d'œuvre et du capital disponibles du responsable du traitement ou du sous-traitant », « Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets under the GDPR with a Special Focus on Smart Robotics », 2021, in *US Law and Tech Journal*, publication pending (forthcoming), consulté en ligne le 20/12/2021.



1.3.1.1 Depuis l'usurpation d'identité au risque de tromperie généralisé

Historiquement sous la forme de vol, de fabrication ou de falsification de titres d'identité physiques, le délit d'usurpation d'identité s'est rapidement immiscé dans la sphère numérique. Les multiples besoins d'accès, d'identification et d'authentification des personnes en ligne ouvrent la voie à de nouvelles méthodes d'usurpation d'identité à distance plus sophistiquées. En 2019, 45 000 usurpations d'identité ont été constatées en France[563]. Dès lors, plusieurs infractions peuvent être retenues selon le contexte d'usurpation d'identité, et de façon non limitative l'atteinte au secret des correspondances[564], l'atteinte à la vie privée, la collecte de données à caractère personnel par un moyen frauduleux[565], la contrefaçon

[563] « Trois questions sur la nouvelle carte d'identité qui entre en vigueur lundi 2 août », in *Franceinfo*, publié le 2 août 2021, consulté en ligne
[564] Art. 226-15 du Code pénal (détournement, utilisation frauduleuse de correspondances privées, même électroniquement).
[565] Art. 226-18 du Code pénal (collecte de données à caractère personnel par un moyen frauduleux, déloyal, illicite).

et l'usage frauduleux de moyen de paiement[566] ou encore l'escroquerie[567]. Pour les institutions judiciaires, une autre forme d'usurpation plus spécifique progresse, la fraude comportementale via des prêts d'identités[568]. A cet égard, certaines administrations luttent contre des prêts d'identité, désignés par les juristes par le concept de fraude comportementale, qui ne sont pas encore traités par le Règlement eIDAS[569] qui est étudié dans la deuxième partie de cette étude. Cette fraude consiste à emprunter à une personne consentante son identité afin de réaliser une ou plusieurs démarches pour son propre compte et moyennant finance. Avec la crise de la Covid-19 et la mise en place du pass sanitaire[570], cette fraude s'est particulièrement développée. Si la motivation première d'une usurpation d'identité est de se faire passer pour un autre, les personnes physiques en sont les premières victimes mais également les personnes morales (fraude au Président, escroquerie, hameçonnage, usurpation de noms de domaine, etc.). En réalité, ce n'est pas l'identité de la personne qui est usurpée mais plutôt ses droits, son identité ne lui est pas retirée, mais plutôt dupliquée pour acquérir indûment tout ou partie de ses droits[571]. L'usurpation de l'identité est définie par la loi LOPPSI 2[572] et à l'article 226-4-1 du Code pénal qui dispose « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier* [un tiers] *en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* (…) »[573]. Il s'agit d'un délit puni d'un an d'emprisonnement et de 15 000 € d'amende, une sanction relativement dissuasive étant donné les conséquences graves et parfois irrémédiables pour la victime. Il est remarqué que la phrase « *d'une ou plusieurs données de toute nature permettant de l'identifier »* permet d'inclure par interprétation tout attribut d'identité appartenant à une personne y compris en cas d'utilisation d'identifiants pseudo-anonymes ce qui constitue une perspective encourageante. Les conséquences d'une usurpation d'identité peuvent être dévastatrices *« l'Internet a ceci de particulier que même si l'on peut poursuivre au pénal une usurpation d'identité, les dégâts éventuels en termes d'image ou de réputation peuvent être irréversibles vu l'impraticabilité du droit à l'oubli. Seul le droit au déréférencement est envisageable* »[574]. Une personne victime d'usurpation de son identité est confrontée à de nombreuses barrières juridiques et administratives avant de pouvoir espérer réintégrer son identité et jouir à nouveau de ses droits, comme l'explique la doctorante en droit Pauline Elie « *les personnes victimes d'usurpation*

[566] Art. L163-3 (contrefaire ou falsifier un chèque) et L163-4 (fabriquer, détenir, céder, mettre à disposition des instruments, programmes informatiques pour commettre des infractions) du Code monétaire et financier.
[567] Art. 313-1 du Code pénal (définition de l'escroquerie).
[568] Il s'agit pour une personne de « prêter » un ou plusieurs éléments de son identité civile à une autre personne dans l'objectif d'obtenir l'accès à un ou plusieurs droits. Cette relation est généralement monétisée, illégale, et caractérise un délit d'usurpation d'identité pour le fraudeur.
[569] V. *infra*, II, Titre 1, 2.1.1.1
[570] ELIE Pauline, LANGLOIS-BERTHELOT Thibault, et al., « Le pass sanitaire au prisme de l'informatique, du droit et de la philosophie », Atelier(s) vidéo(s) et compte(s) rendu(s). 2021. *Les Temps Numériques*. Site internet disponible à l'adresse suivante
[571] DESJARDINS Cécile, 6 décembre 2021, « La certification PVID permet de réduire le risque d'usurpation d'identité », in *Les Echos*, consulté en ligne le 12/01/2022.
[572] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite LOPPSI).
[573] Art. 226-4-1 Code pénal dans sa version en vigueur depuis le 1er août 2020, consulté en ligne
[574] *Op. cit.* BENSOUSSAN Alain, Avocats, décembre 2021, « l'identité numérique 5.0 », in *Lexing*, p.31.

d'identité ont de grandes difficultés à renouer avec leur identité »[575]. Par exemple, en cas de condamnation pour usurpation d'identité, il est extrêmement complexe de faire disparaître les mentions correspondantes aux actes frauduleux annulés[576], jusqu'à la promulgation en 2022 d'une proposition d'amendement de la loi relative à la protection de l'identité « (…) *le présent article résout cette difficulté en imposant que, lorsqu'un acte est annulé par le juge sur le fondement d'une usurpation d'identité, le dispositif du jugement dont la transcription est ordonnée à l'état civil, fasse référence à l'usurpation, ce qui permettra, à l'avenir, de distinguer entre les mentions portées en marge des registres d'état civil, celles qui ont pour cause la fraude et les autres* »[577]. Aujourd'hui, certaines vérifications certifiées sont d'ores et déjà nécessaires dans le cadre de la création d'une identité numérique par certains services de confiance en vertu du Règlement eIDAS (signature électronique[578], cachet électronique visible[579]), ou avec la mise en place d'un référentiel pour les prestataires de vérification d'identité à distance (PVID)[580] qui sont étudiés au deuxième titre de cette étude. Bien que les processus et garanties de ces services de confiance soient efficaces, ils sont encore déployés de manière relativement lente et marginale à l'échelle du nombre de services en ligne existants et des multiples besoins et contextes d'identification des internautes. Ainsi, bien que ces services soient indispensables pour lutter contre l'usurpation d'identité des personnes morales et de leurs services en ligne, ils ne permettent pas encore de lutter massivement contre l'usurpation d'identité des personnes physiques. Cela est particulièrement vrai pour le choix des méthodes de stockage de ces attributs d'identité numérique qui pourraient recourir à une identité décentralisée, par exemple avec un stockage P2P, qui est étudié plus loin, couplé à une blockchain. Il semble effectivement que l'identité numérique décentralisée puisse permettre de lutter efficacement contre ces vols d'identité numérique, en amont et en aval des besoins d'identifications numériques, puisqu'elle propose tout simplement de nouveaux mécanismes de vérification et de contrôle directement ou indirectement (*v*. identité numérique autosouveraine, étudiée plus loin)[581] gérés par les utilisateurs. La reconnaissance juridique accordée par la révision du Règlement eIDAS[582] aux registres blockchains privés et hybrides, ainsi qu'aux attestations vérifiables[583] également étudiées plus loin, reflète une

[575] ELIE Pauline, « Analyser l'identité en droit : comment protéger et définir un nouveau territoire à l'ère dématérialisée ? », *v*. Thèse en cours à l'EHESS, disponible à l'adresse suivante
[576] « Les règles de conservation intégrale des mentions portées à l'état civil, interdit de faire disparaître purement et simplement les mentions correspondant aux actes annulés. Le dispositif du jugement décidant l'annulation est porté en marge sans autre indication, ce qui ne permet pas de distinguer l'annulation dont la cause est l'usurpation de l'annulation pour un motif propre à la personne », Sénat. 1 juin 2022. Proposition de loi relative à la protection de l'identité, in *sénat.fr*, consulté le 20/06/2022 et disponible à l'adresse suivante
[577] *Ibid*.
[578] V, *supra*, I, Titre 1, 2.3.1.1.b
[579] ANTS, *Le cachet électronique visible de la nouvelle carte d'identité*, disponible à l'adresse suivante
[580] L'objectif de ce référentiel est de mettre en lumière des solutions robustes, avec deux niveaux de garanties : le niveau « substantiel », qui offre la même fiabilité qu'une vérification d'identité en face-à-face et le niveau « élevé », qui atteint le niveau de fiabilité de la délivrance d'un titre d'identité en mairie, ou auprès de la gendarmerie. « Publication du référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID) », sur *ANSSI*, en ligne, consulté le 17 février 2022.
[581] V. *infra*, II, Titre I, 1.4
[582] V. *infra*, II, Titre 1, 2.1.1.1
[583] V. *infra*, II, Titre 1, 1.3.1.2

volonté réaffirmée de lutter contre l'impersonnalisation des identités numériques grâce à de nouveaux outils fiables et souverains, toujours au service de l'identité des citoyens.

1.4 Géopolitique comparée des données personnelles entre l'Europe et les États-Unis

Depuis l'adoption d'Internet, le législateur européen a eu tendance à calquer sa règlementation sur la règlementation américaine, malgré un fossé idéologique[584] plutôt paradoxal entre ces deux juridictions, ce que propose d'introduire cette partie visant à comprendre les nécessaires adaptations à envisager. Il est proposé de tendre vers une vue d'ensemble de la façon dont ces juridictions traitent le traitement et la protection des données personnelles, car les technologies blockchains impliquent un stockage transfrontalier de données chiffrées. L'historique de la géopolitique entre ces deux côtés de l'Atlantique aura probablement une incidence sur les cadres juridiques applicables aux crypto-actifs, à la technologie blockchain et à l'identité numérique 3.0. Aux Etats-Unis, les données personnelles peuvent entre autres faire l'objet d'une commercialisation, car elles sont considérées comme la propriété de leurs titulaires et propriétaires[585]. En Europe, le RGPD étudié plus loin, introduit une protection juridique spécifique pour les personnes physiques au regard de la gestion de leurs données à caractère personnel, dont la commercialisation ne représente pas une possibilité voire une opportunité, mais plutôt un risque fondamental. Le secret des affaires ou encore le secret des procédés n'entre pas dans le périmètre du RGPD (étudié au chapitre suivant), contrairement au droit applicable aux Etats-Unis où toutes les données sont commercialisables sans distinction de provenance (selon qu'il s'agisse de personnes physiques ou morales). Outre Atlantique, porter atteinte à ce nouvel eldorado monétisable constitue un préjudice économique pour son titulaire (une entreprise, un particulier). La présence d'un préjudice économique n'est pas une condition préalable essentielle en droit européen pour établir une faute en matière de traitement de données personnelles, contrairement à la pratique aux États-Unis où la protection des individus est moins efficace. Cela soulève la question de la territorialité du droit applicable à Internet : application du droit américain (fédéral où celui d'un Etat) ou des Règlements européens ? La Cour de Justice de l'Union européenne (CJUE) a eu à se prononcer en 2020 sur cette question et a conclu dans un arrêt Schrems II[586], sur lequel nous reviendrons, que le droit américain n'est pas compatible avec le droit européen et que le RGPD européen trouve application en matière de protection de données personnelles[587] (cas d'un citoyen irlandais en l'espèce). En pratique, les autorités

[584] Le *Common Law* traite de faits générateurs de règles de droit, tandis que le *Civil Law* repose majoritairement sur des textes de Loi et des Règlements.
[585] Excepté dans certains états (Utah, Californie, Colorado, Virginie) où le *California consumer privacy act (CCPA)* est en vigueur, pour plus d'informations consultez la carte numérique suivante (mise à jour le 07/04/2023).
[586] Arrêt CJUE du 16 juillet 2020, invalidant la décision n°2016/1250, rendu dans le cadre d'une question préjudicielle posée à la Cour, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, Aff. C-311/18, disponible à l'adresse suivante, v. également Communiqué de Presse de la CJUE « Data Protection Commissioner / Maximillian Schrems et Facebook Ireland », n° 91/20 disponible à l'adresse suivante
[587] *Ibid.* « Le […] RGPD dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu que si le pays tiers en question assure un niveau de protection adéquat à ces données ».

gouvernementales américaines peuvent toutefois accéder aux données personnelles des citoyens européens en cas de lutte contre des activités illégales, terroristes ou de blanchiment d'argent. Les Règlements européens sur la protection des données (RGPD et eIDAS, étudiés plus loin) se trouvent régulièrement en conflit avec diverses règlementations américaines, notamment et de façon non limitative pour les plus récents, le « Patriot Act »[588] de 2001, le « Foreign Intelligence Surveillance Act - (FISA) »[589] de 2018, le « Cloud Act »[590] de 2018 ou les « Executive Order »[591]. Toutefois ces dispositifs sont insuffisamment surveillés, et ne disposent pas de recours adéquats comparables à ceux prévus par le droit communautaire sur la protection des données personnelles. Ces bases juridiques sont celles qui permettent au gouvernement américain et à ses institutions - notamment la National Security Agency (NSA), le FBI, la CIA - un accès permanent aux données personnelles des personnes physiques. En matière de souveraineté numérique des données au sein de l'Union européenne, la Commission européenne assume une part significative de responsabilité du fait de la signature en 2000 de l'accord *Safe Harbor*[592]. Cet accord prévoyait des règles de protection des données prétendument équivalentes, permettant ainsi la libre circulation des données entre les États-Unis et l'Europe. De fait, ce dispositif législatif a permis aux États-Unis de collecter les données des citoyens européens pendant plus d'une décennie, tout en bénéficiant d'un effet de réseau et d'une expérience sans équivalent dans le domaine du Web 2.0. Cette situation a propulsé les États-Unis au rang de leader de l'Internet. Ce constat a progressivement cessé avec l'émergence de certaines révélations troublantes comme l'affaire Snowden[593] en 2013, puis la saisine de la CJUE qui décide de casser le *Safe Harbor* par un arrêt du 6 octobre 2015[594]. De ce fait, est rapidement adopté le 8 juillet 2016 un nouvel accord, le *Privacy Shield*[595], qui sera lui aussi cassé par l'arrêt *Schrems II* le 16 juillet 2020[596]. De cette complexité d'appréhension et d'encadrement par la Commission européenne des données des personnes physiques, s'ensuit un nouveau positionnement politique et juridique face aux Etats-Unis, sur la base de l'adoption du RGPD entré en vigueur le 25 mai 2018 après quatre années de négociation (2012-2016)[597]. Si la Commission

[588] Le *Patriot Act*, entré en vigueur le 26 octobre 2001 au lendemain des attentats du 11 septembre, renforcé depuis à plusieurs reprises.
[589] Committee on civil liberties, Justice and Home Affairs, « Background note on US legal instruments for access and electronic surveillance of EU citizens », in *Europa.eu*, disponible à l'adresse suivante
[590] Le *Cloud Act* permet aux services de renseignement des Etats-Unis d'accéder à tout *cloud* étranger fourni par des entreprises domiciliées aux Etats-Unis. Les *clouds* étant fournis partout dans le monde, les Etats-Unis peuvent en vertu du *Cloud Act* effectuer des recherches sans que leurs clients n'en soient informés et sans autorisation. *Compte rendu de la Commission de la défense nationale et des forces armées*, Assemblée nationale, audition, à huis clos de Mr Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale, 13 juillet 2022, *v.* Compte rendu n° 5
[591] BENZINA Samy, « Les executive orders du président des États-Unis comme outil alternatif de législation », in *Revue de droit politique*, Dalloz, 2018, hal-02900076
[592] Wikipedia contributors, « International Safe Harbor Privacy Principles ». 25 décembre 2021, consulté le 4 avril 2022, à l'adresse suivante
[593] T.d.L, « Tout comprendre sur l'affaire Snowden », 2017, in *Leparisien.fr*. Consulté le 4 avril 2022, à l'adresse suivante
[594] Arrêt CJUE du 6 octobre 2015, Aff. C-362/14, décision rendue dans le cadre d'une question préjudicielle posée à la Cour relative à la transmission par Facebook Ireland Ltd de données à caractère personnel de Mr Schrems et de leur conservation sur des serveurs situés aux Etats-Unis, consulté le 17 octobre 2022, à l'adresse suivante
[595] CNIL : « Invalidation du Privacy shield : les premières questions-réponses du CEPD », consulté le 17 octobre 2022, à l'adresse suivante
[596] Arrêt CJUE du 16 juillet 2020, *op. cit.*, disponible à l'adresse suivante
[597] « The History of the General Data Protection Regulation », in *European Data Protection Supervisor*, consulté le 20 octobre 2022, à l'adresse suivante

européenne apprend donc de ses erreurs passées (*Safe Harbour* puis *Privacy Shield* cassés par la CJUE), force est de rappeler que cette période de réflexion lui a permis de passer d'une perception ultra libérale sur les données à une perception conservatrice et protectrice des personnes physiques. L'objectif de la Commission est de créer un écosystème numérique européen dont les règles applicables et appliquées seront européennes et non pas bilatérales et assujetties à l'extra-territorialité du droit américain mentionné précédemment. Toutefois, la jurisprudence de la CJUE peut mettre plusieurs années avant d'être transposée et appliquée par les institutions de contrôle nationales (CNIL, AEPD en Espagne, BFDI en Allemagne, etc.)[598] au sein des États membres de l'Union européenne. Pendant ces périodes d'influences politiques aux effets juridiques, le législateur est soumis à de fortes pressions venant des États-Unis et particulièrement de ses grandes entreprises technologiques. L'application stricte des arrêts de la CJUE par tous les États membres reviendrait aussi à contraindre les activités des entreprises technologiques américaines qui ont fondé Internet (Microsoft, Google), dont tous les citoyens européens ont paradoxalement besoin quotidiennement. Dès lors, la géopolitique et le droit semblent inconditionnellement liés sur les sujets de protection et de patrimonialisation des données personnelles (*v*. plus loin).

1.4.1 Territorialité du droit applicable : entre territoires et conflits de lois

Cette section explore le transfert massif de données personnelles depuis l'Union européenne vers les Etats-Unis, ce qui soulève de nombreux enjeux en termes de respect de la vie privée, de sécurité nationale et de compétitivité économique. Les grandes entreprises technologiques (GAFAM/BHATX) ont recours à des clauses attributives de compétence dans leurs conditions générales d'utilisation par exemple, aux fins d'imposer bien souvent leur juridiction en cas de litiges. Alors que certains pays cherchent à maintenir des régimes juridiques équivalents en matière de protection de données à caractère personnel à l'instar du RGPD européen, d'autres pays ont tendance à élaborer leurs propres règles en matière de protection de données, comme cela est illustré par le Royaume-Uni depuis sa sortie de l'Union européenne[599]. Les technologies blockchains sont, comme nous l'avons vu, de nature *pseudo-anonyme* et *décentralisée*, ce qui suppose que les participants (ordinateurs validateurs, développeurs, utilisateurs) soient répartis dans plusieurs pays relevant de diverses juridictions. Dans une affaire européenne

[598] CNIL, « La protection des données dans le monde », *v*. en ce sens la carte interactive de la CNIL en matière de protection des données à l'international, à l'adresse suivante

[599] « Le maintien de l'équivalence avec les lois européennes sur la protection des données [RGPD] n'est peut-être plus une priorité pour le Royaume-Uni, qui se dirige vers un nouveau régime favorable à la croissance et à l'innovation - nous pourrions commencer à voir une certaine divergence dans les années à venir, et il sera important de se tenir au courant des nouveaux développements », traduit du rapport en anglais publié par The Law Society. Consulté en ligne le 12/01/2022, in *Blockchain: Legal and regulatory guidance* (No 2), p.144.

récente[600], le titulaire d'un portefeuille de crypto-actifs ouvert auprès d'une société Lituanienne avait assignée cette dernière devant le Tribunal de grande instance (devenu TJ) de Montpellier en réparation de son préjudice après avoir été piraté de la somme de 300 000€. Le contrat les liant faisait application d'une clause attributive de juridiction en Lituanie. Le Tribunal de Montpellier avait débouté le demandeur, mais la Cour d'appel a reconnu la compétence du Tribunal de Montpellier au motif que le demandeur était un consommateur au sens du Règlement Bruxelles I bis[601]. La compétence territoriale reste un point majeur dans la conclusion de contrats européens et internationaux bien que l'Europe soit dotée aujourd'hui de nombreuses dispositions règlementaires, étudiées plus loin, lui permettant d'éviter les écueils imposés par des pays tiers hors Europe, particulièrement présents dans les nouvelles technologies et leurs applications blockchains.

Chapitre 2 : Le droit à la rencontre de la technologie blockchain : enjeux et chronologie

2.1 - La décentralisation au service du bien commun et d'une nouvelle société numérique

Les différentes utilisations possibles des technologies blockchains ont un impact sur plusieurs branches du droit. D'un côté, les acteurs de l'écosystème des crypto-actifs, tels les développeurs et les technophiles, avancent que les programmes informatiques 3.0 ont une portée normative « *code is law* »[602] et de l'autre côté, une majorité de juristes soutiennent le contraire « *law is code* »[603], parfois sans tenir compte du potentiel des programmes décentralisés souvent par manque de connaissances. En pratique, il semble que chacune de ces expressions influence et contribue à faire la loi de l'autre, jusqu'à ce qu'un point d'équilibre soit atteint ou accepté, généralement sous l'impulsion du marché et du législateur. Il peut être considéré que décentraliser signifie redistribuer informatiquement et socialement des rôles à un maximum d'entités différentes. L'objectif est qu'un service en ligne ne repose plus sur un ou plusieurs tiers de confiance, mais sur une multitude d'entités agnostiques qui se font mutuellement confiance grâce à une infrastructure numérique géographiquement répartie, transparente, sécurisée et sur lesquelles les participants sont, comme nous l'avons vu, *pseudo-anonymes* (blockchains publiques). En théorie, une décentralisation est toujours possible lorsqu'elle est pensée comme la désescalade d'un pouvoir déjà existant et centralisateur. Il s'agit de l'envisager comme la recentralisation d'une autonomie

[600] CA de Montpellier, Civ. 2ème ch., 21 octobre 2021, N°RG 21/00224, « L'utilisateur d'une plateforme de services de cryptomonnaies est un consommateur au sens du Règlement Bruxelles I bis », in *Actualité Droit Propriété Intellectuelle Technologie de l'information Innovation* - Cabinet Simon et Associés Avocats, « La Cour s'est prononcée sur la compétence territoriale des juridictions montpelliéraine dans une affaire de piratage d'un portefeuille de cryptomonnaies ayant donné lieu à un vol de l'équivalent de 300.000 euros ». Consulté à l'adresse suivante

[601] Règlement (UE) n°1215/2012 du Parlement Européen et du Conseil du 12 décembre 2012, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions de justice en matière civile et commerciale.

[602] LESSIG Laurence, juriste américaine de renommée internationale, « Code Is Law - On Liberty in Cyberspace », en français cette expression pourrait se traduire par « le code informatique est la loi », Janvier 2000, in *Harvard Magazine*, disponible à l'adresse suivante

[603] En français, cette expression pourrait se traduire par « La loi est du code informatique ».

auparavant dépendante d'un ou quelques tiers, vers une nouvelle forme d'indépendance, plus autonome et gérée par une multitude de nouvelles technologies décentralisées. En d'autres termes, la décentralisation implique un changement de contrôle politique et social, depuis une ou plusieurs entités centralisatrices vers des foules de personnes appartenant à une même communauté en ligne. Cependant, la décentralisation est généralement utopique si elle n'est comprise que sous son angle informatique, c'est-à-dire lorsqu'aucune recherche, ni besoin de tiers de confiance n'intervient ce qui est le cas concernant le protocole Bitcoin qui n'implique que peu de tiers de confiance pour son fonctionnement[604]. Loin de cette radicalité de la norme technique plutôt extrême aux yeux des néophytes, et faisant face à de nombreuses contradictions, il est toutefois admis dans cette recherche que la décentralisation informatique peut apporter certains bénéfices à la société numérique. Il convient néanmoins de ne pas tendre vers une radicalité et suprématie de la technique informatique par rapport aux règles de droit démocratiques et au service des justiciables comme le rappellent Jean Lassègue et Antoine Garapon « *la technique numérique emmène le monde vers toujours plus de radicalité […] une règle qui n'a plus besoin de mots et qui, de ce fait, ne s'interprète plus* »[605]. L'un des principes de base de cette étude est que la société aura toujours besoin de centralisation et de confiance intrinsèque pour prospérer. Les technologies blockchains permettent de tester des hypothèses en fonction de certains éléments actuellement centralisés et qu'il est possible d'imaginer fonctionner de manière partiellement décentralisée. Pour bien comprendre les nuances et les degrés de la décentralisation informatique qui existent pour chaque technologie blockchain, plusieurs considérations non exhaustives peuvent être présentées[606] :

(i) Les mécanismes économiques de chaque blockchain (la *Preuve de travail*, la *preuve d'enjeu* et la *preuve d'autorité*)[607] étudiées plus loin, sont conçus pour motiver et encourager chaque utilisateur du réseau à contribuer à son fonctionnement et à sa validation de manière plus ou moins décentralisée. Il s'avère que plus l'incitation économique est importante, plus les utilisateurs ont un intérêt à s'impliquer dans le réseau, créant un effet de réseau[608] attirant les communautés de développeurs puis celles des internautes.

(ii) Lorsqu'un protocole blockchain offre une transparence et une accessibilité accrues à son code source et à son code logiciel, cela renforce la confiance que les utilisateurs lui accordent.

---

[604] V. Annexe 3, Focus 1 à 6.
[605] *Op. cit.* LASSEGUE Jean, GARAPON Antoine, « Justice digitale », p.158.
[606] SRINIVASAN Balaji, « Quantifying Decentralization », 28 juillet 2017. Certains spécialistes proposent depuis 2017 six sous-systèmes différents pour mesurer la décentralisation d'une blockchain (principalement applicables au mécanisme de *preuve de travail*) : son exploitation minière, sa base de code, sa communauté de développeurs, ses échanges et transactions, ses nœuds et la propriété des adresses de la chaîne, in *news.earn.com*, disponible en ligne
[607] V. Annexe 6, Focus 1 à 3.
[608] Terme popularisé par Robert Metcalfe par sa théorie de *l'effet de réseau* ou *loi de Metcalfe*.

(iii) La taille de la communauté de développeurs est un élément clé pour maintenir une blockchain à jour et bien équipée pour relever les défis informatiques proches comme la congestion des blockchains publiques, ou plus lointaines comme la menace d'une suprématie quantique.

(iv) En principe, une blockchain plus ancienne et ayant un grand nombre d'échanges et de transactions réalisés par ses utilisateurs est considérée comme plus résiliente, décentralisée et susceptible de respecter les critères mentionnés précédemment.

(v) Le nombre d'ordinateurs (nœuds)[609] dédiés à une technologie blockchain est un facteur important, car plus il y a d'ordinateurs interconnectés sur ladite blockchain, plus les données sont immuables et copiées sur un grand nombre d'ordinateurs.

(vi) La répartition des richesses au sein d'une technologie blockchain dépend des mécanismes et des incitations économiques mis en place par sa communauté de développeurs. A cet égard, il est important d'éviter la centralisation financière de fonds en crypto-actifs sur un faible nombre d'adresses blockchains[610], pour garantir une répartition équitable des fonds entre les utilisateurs et assurer une pérennité économique de la blockchain en question.

Les technologies blockchains peuvent prendre différentes formes, plus ou moins robustes et éprouvées, en fonction des choix informatiques et socio-économiques des réseaux informatiques. Toutefois, leur objectif commun est de proposer une nouvelle version décentralisée 3.0 de l'univers numérique, plus transparent et sécurisé pour les internautes. Bien que les technologies blockchains soient parfois synonymes de déresponsabilisation pour certains juristes pour qui la crypto-économie ne serait qu'un moyen de se soustraire aux règles de droit, la présente recherche conçoit plutôt les technologies blockchains comme fondamentalement fiables et porteuses d'une confiance intrinsèque. Pour que cette vision l'emporte, il faut chercher à encadrer ces nouvelles technologies et ses applications avec modération, rigueur et pragmatisme. Il s'agit de comprendre la décentralisation pour mieux la dompter et non pas nécessairement chercher à la réguler ou l'endiguer. En effet, encadrer et contenir trop tôt cette volonté de décentralisation reviendrait à limiter toute chance de réappropriation de la sphère numérique par les internautes ou par les Etats intéressés pour réaffirmer leur souveraineté en ligne. La décentralisation est bénéfique si elle demeure à minima maitrisée dans un Etat de droit. Cela nécessite

[609] V. Annexe 3, Focus 2 et 3.

[610] Par exemple, il est possible de consulter publiquement sur la blockchain Bitcoin les adresses qui contiennent le plus de bitcoins à ce jour. Ces chiffres sont à apprécier en prenant un certain recul, car beaucoup de bitcoins sur ces adresses sont inaccessibles à leurs détenteurs qui en ont perdu l'accès (clés cryptographiques privées). Par exemple, au début de Bitcoin, environ 907 bitcoins auraient été dépensés par *Satoshi Nakamoto* et 1 125 150 bitcoins minés (soit plus de 26 milliards de dollars au 12/08/2022). Ces fonds sont très probablement inaccessibles et bloqués à jamais en raison de la perte des *clés privées* associées (contrairement à une fausse opinion mais largement répandue par certains médias que Bitcoin est un *schéma de Ponzi* puisque *Satoshi Nakamoto* centralise à lui seul cette importante quantité de bitcoins), v. « Top 100 Richest Bitcoin Addresses and Bitcoin distribution », 21 juin 2022, in BitInfoCharts, consulté le 21 juin 2022, à l'adresse suivante. V. Annexe 3 & 6

qu'il puisse concevoir ses propres équipements informatiques[611], ses propres logiciels, applications et langages informatiques. Sans cela, la maîtrise de l'écosystème et de la chaîne de valeur des identités numériques, même décentralisée, pourrait être compromise par des tiers aux objectifs souvent (géo)politiques contraires. L'Etat doit assurer son propre savoir-faire et faire émerger des talents. Sans ces éléments cumulés, les technologies blockchains et l'identité numérique décentralisée demeurent faillibles et sujettes à des dépendances et risques d'attaques[612]. Pour la majorité des cas d'usage et des applications métiers, il est supposé que seule la puissance publique en partenariat avec les acteurs spécialisés de l'écosystème numérique pourrait avoir la capacité d'atteindre et de délivrer un degré de décentralisation informatique et social juste et satisfaisant. Une identité décentralisée régalienne doit reposer sur un contrat et une négociation sociale encadrée par le droit, c'est-à-dire qu'il doit être compris puis consenti par tous les citoyens. Si l'État était en mesure de concevoir ses propres équipements informatiques, logiciels et applications, cela permettrait de maintenir une certaine maîtrise technique de l'écosystème numérique, même en cas de décentralisation de l'identité numérique. Sans cette maîtrise, des tiers pourraient compromettre la sécurité de l'écosystème et de la chaîne de valeur des identités numériques, avec des objectifs souvent contraires à ceux de l'État.

Pour conclure à ce stade, l'identité numérique décentralisée propose une redéfinition du concept d'identité numérique. Avec une identité numérique décentralisée, toute personne connaît et possède une cartographie, un tableau de bord de ses attributs d'identité numérique. Cette nouvelle souveraineté personnelle ne signifie pas pour autant que les individus émettront systématiquement seuls leur propre titre d'identité, mais plutôt qu'ils pourront contrôler certaines fonctionnalités d'utilisation et de partage de leurs données personnelles. L'utilisation de preuves cryptographiques permettra à chaque internaute de recevoir, gérer, stocker et partager en ligne ses attributs d'identité de manière vérifiable grâce à la cryptographie, permettant ainsi aux acteurs avec lesquels il les partage de les vérifier. Cela fait de cette nouvelle technologie accessible, transparente et ouverte, un outil au service du bien commun. Cette recherche considère que la société doit ainsi comprendre et s'approprier sans attendre cette nouvelle perspective technologique.

[611] Il est fait référence à la souveraineté d'un Etat sur ses « *Middlewares* » soit des « *logiciels* » et « *hardwares* » soit des « *matériels informatiques* » : « [Taïwan] détient environ les deux tiers des capacités de production mondiales de « wafers », les galettes de silicone monocristallin qui sont à la base de toutes les puces électroniques », v. aussi « conquérir ou soumettre : réflexion autour des contraintes d'une réunification "forcée" de Taïwan à la République Populaire de Chine », in *Theatrum Belli*, publié le 5 novembre 2021, consulté en ligne le 10 novembre 2021.

[612] Pour pallier à cette dépendance, la Commission européenne propose une loi sur les puces électroniques pour contrer la pénurie de semi-conducteurs et renforcer le leadership technologique de l'EU, in *Digital sovereignty*, European Commission, en ligne, consulté le 4 mars 2022.

2.1.2 La blockchain, une alternative limitée face aux institutions traditionnelles

Pour l'universitaire et juriste français, Professeur émérite du Collège de France Alain Supiot, les institutions sont indispensables à une société « *les institutions sont les cadres dans lesquels va pouvoir s'exprimer la liberté humaine* »[613]. En principe, les institutions sont régies par des règles établies démocratiquement et supervisées par un État. En apparence loin de ces principes et conventions, les systèmes décentralisés se fondent sur de nouvelles règles mathématiques et cryptographiques pour former un nouveau type d'organisation sociale en ligne. Apparaît ainsi une distinction structurelle entre ces deux environnements, car la notion d'institution dans l'un ou l'autre de ces écosystèmes ne fait pas référence aux mêmes définitions, ni réalités. Dans l'univers 3.0, une institution peut être socialement reconnue et juridiquement non conforme au droit positif. Certaines blockchains publiques (Bitcoin, Ethereum)[614] remettent en question le pouvoir de certaines institutions publiques, notamment sur le plan monétaire[615]. Elles tendent vers un réel degré de décentralisation informatique et social, c'est-à-dire qu'elles détiennent un pouvoir inédit de renversement du rôle des institutions monétaires établies. Ainsi, il est légitime de se poser certaines questions concernant l'impact des technologies blockchains dans un État de droit : à quel point une technologie blockchain peut défier un Etat de droit ? Peut-elle s'imposer comme une alternative numérique crédible face aux institutions publiques et politiques ? Certaines blockchains pourraient-elles se substituer à nos modèles sociaux et institutionnels actuels ? Cependant, il semble que la majorité des impacts et des effets physiques des blockchains sont pour l'heure limités. En effet, si les technologies blockchains avec leurs applications informatiques n'intègrent pas systématiquement et rapidement certaines exigences juridiques, institutionnelles et sociales, leur adoption sera plus lente. Les mécanismes d'incitations économiques permettant aux blockchains publiques de fonctionner apparaissent contraires à certains principes sociaux et juridiques, tels les principes d'égalité et de transparence des données ou de lutte contre l'anonymat en ligne. Cependant sur le long terme, la capacité d'innovation des blockchains publiques ne doit pas être sous-estimée, car elles pourraient permettre d'héberger de multiples applications sociales aujourd'hui balbutiantes. Au regard de nos institutions politiques et juridiques, les blockchains publiques souffrent finalement de plusieurs limites en raison de leur complexité d'articulation et de leurs modes de gouvernance. Les gouvernements et les régulateurs sont mieux équipés pour surveiller et réglementer les institutions traditionnelles, tandis que les blockchains restent encore inexplorées sur le plan réglementaire. En fin de compte, les technologies blockchains sont une alternative prometteuse aux institutions traditionnelles, mais elles restent encore limitées dans leur potentiel et leur capacité à remplacer complètement les systèmes existants. Seuls certains domaines semblent être à court et moyen termes directement confrontés à un haut degré de décentralisation informatique.

---

[613] SUPIOT Alain, Professeur émérite du Collège de France, « Le problème est de savoir comment mettre nos nouveaux outils à notre service au lieu de nous y identifier et de chercher à nous programmer », « compte-rendu d'un échange », CNNum, 24 septembre 2021, in *cnnumerique.fr*, consulté le 24/09/2021 à l'adresse suivante aussi disponible à l'adresse suivante

[614] V. Annexe 6, Focus 2.

[615] V. *infra*, II, Titre 2, 2.4

2.1.3 Introduction au concept du degré de décentralisation informatique

En droit interne, le terme de « *décentralisation* » est évoqué par l'article 1er de la Constitution du 4 octobre 1958 qui dispose que l'organisation de la République française et de ses collectivités territoriales est décentralisée[616]. En informatique et au sens de la présente étude, ce terme revêt une signification tout autre[617], celle de la désintermédiation et/ou de la dissémination géographique d'ordinateurs, c'est-à-dire de la capacité à se passer d'intermédiaires significatifs pour la conception et le fonctionnement de solutions informatiques. Pour Pierre Person, ancien député et juriste « *le niveau de décentralisation apparaît donc comme une construction complexe dont l'exhaustivité ne saurait être simplement résumée en quelques lignes* »[618]. En juin 2018, la Commission des valeurs mobilières et des changes aux Etats-Unis (« *Securities Exchange Commission – SEC* ») a introduit le concept de décentralisation informatique suffisante[619], une notion dont s'inspire le concept de degré de décentralisation introduit ci-après. Ce principe technique dispose qu'un réseau blockchain n'est véritablement décentralisé que lorsqu'aucune entité n'a la capacité de le contrôler. A cet égard, Bitcoin[620] semble particulièrement décentralisé, car une seule entité ne peut pas restreindre la capacité de ses utilisateurs à l'utiliser librement. La blockchain publique et ouverte Bitcoin se situe par conséquent au plus haut niveau de décentralisation par rapport aux autres blockchains, les termes « décentralisé » ou « décentralisation » devraient donc être réservés et circonscrits sur le plan épistémologique à ce registre (vraiment) décentralisé[621]. Dans les faits, de nombreux acteurs du Web 3.0 utilisent ces termes pour des situations et niveaux de décentralisation informatique faible ou relative, ce qui génère une large confusion dans l'esprit du public ciblé par le Web 3.0. En 2017, le coefficient de Nakamoto (venant de Satoshi Nakamoto mentionné précédemment) est décrit pour la première fois par l'ancien directeur technique de la société américaine Coinbase, Balaji Srinivasan[622]. Ce coefficient propose une mesure pour la décentralisation d'une blockchain et représente le nombre minimum d'acteurs et de critères requis pour perturber un tel réseau. Plus ce coefficient est élevé pour une technologie blockchain, plus elle est décentralisée, c'est-à-dire résiliente aux attaques informatiques[623]. Cet outil confirme depuis 2017 que

[616] Texte intégral de la Constitution du 4 octobre 1958 en vigueur, *v*. Conseil constitutionnel, disponible à l'adresse suivante
[617] GOUJON Pierre, mathématicien, « Le triomphe de la décentralisation », in *Universalis.fr*, consulté à l'adresse suivante
[618] PIERSON Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et monétaire », in *Rapport de l'Assemblée Nationale*, 2022, p.32.
[619] HINMAN William, « Digital asset transactions: when howey met gary (plastic) », 2018, traduction libre de l'anglais, pour savoir qu'est-ce qu'une décentralisation suffisante « Si le réseau sur lequel le jeton ou la pièce de monnaie doit fonctionner est suffisamment décentralisé - où les acheteurs ne s'attendraient plus raisonnablement à ce qu'une personne ou un groupe réalise les efforts essentiels de gestion ou d'entreprise - les actifs peuvent ne pas représenter un contrat d'investissement ». En d'autres termes, si un protocole et réseau n'est pas suffisamment décentralisé, la valeur du crypto-actif associé peut être dérivée des efforts d'une équipe centralisée, soit une personne ou un groupe de personnes qui, selon le public, se coordonne pour augmenter sa valeur. Inversement, si le protocole est suffisamment décentralisé, la valeur du crypto-actif ne découle pas de ce que le public croit être les efforts d'une équipe centralisée. Disponible à l'adresse suivante
[620] V. Annexe 3.
[621] V. Annexe 7.
[622] SRINIVASAN Balaji, « Quantifying Decentralization », 2017, *op. cit.*
[623] Bitcoin possède le coefficient de Nakamoto le plus élevé. Ses mesures sont nettement plus élevées que pour la plupart des autres blockchains. Cela fait de Bitcoin l'une des blockchains les plus décentralisées. Par exemple, Bitcoin compte 14 409 validateurs et obtient un *score de Nakamoto* de 7 349, alors que la plupart des blockchains obtiennent un score inférieur à 15. PLATIS Mike, SANDERFORD Bergen, « Nakamoto Coefficient », 2022, in *CrossTower*. Disponible en ligne

seule la blockchain Bitcoin est informatiquement décentralisée et résiliente. En effet, plus le nombre de nœuds[624] d'une blockchain est important, plus ses données sont décentralisées et immuables. Inversement et toujours d'un point de vue informatique, si la technologie blockchain est peu décentralisée, c'est-à-dire avec un nombre limité de nœuds (*v.* Annexes 3 et 6), l'utilisation du terme « distribué » semble plus appropriée que celui de « décentralisé ». Dans les faits, ces deux termes sont aujourd'hui utilisés de façon interchangeable et équivalente au sein du Web 3.0, en méconnaissance de ces distinctions graduelles pourtant fondamentales. Réaffirmer le concept d'un degré de décentralisation permet d'affiner les contours théoriques relatifs aux technologies blockchains pour mieux distinguer celles qui sont ouvertes, fermées ou hybrides. Cette échelle de décentralisation est également indispensable pour que les juristes puissent appréhender et qualifier avec précision chaque solution 3.0 et leurs implications juridiques. De plus, à la lumière de l'Annexe 7 de cette recherche, il est essentiel de faire la distinction entre le concept précité de décentralisation informatique et celui de décentralisation sociale, trop souvent confondue (v. Annexe 7). Le premier fait référence à la capacité d'un système informatique à fonctionner de manière autonome, c'est-à-dire sans dépendre d'autres systèmes informatiques. Le second est plus large et concerne l'indépendance sociale dans les interactions humaines, ce qui est considéré comme une utopie puisque l'Homme est intrinsèquement un être social comme exposé dans les parties précédentes. Les tentatives de décentralisation sociale s'opposent ainsi paradoxalement à toute tentative de décentralisation informatique, car la confiance en autrui est essentielle dans les interactions humaines y compris lorsqu'elles se numérisent. Par exemple, la blockchain Bitcoin est certes particulièrement décentralisée sur le plan informatique, mais son écosystème social demeure aujourd'hui centralisé par des entreprises privées et bon nombre de leurs développeurs-salariés. Si les utilisateurs de bitcoins pensent utiliser des applications informatiquement décentralisées et incensurables, leurs composantes sociales et juridiques demeurent majoritairement centralisées à ce jour. Ce constat est particulièrement vrai pour le « *Lightning Network - LN* »[625] étudié en Annexe 3, qui est un protocole informatique partiellement décentralisé, car attaché à la blockchain Bitcoin, bien que souffrant d'une centralisation sociale et informatique en raison de son jeune âge (2017). Il convient cependant de se questionner pour savoir si cette recherche de décentralisation est réellement nécessaire et dans quelles situations ? Une réponse affirmative est attribuée aux blockchains publiques qui ont par exemple pour objectif d'offrir une monnaie cryptographique au service du bien commun, tout particulièrement pour les pays où règne une instabilité monétaire ou politique. En revanche, ce n'est pas forcément le cas pour les technologies blockchains privées et hybrides d'ores et déjà utilisées à juste titre pour la gestion de l'identité numérique des personnes.

[624] V. Annexe 6, Focus 1 et 3.
[625] V. Annexe 3, Focus 4.

2.2 Les problématiques juridiques soulevées par la blockchain

Depuis plusieurs années, les technologies blockchains suscitent différentes questions juridiques, auxquelles le législateur tente de répondre de manière hétérogène mais parfois contradictoire. Le défi majeur réside dans la capacité du législateur à élaborer des règles de droit appropriées et cohérentes pour le marché, sans freiner le cycle de vie et l'adoption des technologies de troisième génération étudiées dans cette thèse. La difficulté se trouve accrue par le caractère transfrontalier et universel de la transmission des technologies blockchains, défiant la notion traditionnelle d'espace et de territoire. Dès lors, émerge la question de savoir si le droit doit s'adapter aux technologies blockchains ou si celles-ci doivent se conformer aux règles de droit existantes. Il faut de plus considérer les impacts potentiels de chaque type de blockchains sur le droit. La protection des données personnelles constitue un défi majeur, étant donné que les technologies blockchains peuvent permettre de stocker directement ou non des données de manière permanente et transparente, ce qui peut compromettre la confidentialité des données personnelles. La propriété industrielle, littéraire et artistique est également un enjeu majeur, car il peut être difficile de déterminer qui détient les droits attachés à des œuvres, innovations ou créations liées à une blockchain. Partiellement évoquée jusqu'ici et approfondie dans les parties suivantes, la règlementation des transactions financières est un autre enjeu essentiel, car les technologies blockchains permettent avant tout des échanges financiers sans l'intermédiaire de banques traditionnelles. Enfin, la responsabilité des acteurs impliqués dans l'écosystème blockchain doit être considérée au même titre que la conformité de cet écosystème aux lois et règlementations nationales et internationales qui demeurent un enjeu important pour garantir une utilisation conforme, responsable et éthique de toute blockchain. Les technologies 3.0, avec leurs algorithmes et applications décentralisées, les contrats intelligents, les DAO et les standards de l'identité décentralisée[626] se distinguent des algorithmes centralisés étudiés au préalable. Contrairement à ces derniers, complexes à réguler et à auditer en raison de leurs codes sources fermés[627], les technologies 3.0 bénéficient de leur situation permettant d'être auditées et considérées comme plus transparentes et sécurisées. Cependant, malgré la transparence supposée de ces technologies décentralisées, leur encadrement juridique s'avère également complexe, surtout pour ce qui concerne les blockchains publiques. Selon qu'un acteur économique retienne une blockchain publique, privée ou hybride pour ses besoins et/ou ses services, les conséquences juridiques ne sont pas neutres, notamment au regard du droit applicable, des juridictions compétentes, des responsabilités et des droits et obligations de chaque partie prenante[628]. Le tableau ci-après propose une photographie à ce jour des implications juridiques qu'emportent les blockchains publiques, privées ou hybrides pour leurs utilisateurs.

---

[626] V. *infra*, II, Titre I, Chap. 1

[627] JEAN Aurélie, « Les algorithmes font-ils la loi ? », « […] il est impossible de réguler un algorithme pour la simple et bonne raison qu'il est impossible de l'évaluer entièrement », *op. cit.* Position de lecture dans le livre : 23%.

[628] BOURDAIS Gaëtan, « DSA : quelle responsabilité pour les fournisseurs de service intermédiaires ? (2/7) », in *Shift-avocats*, disponible à l'adresse suivante

Branches du droit impactées[629]	**Blockchain(s) publique(s)**	**Blockchain(s) privée(s)**	**Blockchain(s) hybride(s)**
Protection des données à caractère personnel (RGPD)	✕ ou ~	✓✓	✓✓
Protection des libertés fondamentales des internautes	✓✓	✓✓	✓✓
Respect du droit des obligations	~	✓✓	✓✓
Respect de la propriété intellectuelle	~	✓✓	~ ou ✓✓
Respect du droit de la consommation	~	✓✓	✓✓
Respect du droit bancaire, fiscal et financier	~ ou ✕	~ ou ✓✓	~ ou ✓✓
Identification des parties	~	✓✓	✓✓
Principales problématiques juridiques	*Quelle juridiction compétente ?* *Qui possède la personnalité juridique ?* *Quel droit applicable ?* *Qui est responsable des dommages* *(Nœuds du réseau, développeurs, fournisseurs de service) ?*	*Quelle juridiction compétente ?* *Qui possède la personnalité juridique ?* *Quel droit applicable ?* *Qui est responsable des dommages* *(Nœuds du réseau, développeurs, fournisseurs de service) ?*	*Quelle juridiction compétente ?* *Qui possède la personnalité juridique ?* *Quel droit applicable ?* *Qui est responsable des dommages* *(Nœuds du réseau, développeurs, fournisseurs de service) ?*

[629] V. également Annexe 12.

En 2022, bien que le nombre de litiges relatifs aux blockchains ouvertes et publiques soit en constante augmentation en raison d'une adoption progressive par les internautes et les entreprises (à titre d'exemple les litiges liés aux bitcoins[630]), nombreuses sont les questions précédentes à rester sans réponse ou certitude. Si le nombre de ces litiges demeure aujourd'hui marginal par rapport à d'autres secteurs, il est probable à l'avenir que les tribunaux soient contraints de trancher les litiges en fonction de chaque catégorie de blockchain concernée. Les blockchains publiques rendent complexe la recherche de responsabilités, notamment en raison du pseudo-anonymat évoqué au chapitre précédent. En effet, chaque interaction se trouve potentiellement répartie entre de nombreux ordinateurs géographiquement répartis dans le monde et dont les propriétaires peuvent être difficilement identifiables. Cette complexité d'identification numérique peut devenir une source de difficulté en matière notamment d'application de décisions de justice complexes (recherche des auteurs des faits, des responsabilités, des préjudices subis). En effet, chaque transaction est potentiellement distribuée entre de nombreux ordinateurs situés dans le monde entier et appartenant à des propriétaires dans certains cas impossibles à identifier. La gestion des données personnelles est un sujet particulièrement sensible pour toute blockchain publique sur lesquelles il est en principe interdit de publier ou d'administrer des données personnelles qui seraient non chiffrées par des mécanismes de pseudo-anonymisation. Certaines menaces sont réelles comme la publication et l'exposition délibérée[631] de données personnelles ou le vol et la perte de clés cryptographiques. Ces quelques exemples peuvent engendrer de graves violations de la vie privée des personnes, parfois en viciant leurs consentements numériques que l'identité décentralisée propose précisément de renforcer.

Les blockchains privées et hybrides proposent, quant à elle, une infrastructure technique plus malléable, permettant ainsi une conformité par conception. La gouvernance représente le socle technique autant que juridique au sein duquel il est possible de savoir qui est décisionnaire et qui contrôle la blockchain, qui y a accès et comment y avoir accès, ainsi qu'où se trouvent chaque nœud (v. Annexes 3 et 6). En somme, une blockchain fermée assure l'identification des responsables techniques et éventuellement de leurs responsabilités afférentes. De ce fait, il est plus facile de déterminer dès sa conception les lois applicables et de connaître les juridictions concernées en cas de litige. Pour un utilisateur, le dilemme est de savoir s'il doit faire confiance à une blockchain contrôlée par des programmes informatiques régis par une communauté d'internautes (blockchains ouvertes), ou à une blockchain contrôlée par du code informatique encadré par des responsables et des lois clairement identifiés (blockchains fermées). Répondre à ce dilemne impliquerait de comprendre les besoins de la société susceptible d'avoir probablement besoin des deux systèmes. Finalement, prendre connaissance de la catégorie de blockchain concernée permettrait par exemple d'orienter en droit par exemple les juridictions compétentes, de

[630] PAPPERS, « Recherche de décisions de justice – Pappersjustice ». Consulté le 19 octobre 2022, à l'adresse suivante
[631] Début 2023, une nouvelle fonctionnalité permet à tout internaute de publier sur la blockchain Bitcoin de façon immuable des informations de toutes natures (photos, vidéos, codes, etc.). Des informations personnelles ont d'ores et déjà été publiées et injectées directement dans les blocs de Bitcoin. Pour plus d'informations, voir le site suivant

connaître les effets juridiques potentiels, tels qu'un lieu de stockage, le traitement et le transfert de données, avant la qualification exacte dudit réseau décentralisé. Les technologies blockchains n'engendrent pas a priori de vide juridique (à l'exception peut-être de Bitcoin), à l'instar de l'Internet lors de sa création, mais plutôt des incertitudes juridiques, notamment par des conflits de lois et des difficultés d'interprétation et d'application.

2.3 Le statut juridique de la blockchain et des crypto-actifs en droit interne

Une première reconnaissance légale de la blockchain est intervenue en 2016 par la reconnaissance juridique du « Dispositif d'Enregistrement Électronique Partagé - DEEP »[632], davantage connu du grand public sous son appellation anglophone de « *blockchain technology* ». La Commission[633] d'enrichissement de la langue française a publié une liste de termes et de définitions (actifs numériques, contrats intelligents, cyber jeton, etc.) applicables aux technologies blockchains et à leurs applications sans oublier de rappeler dans le même temps l'usage de la langue française pour certaines situations[634]. Cette reconnaissance normative et linguistique française témoigne de l'intérêt et de l'adoption progressive de ces nouvelles technologies qui révolutionnent techniquement le partage d'informations numériques, et conceptuellement, son approche par le marché. La France est le second pays d'Europe, après l'Estonie[635], à avoir adopté un cadre juridique dédié aux technologies blockchains avec la loi PACTE du 22 mai 2019 qui a notamment introduit une définition du *jeton numérique*, initialement non défini dans le Code monétaire et financier (CMF), traduit de l'anglais « *digital token* », par « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé* [DEEP] *permettant d'identifier, directement ou indirectement, le propriétaire dudit bien* »[636]. Il peut être d'ores et déjà rappelé que la qualification juridique du *jeton*, évoqué plus loin, dépend en réalité de sa nature, c'est-à-dire que s'il est considéré comme un actif numérique, il est soumis aux dispositions du CMF,

---

[632] Art. L. 223-12 et L. 223-13 du CMF, *v.* Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse, prise en application de la loi Macron du 6 août 2015 pour la croissance, l'activité et l'égalité des chances, qui confère à la technologie blockchain une première reconnaissance légale, *v.* également, « La France entérine l'usage de la blockchain pour certains titres financiers et confirme son avance législative à l'échelle internationale », in *Actualités & Publications*, Gide Loyrette Nouel, cabinets avocats, 7 janvier 2019, disponible en ligne

[633] Avis et communication, JOEA n°0013 du 15 janvier 2021, Commission d'enrichissement de la langue française, v. Vocabulaire des actifs numériques

[634] Art. 3 et 4 de la Loi Toubon n° 94-665 du 4 août 1994 relative à l'emploi de la langue française : « toute inscription ou annonce apposée ou faite sur la voie publique, dans un lieu ouvert au public ou dans un moyen de transport en commun et destinée à l'information du public doit être formulée en langue française lorsqu'elles sont apposées ou faites par des personnes morales de droit public ou des personnes privées exerçant une mission de service public. Seules les personnes morales de droit public sont dans l'obligation d'utiliser ces traductions officielles. »

[635] PICRON Antoine, « L'Estonie : modèle d'un état plateforme e-gouverné », in *Institut Sapiens*, « D'abord à partir de 2008, les pouvoirs publics estoniens ont progressivement intégré la blockchain au sein des administrations », p.31., accessible en ligne. V. *supra*, I, Titre 1, 2.2.2.1.c

[636] Art L.552-2 du CMF, *v.* CARRIER Marine, avocate, « Ce que MiCA va changer pour les prestataires de services sur crypto-actifs (PSAN/CASP) », in *Village de la Justice*, 17 octobre 2022, disponible à l'adresse suivante

mais s'il est considéré comme un titre financier[637] il renvoie dès lors aux caractères communs d'un titre financier à savoir créé par voie d'émission, matérialisé par une inscription en compte ou par une inscription dans une blockchain, négociable par virement de compte à compte et que sa possession vaut titre. Sa qualification juridique importe par conséquent que s'il est considéré comme un titre financier, il se trouve ainsi soumis à des règles beaucoup plus strictes lors de son émission et de sa négociation.

Il peut être rappelé brièvement la genèse des principaux textes intervenus en droit interne de 2016 à 2022 au bénéfice des technologies blockchains :

- L'ordonnance n°2016-520 du 28 avril 2016[638] relative aux bons de caisse introduisant dans le CMF une section 2 relative aux minibons et prévoyant leur émission et cession via une blockchain. Il est remarqué qu'aucune distinction entre blockchains ouvertes et blockchains fermées n'est retenue.
- La loi n°2016-1691 du 9 décembre 2016, dite Sapin 2[639], habilitant le gouvernement à prendre des mesures concernant le droit applicable aux titres financiers et aux valeurs mobilières afin de permettre leur représentation et transmission au moyen d'une blockchain.
- L'ordonnance n°2017-1674 du 8 décembre 2017[640] relative à l'utilisation d'un DEEP pour la représentation et la transmission de titres financiers prévoyant la représentation et la transmission de titres financiers au moyen d'une blockchain.
- Le Décret n°2018-1226 du 24 décembre 2018[641] relatif à l'utilisation d'un DEEP pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons, précisant les conditions d'application des ordonnances du 28 avril 2016 et du 8 décembre 2017 sus visées.
- La Loi n°19-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite loi PACTE[642], encadrant les ICO[643] et les actifs numériques au sens de l'article L. 54-10-1 du CMF, ou d'un jeton au sens de l'article L. 552-2 du même code. C'est la reconnaissance de l'inscription de la propriété d'un actif sur une blockchain.
- Le Décret n°2019-1213 du 21 novembre 2019[644] relatif aux prestataires de services sur actifs numériques venu compléter le titre IV du livre V du CMF avec le nouveau chapitre X Prestataire sur actifs numériques (PSAN) intégrant la notion de DEEP. Remarquons que ce régime français des PSAN soumis à un enregistrement obligatoire auprès de l'AMF ou à un agrément optionnel

[637] Art. L.211-1 du CMF.
[638] JORF n°0101 du 29 avril 2016.
[639] JORF n°0287 du 10 décembre 2016.
[640] JORF n°0287 du 9 décembre 2017.
[641] JORF n°0298 du 26 décembre 2018.
[642] JORF n°0119 du 23 mai 2019.
[643] BOUILLET-CORDONNIER Ghislaine, et al. « La finance numérique, aspect juridiques et fiscaux du crowdfunding et des cryptoactifs », Titre I, chap. 2, pp.135-143, Cabinet Albatross Legal, 2021, *v*. également, « Tour d'horizon du droit financier suisse, crowdfunding - ICO-STO », *op. cit.* ⟨hal-03282220⟩.
[644] JORF n°0271 du 22 novembre 2019.

est régulièrement remis en question par de nombreux acteurs de cet écosystème (avocats, sociétés, associations) et ce pour de multiples raisons[645].

- L'ordonnance n°2020-1544 du 9 décembre 2020[646] renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques.
- La proposition de Règlement européen sur le marché des crypto-actifs (« *Markets in Crypto-Assets* ») du Parlement et du Conseil, dit MiCA, publié le 5 octobre 2022, ambitionnant de créer un cadre juridique harmonisé au sein de l'UE pour les activités concernant les crypto-actifs. Ce Règlement fait l'objet d'une étude détaillée plus loin dans ce chapitre.

Les observations précédentes nous amènent à considérer que le législateur français a opté pour une « *régulation par le marché* » tandis que le législateur européen a opté pour une « *régulation par l'infrastructure logicielle* », ce que nous étudierons plus loin, mais également « *par le marché* », toutefois inspirée des textes du législateur français.

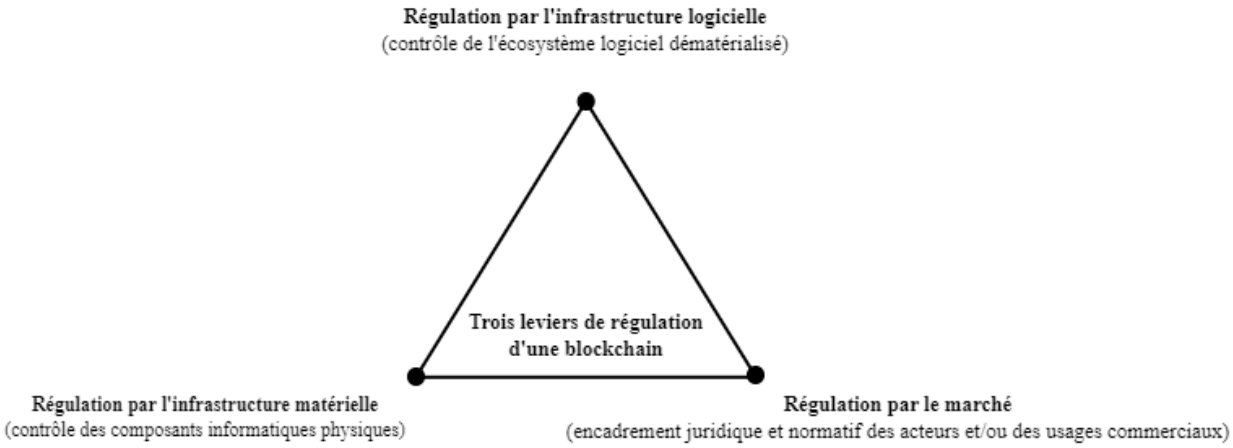


Schéma inspiré des propos du chapitre 11 : Blockchain & regulation 1, in « Blockchain and the Law »,

De FILIPPI Primavera.

[645] Si le régime des PSAN a le mérite de faire office de *« bac à sable »* règlementaire à l'échelle de l'UE, il est souvent remis en cause en raison de son coût est important (entre 35.000€ et 150 000€ pour obtenir cet enregistrement via un cabinet d'avocats). De plus, cet enregistrement n'améliore pas le respect d'un *droit au compte* pour les PSAN (dont les comptes bancaires sont régulièrement fermés sans justifications). Finalement, ce statut n'empêche pas des acteurs étrangers de proposer leurs services à des clients français en vertu du principe et de l'exception de la « reverse solicitation » ou « fourniture de services sur la seule initiative du client » dont dispose la Directive MiFID 2 (la *sollicitation inversée* est dans notre cas le nom donné aux circonstances dans lesquelles un client potentiel approche, supposément à sa propre initiative, une plateforme d'échange de crypto-actifs étrangère). Cette demande ne doit en principe pas être en réponse à une publicité ou à un marketing de quelque nature que ce soit de la part de la plateforme d'échange (ce qui n'est souvent pas le cas, car ces plateformes étrangères sollicitent les internautes français depuis 2016).

[646] JORF n°0298 du 10 décembre 2020.

En définitive, malgré les efforts précurseurs et non négligeables du législateur français concernant la qualification et l'encadrement juridique des crypto-actifs, diverses difficultés subsistent. Une première étape pour les résoudre pourrait consister à les reconnaître en levant les tabous - des lobby - bancaires et institutionnels persistants et à promouvoir en même temps un décloisonnement des consciences grâce à une subtile association entre éducation, innovation et collaboration. Ceci permettrait de légiférer en faveur de nouvelles approches juridiques et économiques compte tenu du contexte actuel technologique, particulièrement riche, en collaboration active avec les grandes institutions publiques, financières et gouvernementales.

2.4 La blockchain face à la protection des données (RGPD) au sein de l'UE

Le 9 mars 1993, le mathématicien, ingénieur informatique et Cypherpunks Eric Hugues considérait qu'« *une affaire privée est une chose que l'on ne veut pas que le monde entier sache, mais une affaire secrète est quelque chose que l'on ne veut pas que quiconque sache*. *La vie privée c'est le pouvoir de révéler ce que l'on veut à qui on le veut* »[647]. Plusieurs décennies plus tard, les écosystèmes des crypto-actifs ainsi que des technologies blockchains s'inspirent toujours des idées publiées par Eric Hugues dans son « *Manifeste du Cypherpunk* »[648]. Depuis plusieurs années, certains de ces principes apparaissent en accord avec certains textes et règles de droit consacrés à la protection des données à caractère personnel. La notion de donnée trouve son origine dans la loi Informatique et Libertés du 6 janvier 1978[649] . En 2004, l'article 2, 2ème §, d'une nouvelle version de la loi, aujourd'hui abrogée pour être amendée, énonçait que « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification* (…) »[650]. L'évolution laisse paraître un attachement tout particulier à la protection des données et des identifiants à caractère personnel, en référence au pseudo-anonymat en ligne précédemment évoqué. Plus tard, le Règlement (UE) 2016/679 du Parlement européen et du Conseil sur la protection des données, dit RGPD[651], entre en vigueur le 25 mai 2018 et transpose les principes fondamentaux de la définition susmentionnée du législateur français en matière de protection des

[647] HUGHES Eric, traduction libre de l'anglais, « A Cypherpunk's Manifesto », disponible à l'adresse suivante
[648] Wikipedia contributors, « Cypherpunk », 2023, disponible à l'adresse suivante
[649] L'art. 4 de la loi introduit la notion de « données nominatives » en 1978, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale », disponible à l'adresse suivante
[650] *Ibid*. Version en vigueur du 07 août 2004 au 25 mai 2018.
[651] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), entré en vigueur le 25 mai 2018, consulté en ligne le 10 novembre 2021.

données à caractère personnel. Ce Règlement énumère les éléments constitutifs de l'identité d'une personne physique ciblée, aux fins d'assurer une protection accrue de ses données, au visa de son article 4 : « *toute information se rapportant à une personne physique identifiée ou identifiable* (…) *; est réputée être une 'personne physique identifiable' une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ». Outre cette définition juridique consacrée à la notion de donnée, il faut considérer sa définition informatique, plus générale, selon laquelle il s'agit de « *l'ensemble des informations qui décrivent quantitativement ou qualitativement une entité, un individu, une situation, un phénomène ou encore une personne morale* »[652]. Avant d'examiner en détail les conséquences juridiques du RGPD applicable aux technologies blockchains et à l'identité numérique décentralisée (IND) étudiée plus loin, il paraît judicieux d'introduire le tableau suivant :

[652] JEAN aurélie, « Les algorithmes font-ils la loi ? », in *Humensis*, *op. cit.*, position de lecture dans le livre : 16%.

Qui est concerné par le RGPD ?	Quelles sont les données visées par le RGPD ?	Quels droits possèdent les personnes ?	Quelles obligations pour les organisations ?	Comment prouver sa conformité ? Quelles sont les sanctions ?
Toutes les organisations traitant les données personnelles de personnes physiques : administrations, établissements publics, les associations, les entreprises et leurs sous-traitants.	Toute information qui se rapporte à une personne physique identifiée ou identifiable : nom, prénom, adresse postale, géolocalisation, adresse électronique (personnelle ou professionnelle), adresse IP, les cookies de navigation, n° d'identification personnelle (CNI, carte de sécurité sociale, etc.).	La protection des droits des individus est renforcée. Les personnes doivent être informées de façon concise, compréhensible et aisément accessible sur l'usage des données collectées. Elles doivent donner leur consentement pour ce traitement et peuvent s'y opposer. L'objectif est de redonner aux personnes la maîtrise des données les concernant.	Obligation de mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires et adaptées à leur activité pour la protection des données personnelles, tout au long du processus de développement de leurs produits ou services.	Plusieurs solutions s'offrent aux organisations : Informer les personnes physiques au moment de la collecte des données sur les finalités et la durée de conservation de données ainsi que sur leurs droits (cf. ci-après) ; Recueillir la preuve de leurs consentements ; Notifier à la CNIL toute faille de sécurité dans son système de traitement des données et prévenir dans les meilleurs délais les personnes concernées en cas de destruction, perte ou fuite de leurs données ; Maintenir un registre listant tous les traitements de données ; Analyser l'impact des éventuels traitements numériques à risque ;

				Désigner un délégué à la protection des données (*DPO*) pour les entreprises. Selon la catégorie de l'infraction constatée, l'amende s'échelonne de 2% à 4% du chiffre d'affaires annuel mondial consolidé de l'entreprise (ou de 10 à 20 millions d'euros).

En droit communautaire, le RGPD prévoit, dans ses 176 considérants introductifs et 99 articles, de fluidifier les données à l'échelle européenne. C'est pourquoi le choix d'un Règlement et non d'une directive a été privilégié pour favoriser une telle harmonisation qui s'avère en pratique peu intuitive pour les internautes. Il s'applique à tout responsable de traitement[653] de données, entreprises, institutions publiques, associations[654], qu'ils soient au sein de l'UE ou qu'ils visent tout simplement des résidents européens[655]. Les différents acteurs de l'environnement numérique se trouvent aujourd'hui contraints d'observer une multitude de principes fondamentaux et de critères définis par le RGPD, notamment un droit à l'effacement, à la portabilité, à la transparence des données, à la durée de conservation des données, au consentement des individus, à un droit de rectification, à la responsabilité des responsables de traitement, à un droit à l'information. Il dispose dans son article 5 « *Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* [principe de minimisation des données] »[656]. Ce principe représente un Graal sécuritaire identifié comme un fondement en matière de gestion et de protection des données personnelles, notamment au regard du nouveau concept informatique d'identité numérique décentralisée. En complément des considérations précédentes, il est nécessaire de prendre en compte à tout le moins trois situations principales pouvant justifier une collecte, une utilisation commerciale, ou

[653] CNIL, Règlement européen sur la protection des données, Chap. 4, Responsables du traitement et sous-traitants, art. 24, consulté en ligne le 10 novembre 2021.
[654] CNIL, « Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal », consulté le 19 octobre 2022, à l'adresse suivante
[655] JEAN Aurélie, « Les algorithmes font-ils la loi ? », « Le RGPD a en cela bousculé la règle qui regardait auparavant le lieu de stockage des données uniquement », position de lecture dans le livre : 86%.
[656] CNIL, Rectificatif du Règlement (UE) 2016/679, JOUE L127 2 du 23/05/2018, art. 5.1-c : principes relatifs au traitement des données à caractère personnel, CHAPITRE II - Principes, consulté en ligne le 15 septembre 2021.

d'autres formes de traitement licite de données à caractère personnel conformément à l'article 6 du Règlement[657]. En premier lieu, le traitement peut être fondé sur l'exécution d'un contrat auquel la personne concernée est partie ou sur des mesures précontractuelles prises à sa demande. Ensuite, le traitement peut être nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée. Enfin, le traitement peut être imposé par des textes ou être nécessaire à l'exécution d'une mission d'intérêt public, ou à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers. Si le traitement ne correspond pas aux points susvisés, alors il ne peut être réalisé qu'avec le consentement de la personne concernée. A cet égard, les cookies[658] et les publicités en ligne ciblent aujourd'hui les personnes sans pour autant que leur consentement soit pleinement libre et éclairé[659]. Remarquons qu'aucun article ne prohibe la conservation de données biométriques sur des serveurs centralisés, dès lors que des mesures et niveaux de garanties et de sécurité suffisants ont été adoptés pour faire face aux risques spécifiques en la matière. Toute négligence ou violation entraînera des sanctions ensuite d'une mise en demeure de la CNIL[660]. Si les moyens déployés par le(s) responsable(s) de traitement étaient insuffisants, une amende jusqu'à 2% du chiffre d'affaires mondial consolidé du groupe ou 10 millions d'euros peuvent être prononcés[661]. S'il existe une atteinte aux données personnelles, cette amende peut monter jusqu'à 4% du chiffre d'affaires mondial consolidé du groupe ou bien 20 millions d'euros du chiffre d'affaires mondial consolidé du groupe[662]. Deux années sont passées entre l'adoption en 2016 du RGPD et de son application en 2018, un délai mis en place pour laisser le temps aux acteurs du numérique européens de s'y conformer. Dans les faits, la CNIL a prononcé des sanctions réellement dissuasives à partir de 2019[663]. De nombreux sites internet se sont mis en conformité, mais l'application stricte et par conception du Règlement pour certains d'entre eux reste encore insuffisante. Son effectivité juridique demeure variable selon les acteurs concernés. En 2021, Google a écopé d'une amende prononcée par la CNIL de 100 millions d'euros[664] avec une augmentation des amendes ces dernières années[665], dont celle de 125.000 euros, prononcés à l'encontre

[657] CNIL, RGPD, Chapitre II - Principes, art. 6, consulté en ligne le 10 novembre 2021.
[658] Pour plus d'informations sur les cookies et autres traceurs, *v.* le site de la CNIL à l'adresse suivante
[659] Remarquons qu'avant l'application du RGPD le consentement en ligne était majoritairement tacite, c'est-à-dire que le simple fait de naviguer un certain temps sur un site internet supposait le consentement tacite de la personne.
[660] Selon l'article 83 du RGPD, une mise en demeure peut ainsi être dommageable pour les entités ciblées en matière d'image de marque et en raison du caractère public des sanctions imposées par la CNIL, *v.* la liste des sanctions sur le site de la CNIL, consulté en ligne le 10 novembre 2021.
[661] « Sanctions et amende en cas de non-respect du RGPD », in *LegalPlace*, en ligne, publié le 23 mars 2018, consulté le 10 novembre 2021.
[662] CNIL, « Sanctions », consulté en ligne le 10 novembre 2021.
[663] *Ibid.* Disponible à l'adresse suivante
[664] CNIL, « Cookies : le Conseil d'État valide la sanction de 2020 prononcée par la CNIL contre Google LLC et Google Ireland Limited », Consulté le 20 octobre 2022, à l'adresse suivante
[665] VITARD Alice, « Avec 1,2 milliard d'euros d'amendes, l'année 2021 marque-t-elle un tournant dans le respect du RGPD ? » in *usine-digitale.fr*, « En 2021, le montant des amendes infligées au sein de l'UE dans le cadre du RGPD a été multiplié par 7 par rapport à l'année précédente. Il a atteint 1,2 milliard d'euros avec la sanction record de 746 millions d'euros infligée à Amazon par le Luxembourg », 28 janvier 2022.

de la société Cityscoot[666] pour avoir manqué à son obligation de veiller à la minimisation des données en violation de l'article 5.1.c du RGPD, dans le prolongement de celle de 175.000€ prononcé à l'encontre de la société de location de voiture de courte durée UBEEQO[667]. En réalité, les moyens de contrôle de la CNIL demeurent dérisoires pour les violations de données à caractère personnel de citoyens européens (seulement 145 sanctions prononcées par la CNIL depuis 2011, soit une moyenne d'environ 13 sanctions par an)[668]. Aussi, certaines sociétés étrangères arrivent à contourner l'application du RGPD, une pratique à laquelle la CNIL a été confrontée malgré elle début 2023[669].

Certes, si l'application du RGPD est lente, elle est progressive et structurelle pour les acteurs évoluant dans la sphère numérique. Le Règlement sert en effet de référence à d'autres régulations sur la protection des données comme en Chine et en Californie (v. ci-après). A cet égard, le RGPD contribue à une forme de sevrage numérique des acteurs du Web à propos de la récolte massive de données à caractère personnel des internautes. En 2019, l'Organisation internationale de normalisation (ISO) lance une initiative de normalisation pour établir des lignes directrices concernant la protection des données personnelles en réponse à l'adoption et à la mise en œuvre du RGPD. Ce mouvement de normalisation a pour objectif de soutenir l'application d'autres législations concernant la protection des données personnelles et inspirées du RGPD, tels le PIPL[670] adopté en Chine et le CCPA[671] adopté aux Etats-Unis[672]. Des normes ISO/IEC 27701[673] viennent compléter une certification permettant de faire reconnaître un système de management de la protection de la vie privée dans le cadre de la gestion des risques liés aux traitements des données personnelles. Ces normes sont conçues de manière à avoir une portée aussi large que possible. Le RGPD ne concerne que les personnes physiques et non les personnes morales[674], ce qui est une lacune que l'identité décentralisée pourrait contribuer à combler. Dans de nombreux cas d'utilisation, les attributs d'identité numérique des personnes morales, tels leurs chiffres d'affaires, leurs statistiques comptables et leurs données de géolocalisation, sont collectés puis revendus

[666] CNIL, « Géolocalisation de scooters de location : sanction de 125 000 euros à l'encontre de CITYSCOOT », 16 mars 2023, Citysccot collectait des données relatives à la géolocalisation des scooters toutes les 30 secondes, disponible à l'adresse suivante
[667] BOURDAIS Gaëtan, « Géolocalisation de véhicules : le gendarme CNIL contrôle ! », in *Shift avocats*, 29 mars 2023. Disponible à l'adresse suivante
[668] CNIL, « Les sanctions prononcées par la CNIL, année 2022 », consulté le 20 octobre 2022, à l'adresse suivante
[669] TAZROUT Zacharie, « La CNIL met en lumière une possible faille du RGPD », in *Siècle Digital*. 25 janvier 2023, disponible en ligne
[670] La Personal Information Protection Law (PIPL) est une loi adoptée le 20 août 2021 en Chine. Elle s'inspire du RGPD européen pour fournir une première loi dédiée à la protection des données personnelles des citoyens chinois.
[671] California Consumer Privacy Act (CCPA) adopté en 2018 et entré en viguer au 1er janvier 2020 dans plusieurs Etats américains, in *US State Privacy Legislation Tracker*, consulté en ligne le 19 janvier 2022.
[672] Bien que chaque texte législatif confère une reconnaissance et une protection aux données personnelles, leur portée et leur application diffèrent considérablement, notamment en raison de leur titre respectif. Par exemple, le CCPA protège les personnes en tant que consommateur, tandis que le RGPD protège les personnes et leurs données contre toute atteinte à leur vie privée. De plus, les sanctions en cas de violation du CCPA sont peu dissuasives et dérisoires, allant de 2500 à 7500 dollars par violation, comparée aux sanctions plus strictes applicables en vertu du RGPD. Le RGPD est plus guidé par une finalité humaniste, tandis que le CCPA poursuit une finalité capitalistique, *v. supra*, II, Titre 1, 2.2.6
[673] Norme publiée en août 2019 qui étend le champ d'application du Système de Management de la Sécurité de l'Information - SMSI de la norme ISO 27001 pour assurer dorénavant la protection des données personnelles. Cette norme est une extension des ISO/IEC 27001 et ISO/IEC 27002.
[674] Le considérant 14 du RGPD dispose que « la protection conférée par le présent règlement devrait s'appliquer aux personnes physiques (…) ».

sans transparence, ni consentement des représentants et gestionnaires de ces personnes morales. En d'autres termes, la collecte et l'utilisation (revente) de ces données se font sans la confiance nécessaire. Il serait souhaitable que le RGPD protège davantage certaines données des personnes morales ou clarifie la notion de consentement de la personne physique agissant pour le compte d'une personne morale. Pour répondre à cette problématique, les sociétés IN Groupe, Orange et Agdatahub proposent une solution d'identité numérique décentralisée inédite désignée « Agriconsent »[675]. Grâce à l'identité numérique décentralisée, les agriculteurs peuvent déjà gérer de manière autonome et en toute confiance leurs données personnelles en tant que personnes physiques et représentants de personnes morales générant de multiples données sensibles, comme mentionné précédemment. Pour cela, une application mobile spécifique permet d'émettre et de révoquer des attestations vérifiables, étudiées plus loin, liées à une blockchain privée pour gérer les activités professionnelles des exploitations agricoles (demandes de certificats phytosanitaires, cycle de vie d'une exploitation auprès du RCS par exemple). Le RGPD pourrait ainsi être amendé pour renforcer le déploiement de telles solutions.

A l'origine, les technologies blockchains ont pour vocation de libérer les personnes du principe d'autorité comme nous l'avons évoqué. A l'inverse, le RGPD exige que les responsabilités soient identifiées puis clairement désignées en matière de gestion des données à caractère personnel. En raison de l'absence d'intermédiaire et donc de responsable de traitement dans un protocole numérique comme une blockchain, le RGPD semble incompatible avec cette technologie[676]. De plus, les outils cryptographiques qu'utilisent les blockchains et qui favorisent par conception le pseudo-anonymat des internautes ne sont pas infaillibles et peuvent permettre de ré-identifier directement ou indirectement une personne physique[677]. Pour rappel, toute technologie blockchain requiert l'utilisation native d'une clé publique, qui dans certaines situations représente un moyen d'identification pour ses utilisateurs. Cette clé publique est systématiquement inscrite et enregistrée dans une blockchain afin de permettre des enchaînements cryptographiques infalsifiables. Similaire à un identifiant numérique tel qu'une adresse *IP* (« *Internet Protocol* »), une clé publique peut ainsi se voir imposer certaines contraintes légales au regard du RGPD (voir le tableau suivant). Selon la jurisprudence européenne[678] et française[679], une adresse IP représente une donnée à caractère personnel, ce qui signifie par transposition qu'une clé

[675] « Agdatahub : une identité numérique sur blockchain pour le monde agricole ». 2 mars 2022, [Vidéo]. Disponible sur YouTube
[676] CNIL, « Premiers éléments d'analyse de la CNIL - Blockchain », septembre 2018, consulté en ligne le 04/10/2021, p.2, « Le modèle décentralisé de gouvernance des données de la technologie Blockchain et la multiplicité des acteurs intervenant dans le traitement de la donnée complexifient la définition des rôles de chacun ».
[677] Notons que les systèmes de services et de courriels en ligne (Gmail, Outlook) ne sont en principe pas dénué de toute donnée personnelle et incluent les noms et prénoms des destinataires, alors même que l'identité décentralisée peut permettre de s'assurer d'une correspondance avec un destinataire sans pour autant posséder certaines de ses informations personnelles.
[678] CJUE, Arrêt de la Cour (grande chambre) du 24 janvier 2008, (affaire C-275/06) dans laquelle la Cour a été saisie d'une question préjudicielle dans le litige opposant l'association Promusicae à la société Telefonica (Italienne) au sujet de son refus de divulguer des données à caractère personnel relatives à l'utilisation de l'Internet aux moyens de connexion fournies par elle. V. également ITEANU Olivier « Quand le digital défie l'Etat de droit », Ed. Eyrolles, l'auteur cite cet arrêt de la CJUE en rappelant que cette dernière reconnaît par conséquent qu'une adresse IP est une donnée à caractère personnel.
[679] Cass. civ. 3 novembre 2016, 15-22.595, Publié au bulletin | La base Lextenso, consulté en ligne le 10 novembre 2021.

publique pourrait l'être également (au même titre qu'un VC et DID étduiés plus loin). Si une clé publique est qualifiée de donnée à caractère personnel, il faut alors considérer qu'une blockchain traite de données personnelles. De même, selon le groupe de travail « *Article 29* » sur la protection des données (G29)[680], certaines techniques cryptographiques adjacentes comme le hachage[681] peuvent être qualifiées de donnée à caractère personnel et ainsi se voir encadrées par le RGPD selon les situations comme le suggère le tableau suivant. Même si un acteur utilise des clés privées et publiques pour signer des transactions et des algorithmes d'horodatage pour garantir l'intégrité des données sur une blockchain, cela ne signifie pas que les données personnelles ne sont pas traitées. Le pseudo-anonymat n'est pas totalement sûr et peut permettre d'identifier indirectement une personne physique dans certaines circonstances. Dès lors, l'application des principes et des exigences du RGPD est incontournable pour les technologies blockchains, une exigence que toutes les blockchains publiques ne remplissent pas à ce jour. A ce titre, nous supposons que certaines blockchains publiques développeront de nouvelles mises à jour dont la conformité juridique pourrait être partielle ou totale, car fondés sur des solutions d'engagement cryptographiques et/ou sur des écosystèmes de tiers de confiance conformes et dédiés à cet effet. Aujourd'hui, cette recherche de conformité des acteurs du Web 3.0 est, certes, balbutiante, mais trop largement sous-estimée par les juristes. Comme le constate le tableau suivant, selon qu'il s'agisse d'une blockchain publique, privée ou hybride, les droits des personnes mentionnés en vertu du RGPD ne s'appliquent pas de façon systématique, ni linéaire :

[680] *Op. cit.*, « Article 29 Working Party | European Data Protection Board », vu in « L'identité numérique : quelle définition pour quelle protection ? », disponible en ligne

[681] Pour rappel, le *hachage* est un condensé de preuve de données chiffrées qui conduit en principe à une anonymisation des informations d'origine (post-chiffrement). TechTarget, « Hachage (hashing) », in *LeMagIT*. Consulté le 12 juin 2022, à l'adresse suivante, « Le hachage est la transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine. Le hachage est notamment employé pour indexer et récupérer les éléments d'une base de données. Il est en effet plus rapide de trouver l'élément d'après la clé de hachage réduite plutôt qu'à l'aide de la valeur d'origine. Cette fonction est également utilisée dans de nombreux algorithmes de chiffrement ».

Type de blockchain (1/2)	Consentement	Rectification	Récolte de données personnelles	Responsabilités clairement identifiées	Habilitations techniques et droits afférents
Publique	Oui	Non	Non / Partiellement	Non	Oui / Partiellement
Privée	Oui	Oui	Oui / Partiellement	Oui	Oui
Hybride	Oui	Oui / Partiellement	Oui / Partiellement	Oui	Oui

Type de blockchain (2/2)	Durée de conservation limitée	Droit à l'oubli/effacement	Portabilité des données[682]	Accessibilité et ouverture des données
Publique	Non	Non	Oui / Partiellement	Oui
Privée	Oui	Oui	Oui / Partiellement	Non / Partiellement
Hybride	Oui	Oui	Oui / Partiellement	Non / Partiellement

Il convient de préciser quelques remarques concernant le droit de rectification. En théorie, il est informatiquement difficile de modifier ou supprimer de manière stricte un bloc d'une blockchain, car cela violerait son principe d'immuabilité et d'enchaînement cryptographique (des blocs précédemment validés). Toutefois, dans la pratique, il est possible d'ajouter une nouvelle transaction pour corriger une entrée déjà présente, ce qui peut être effectué dans le cadre de contrats intelligents proposant une telle fonctionnalité. Pour rappel, cette fonctionnalité au sein d'un AEC (contrat intelligent, évoqué au chapitre précédent) doit être prévue dès l'initiation du protocole blockchain en question. De même, au regard du

[682] ALIAS, « La portabilité des données : le droit oublié du RGPD, le rapport qui dénonce les ratés du RGPD contre les GAFAM », 2022, in *Global Security Mag Online*, disponible à l'adresse suivante

principe d'un droit à l'oubli/effacement concernant ses données personnelles, la minimisation et le chiffrement de telles données contenues dans une blockchain semblent incontournables en 2022. Pour arriver à une utilisation pratique et conforme au RGPD, un principe de destruction (utilisation temporaire puis destruction) ou de parcellement de la clé de chiffrement reste possible. Ces méthodes rendent respectivement indéchiffrables et illisibles les données à caractère personnel[683]. A ce titre, la CNIL recommande un strict respect du principe de minimisation des données[684], y compris via l'utilisation d'engagement cryptographique. Si ces méthodes de pseudo-anonymisation cryptographiques des données personnelles sont difficiles à mettre en œuvre, une étude d'impact doit néanmoins être réalisée afin d'identifier si les risques sont acceptables. Il est souligné que la blockchain estonienne privée et étatique a partiellement réussi à résoudre la problématique du respect du droit à l'oubli en instaurant une règle spécifique et obligatoire pour toutes les parties impliquées dans la gestion de cette infrastructure. En cas d'ancrage d'une preuve de donnée sur cette chaîne, toute modification de cette transaction doit permettre d'identifier son auteur. Si cette solution ne répond pas strictement aux critères juridiques du droit à l'oubli, y compris au regard des blockchains publiques, elle permet néanmoins d'assurer une forme d'obligation d'information puis de traçabilité stricte pour les gestionnaires des blockchains privées étatiques. Ce principe de transparence accrue pourrait ainsi inspirer certaines blockchains publiques soucieuses de se conformer au moins partiellement à cette règle de droit. En complément du tableau et des parties précédentes, il semble important de compléter et d'insister sur le rôle et la responsabilité de trois acteurs essentiels à toute infrastructure blockchain :

(i) Les ordinateurs, nœuds et validateurs[685] : il s'agit de personnes qui mettent à disposition des ressources informatiques physiques et matérielles pour faire fonctionner un protocole blockchain. Si l'existence de nœuds validateurs est essentielle pour toute blockchain, leur participation au protocole n'implique pas nécessairement de les qualifier de responsables de traitement. En effet, cela est sujet à interprétation, tout particulièrement concernant les blockchains publiques où en l'espèce les validateurs ne font que valider automatiquement et indistinctement des transactions via un ou plusieurs logiciels, dont les règles et responsabilités sous-jacentes ne peuvent pas systématiquement leur être imputées.

(ii) Les développeurs : ces internautes et personnes physiques utilisent leurs compétences techniques singulières de façon généralement assumée ou pseudo-anonyme, parfois anonyme, afin de participer au développement informatique

[683] CNIL, « Premiers éléments d'analyse de la CNIL - Blockchain », *op. cit.*, « lorsqu'un engagement cryptographique est parfaitement indistinguable (perfectly hiding), la suppression du témoin et de la valeur engagée est suffisante pour anonymiser l'engagement de telle façon à ce qu'il perde sa qualification de donné à caractère personnel », note de bas de page 2.
[684] *Ibid.* « Le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».
[685] V. Annexe 6, Focus 1 à 3.

d'une blockchain. Généralement couvert par de multiples licences libres et codes sources ouverts, ces communautés de développeurs représentent l'essence de toute blockchain. Elles recherchent donc à attirer un maximum de développeurs sur leurs protocoles et écosystèmes logiciels afin de s'assurer une pérennité technologique et par extension commerciale (tout en diminuant la centralisation sociale de sa communauté de développeurs, exposée précédemment). Toutefois, plus il y a de développeurs, plus cette gouvernance algorithmique devient complexe et politique. Cela implique souvent des luttes de pouvoirs internes, un constat que la communauté de développeurs Bitcoin expérimente depuis 14 ans[686], la communauté Ethereum depuis 7 ans, et les communautés de blockchains consortium et privées depuis peu.

(iii) Les utilisateurs : il s'agit majoritairement des internautes dont les données à caractère personnel (généralement pseudo-anonymisées[687]) font l'objet d'un traitement informatique par les systèmes blockchains qu'ils utilisent. Chaque internaute est ainsi largement dépendant des deux acteurs précédents pour réaliser des transactions, ce qui explique pourquoi le législateur souhaite protéger les consommateurs avec un encadrement juridique strict de leurs données personnelles.

Par conséquent, si les technologies blockchains prônent une décentralisation des tiers de confiance, il existe souvent un responsable de traitement qui doit respecter certains principes juridiques propres à la collecte, au traitement et à la conservation de données personnelles, tout particulièrement concernant les blockchains fermées et centralisées, comme le confirme un rapport de l'EBSI[688]. S'agissant de la responsabilité afférente aux solutions d'identité numérique décentralisée (IND), étudiée plus loin, un juge pourra tout d'abord rechercher en cas de litige si un régime spécifique de responsabilité s'applique

[686] Bitcoin possède une communauté éprouvée et grandissante comme l'explique sur son blog personnel l'analyste bitcoin et mining Guillaume Girard de la société Galaxy Digital (traduction libre de l'anglais) : « Beaucoup de gens critiquent le maximalisme comme une forme d'extrémisme et de mentalité fermée, mais si la courte histoire de CryptoTwitter nous apprend quelque chose, c'est que pour qu'une communauté d'individus soit inspirée à se lever et à lutter [...], elle doit être unie par des valeurs simples. Lorsque les valeurs fondamentales de Bitcoin ont été attaquées, nous avons eu besoin de maximalistes pour se lever et mener la charge contre un ennemi organisé. […] Cependant, le Maximalisme, sous la forme d'un Ordre extrême, doit rester une mesure d'urgence. [...] J'implore mes collègues Bitcoiners et Ethereans d'être des maximalistes de la decentralization enragée », « A tale of chaos vs order: the ideological war between Bitcoin and Ethereum doesn't need to happen », 2022, consulté à l'adresse suivante. Si ce maximalisme communautaire sur lequel repose Bitcoin est nécessaire à sa stabilité informatique et économique, il est toutefois probable que ce mouvement social soit dilué avec le temps par la majorité tardive de nouveaux entrants non-maximalistes (grand public, entreprises, institutions, Etats, etc.). Pour la blockchain Bitcoin, la complexité réside ainsi dans cette conduite inévitable de ce changement communautaire et social à venir, plutôt que dans la recherche de résilience informatique de ce protocole qui est déjà acquise.

[687] Les techniques d'anonymisation se rapportent aux moyens de transformer des jeux de données - effacement de certains attributs, généralisation, bruitage et autres manipulations - afin de rendre très difficile, voire impossible, la réidentification ou l'inférence de connaissances sur des personnes physiques.

[688] CE, « EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure », pp7- 8, traduit librement de l'anglais, « [les responsables de traitement] doivent prendre toutes les mesures nécessaires pour que les personnes concernées soient suffisamment informées et aient la possibilité d'exercer leurs droits en matière de protection des données », consulté le 23/03/2022 et disponible à l'adresse suivante, *v. supra,* I, Titre 1, 2.2.2.2

à la situation donnée. Si aucun régime spécifique ne s'applique, il identifiera dans un second temps si les conditions d'une responsabilité contractuelle sont réunies, ce qui sera souvent le cas concernant la fourniture ou l'utilisation de solution d'identité décentralisée. Toutefois, si cette dernière est exclue, la responsabilité civile délictuelle pourrait néanmoins être recherchée, en fonction, le cas échéant, du cas d'espèce. Les blockchains publiques sont accessibles à tous les utilisateurs, ce qui signifie que chaque validateur participant au consensus pourrait être considéré comme un responsable de traitement de données en cas de violation de données, de blanchiment d'argent et de financement du terrorisme. Cependant, le raisonnement juridique actuellement utilisé pour identifier les responsables de traitement informatique est insuffisant lorsqu'ils sont appliqués aux validateurs d'une blockchain publique. Par conséquent, une analyse d'impact juridique détaillée doit être effectuée pour chaque blockchain afin d'identifier les véritables responsables de traitement en termes de gouvernance[689], plutôt que de traitement informatique direct.

En dépit de quelques observations et de la perplexité de la doctrine, en partie due à une difficulté d'interprétation juridique des technologies blockchains, la CNIL a émis un avis incontournable quant à l'utilisation d'une technologie blockchain au visa du RGPD. Elle estime en effet que toute technologie blockchain est globalement compatible avec le Règlement. En matière d'identification des responsables du traitement, elle énonce que les acteurs qui possèdent « (…) *un droit d'écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peuvent être considérés comme responsables de traitement* »[690], en précisant qu'un acteur [validateur ou développeur] est une partie prenante responsable de traitement dès lors qu'elle « *détermine les finalités (les objectifs poursuivis par le traitement) et les moyens mis en œuvre (format de la donnée, recours à la technologie Blockchain, etc.)* ». Toujours selon la CNIL, « *il convient de privilégier une Blockchain à permission* [blockchain hybride] *qui permet d'avoir une meilleure maîtrise sur la gouvernance de la donnée personnelle, s'agissant notamment des transferts hors UE* », car « *les règles d'entreprises contraignantes ou les clauses contractuelles types, sont entièrement applicables dans la Blockchain à permission* ». En effet, le comité européen de la protection des données (CEPD) a publié en juin 2021 une série de « protections supplémentaires » ayant conduit la Commission à abroger les anciennes clauses contractuelles (CCT) pour en adopter des nouvelles. La CNIL précise également en propos conclusifs qu'une « *vigilance particulière devrait être portée sur les mesures mises en œuvre pour assurer la confidentialité de la Blockchain si celle-ci n'est pas publique* »[691]. A cet égard, si la majorité des blockchains privées et hybrides ne sont donc pas décentralisées, ces dernières sont par conception conformes au RGPD et, à ce titre, plébiscitées par les acteurs recherchant une conformité légale. D'après le groupe de travail G29 déjà cité, sur la protection des données, la qualité de responsable de traitement au sein d'une technologie

[689] V. Annexe 3 et Annexe 6, Focus 1 à 3.
[690] CNIL, « Premiers éléments d'analyse de la CNIL – Blockchain », *op.cit.*, p.7., consulté en ligne
[691] *Ibid.* p.7.

blockchain peut être acquise ou attribuée dès lors que chaque nœud agit en tant que processeur ou contrôleur de données, c'est-à-dire en participant directement ou par délégation à leur traitement. En outre, le rapport dédié au RGPD d'une blockchain européenne (EBSI) précise « *en cas de contrôle conjoint, les responsables du traitement des données peuvent contractuellement attribuer une responsabilité partielle sur la base d'étapes distinctes du traitement des données* »[692]. Si un accord entre ces responsables du traitement existe et permet de définir chaque responsabilité, alors « *les personnes concernées devront pouvoir exercer leurs droits à l'encontre de chaque responsable conjoint du traitement* » et « *les nœuds qui ajoutent et traitent les données du ledger on-chain* [protocole blockchain principal] *afin de maintenir le consensus seront individuellement qualifiés de responsables conjoints du traitement des données et ce, indépendamment d'une relation contractuelle stipulant le contraire* ».

En se fixant sur l'identité numérique décentralisée, et plus précisément sur l'utilisation d'identifiants numériques décentralisés (DID) qui sont étudiés plus loin, représentant des identifiants numériques au sens de la CNIL, celle-ci « *considère qu'il n'est pas possible de les minimiser davantage* [les identifiants] *et que leurs durées de conservation sont, par essence, alignées sur celles de la durée de vie de la Blockchain* »[693]. Cette considération est aujourd'hui partiellement dépassée, c'est-à-dire qu'il est possible d'utiliser des « *mécanismes d'engagements cryptographiques* » garantissant un haut degré de protection contre toute tentative de réidentification de leurs bénéficiaires. Par conséquent, les identités décentralisées (DID) représentent non seulement des mécanismes d'engagement cryptographique au sens de la CNIL, mais il semble également être en conformité avec le principe de minimisation des identifiants numériques reposant sur une blockchain. À l'échelle internationale, il existe un débat pour déterminer si les identifiants décentralisés, qui ne sont pas encore considérés de manière uniforme comme des données personnelles selon les juridictions, peuvent être stockés tel quel ou bien sous la forme d'un « hash »[694] dans une blockchain. La question de savoir si un hash constitue une donnée personnelle reste controversée et les agences nationales de protection des données ont du mal à définir clairement si le hachage peut être considéré comme un mécanisme suffisant d'anonymisation ou plutôt comme un mécanisme de pseudo-anonymisation. Il est probable que ce débat se poursuive dans les prochaines années. Les contrats intelligents (AEC) évoqués au chapitre précédent entrent également en considération dans l'élaboration d'une solution d'identité décentralisée, notamment concernant la gestion d'identités numériques décentralisées et d'attestations vérifiables qui, pour ces derniers, font l'objet d'une étude détaillée au titre suivant de cette étude. En principe, les mesures appropriées[695] évoquées par la CNIL pour garantir la disponibilité de telles solutions 3.0 en réalité informatiquement

[692] « EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure », *op. cit.*
[693] *Ibid.* p.7.
[694] V. *supra,* Titre I, 2.3.1.1.b
[695] Art. 32 du RGPD : « […] le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris selon les besoins : […] des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ».

hybrides (multiples couches technologiques), impliquent une certaine difficulté de mise en œuvre. Par exemple, un utilisateur devrait pouvoir obtenir une intervention humaine, exprimer son point de vue ou contester une transaction validée après l'exécution d'un contrat intelligent (AEC précité). Autrement dit, une négociation doit être possible. Il convient donc que le responsable de traitement puisse prévoir la possibilité d'une intervention humaine permettant de remettre en cause la transaction effectuée en accordant à la personne concernée le droit de contester la transaction « *même si le contrat a déjà été exécuté, et ceci indépendamment de ce qui est inscrit dans la blockchain* »[696]. Dans les faits, si cela est informatiquement possible à mettre en place pour les blockchains de type privées et hybrides, une telle fonctionnalité s'avère compliquée à implémenter pour les blockchains publiques en raison de la conformité juridique qui n'est pas encore au cœur des préoccupations de ces communautés de développeurs 3.0. En complément de ce qui précède, le Règlement eIDAS révisé (eIDAS-2) étudié dans la deuxième partie de cette étude, imposera une protection accrue des données personnelles. Tout d'abord, cette révision impose un principe d'interdiction de la collecte des données 3.0 issues de l'utilisation des portefeuilles d'identité numérique (PIND) qui sont également étudiés dans la seconde partie de cette étude. Ainsi, le fournisseur d'un PIND ne peut collecter ces données 3.0, excepté si elles sont strictement nécessaires à son fonctionnement (mises à jour). De même, une combinaison limitée des données personnelles est possible par ces PIND, c'est-à-dire que leurs fournisseurs publics (États) et privés (entreprises) ne pourront pas combiner des données d'identification avec des données personnelles provenant d'autres services, excepté si l'utilisateur en fait la demande. Lorsqu'un fournisseur d'une attestation vérifiable est également un fournisseur de service en ligne, les services fournis devront l'être avec des entités juridiques distinctes pour prévenir toute possibilité de corrélation (réidentification) des données personnelles par lesdits services en ligne. Par ailleurs, des mesures organisationnelles doivent permettre de garantir un niveau de sécurité élevé et une notification rapide aux autorités de protection des données en cas de violation des données. Finalement, la mise en œuvre d'une certification ou *marque de confiance* des PIND précités est possible pour chaque État membre, au visa de l'article 42 du RGPD[697]. Notons que ces considérants juridiques, qui ont pour fondement la protection des données à caractère personnel des personnes physiques, sont particulièrement contraignants pour les fournisseurs d'identité et de services en ligne 3.0. En pratique, ces mesures reflètent une volonté de changer de paradigme en ce qui concerne le traitement des données personnelles des personnes, ce qui permet une forme d'optimisme au regard de cette identité numérique de troisième génération.

En matière de responsabilité concernant la gestion d'un PIND, le rapport sur la protection des données au sein de l'infrastructure EBSI[698] constate qu'« *il existe un consensus croissant sur la possibilité pour*

[696] « Premiers éléments d'analyse de la CNIL - Blockchain », *op. cit.*, p.10., consulté en ligne
[697] Art. 42 du RGPD, 2 juillet 2021, disponible à l'adresse suivante
[698] « EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure », *op. cit.* Consulté en ligne le 10 novembre 2021.

les personnes concernées d'être simultanément considérées comme des responsables du traitement des données qui les concernent ». Dès lors, une solution d'identité numérique décentralisée qui tend vers une forme de souveraineté individuelle permettrait aux fournisseurs d'identité numérique de s'exonérer de toute ou partie de leur responsabilité en cas de faute de l'utilisateur dans l'administration de ses données. Ce même rapport recommande que « *les mesures techniques et organisationnelles de préservation de la vie privée du portefeuille et les transmissions de données personnelles devraient garantir que les garanties nécessaires sont en place afin de ne pas limiter l'autonomisation de la personne concernée par le modèle DLT* [blockchain] *choisi* »[699]. Notons que l'article 109 de la loi Informatique et Liberté de 1978, modifiée, permet à toute personne l'exercice d'un droit d'accès, de rectification ou d'opposition sur ses données par voie électronique, dès lors que le responsable du traitement des données les a collectées par ce moyen[700]. Ainsi, les attestations vérifiables permettent de respecter strictement ces règles, notamment grâce à leur caractère révocable et parfois temporaire. Les personnes morales sont visées par le Règlement eIDAS-2 et non, comme déjà exposé précédemment, par le RGPD. En effet, entre l'importante protection des personnes physiques et celle inexistante des personnes morales par le RGPD, l'introduction d'une protection des personnes morales au sein d'eIDAS-2 représente en ce sens une sécurité. En d'autres termes, cela permet d'éviter une forme de concentration disproportionnée des attributs d'identité numérique des personnes morales (chiffre d'affaires, données d'activités) par certains fournisseurs d'identité comme cela est déjà le cas dans certains secteurs industriels 2.0 (bancaires, agricoles[701], pharmaceutiques). Finalement, les données contenues dans une application de portefeuille d'identité numérique décentralisée seront considérées comme des données à caractère personnel et donc soumises au RGPD. Bien qu'il existe une présomption de fiabilité selon laquelle les solutions d'identité décentralisée seraient conformes par conception au RGPD, seules les décisions rendues par les tribunaux et la jurisprudence permettront de confirmer une telle hypothèse sur le fondement d'une évaluation au cas par cas. En attendant, il convient d'éviter l'exposition de données personnelles sur une blockchain publique, par des personnes physiques en n'écrivant pas leurs identifiants numériques, comme le suggèrent déjà certaines solutions d'identité numérique auto-souveraine, étudiée dans la deuxième partie de notre étude. Les technologies blockchains et le RGPD ne sont en principe pas incompatibles comme l'affirment certains juristes[702]. En pratique, l'utilisation d'une technologie blockchain permet de mettre en place une forme de

[699] *Ibid*. p.12.
[700] Les informations mentionnées aux articles 104 à 106 sont fournies par le responsable de traitement à la personne concernée par tout moyen approprié, y compris par voie électronique et, de manière générale, sous la même forme que la demande, disponible à l'adresse suivante
[701] VITARD Alice, « Agdatahub, la plate-forme pour protéger et valoriser les données agricoles françaises », 2020, in *www.usine-digitale.fr*, *v*. le cas d'usage industriel d'une identité décentralisée proposée par IN Groupe et Orange aux agriculteurs français.
[702] DEROULEZ Jérôme, avocat, « Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies », avocat, *«* en dépit d'un mode de fonctionnement parfois antinomique avec les principes du droit à la protection des données, la blockchain apportera peut-être paradoxalement les solutions techniques les plus à même de protéger ces données à l'ère du numérique et de garantir l'effectivité d'un droit parfois mis à mal dans un environnement technologique de plus en plus complexe et transnational », in *Sénat.fr*, consulté en ligne le 05/10/2021.

gouvernance optimisée des données[703], en accord avec les principes du RGPD, sous réserve qu'une attention préalable à ses règles soit accordée aux projets impliquant la technologie blockchain et les solutions d'identité numérique décentralisée. Par le consentement des personnes, leurs droits se trouvent renforcés[704], par exemple via la révocation[705] de leurs attributs numériques possible à tout moment et à leur initiative. La complémentarité de ces outils et technologies 3.0 permet d'assurer une transparence de tout ou partie de la chaîne de valeur d'une identité numérique, à condition que les grands principes de ces technologies et du RGPD soient articulés et respectés dès leur conception. En fin de compte, si le postulat d'une conformité par conception des blockchains fermées est privilégié dans cette étude, il est important de constater que certaines blockchains privées ou hybrides ne se conforment pas toujours aux textes en vigueur, en particulier au droit financier, par exemple lorsqu'une « tokenisation » de ces infrastructures est envisagée. Cela peut se produire lorsque les parties impliquées dans la blockchain décident collectivement de ne pas donner la priorité pour diverses raisons au respect de la loi, en rappelant toutefois que cette situation ne concerne actuellement qu'une minorité de blockchains privées et hybrides.

2.5 Le droit communautaire au service de la politique : Règlements MiCA et TFR

Depuis 2019, le législateur européen adopte une position active et souhaite se positionner comme précurseur en matière de règlementation et d'encadrement juridique des crypto-actifs. L'adoption de ces actifs numériques varie considérablement selon les régions du monde (v. Annexe 14), mais selon une étude menée en 2022 par la Banque centrale européenne[706], environ 10% des Européens détiennent des crypto-actifs. Ces chiffres sont conformes aux estimations de 6% à 8% de Français détenant des cryptomonnaies[707]. La Suisse, considérée comme pionnière dans ce domaine avec ses institutions publiques[708], a rapidement adopté une position innovante et proactive sur le plan juridique. Cela s'explique en partie par leur approche souple de la règlementation de ces technologies 3.0, une stratégie qui porte aujourd'hui ses fruits[709]. D'ici 2030, les crypto-actifs seront probablement réglementés dans

[703] *Op. cit.,* « Premiers éléments d'analyse de la CNIL – Blockchain », 2018, « Outre la minimisation des risques pour la personne, vue précédemment, le format [VC/DID ?] choisi pour inscrire la donnée sur une Blockchain peut permettre de faciliter l'exercice des droits des personnes », p.9, disponible à l'adresse suivante
[704] V. *infra*, II, Titre 1, 2.2
[705] La notion de révocation est essentielle : en cas d'usage abusif d'une ou plusieurs *attestations vérifiables* (*VC*), leur révocation puis renouvellement (avec un nouveau certificat) permet de limiter toute tentative d'usurpation d'identité tout en assurant une continuité (puis confiance afférente) pour l'identité numérique de la personne.
[706] Discours à la BCE, 25 avril 2022, « For a few cryptos more : the Wild West of crypto finance », traduction libre de l'anglais, « Cette offre de crypto-actifs a suscité une forte demande de la part des investisseurs professionnels et du public. En 2021, environ 16 % des Américains et 10 % des Européens », disponible à l'adresse suivante
[707] Les Echos, 24 mai 2022, « Un foyer sur dix en zone euro détient des crypto-actifs », consulté le 20 octobre 2022, à l'adresse suivante
[708] Le droit Suisse est une référence en matière d'adoption des crypto-actifs, tant en matière de règlementations (qualification juridique claire et accompagnement des prestataires de services sur crypto-actifs), que d'incitations fiscales (pour attirer des investisseurs et favoriser l'innovation).
[709] GREGORY Raymond, « Comment la Suisse est devenue la première crypto-nation », 2022, in *Capital*, consulté le 21 octobre 2022, à l'adresse suivante

tous les pays développés, dont les cadres juridiques ruissèlent et influencent généralement les pays en voie de développement dans un second temps. Les 5 et le 10 octobre 2022, le Conseil et le Parlement européen ont statué sur deux règlementations, à savoir le Règlement MiCA[710] et le Règlement TFR[711] qui devraient prendre effet courant 2024. Deux parties spécifiques sont consacrées à l'analyse de ces textes dans leur contexte politique, leur analyse visant à mieux comprendre les conséquences directes de ces règles sur les technologies, applications et écosystèmes 3.0. Le législateur européen estime depuis 2020 qu'il est essentiel d'adopter de nouvelles règles pour offrir un environnement de développement sain et sécurisé à la fois pour les citoyens et les acteurs professionnels du secteur des crypto-actifs. Toutefois, l'application de ces règles nécessite des moyens de supervision appropriés pour garantir leur respect, ce qui n'a été que partiellement le cas à l'échelle nationale depuis 2019[712]. En effet, les prestataires français de services sur actifs numériques sont contraints de respecter un régime d'enregistrement et parfois d'agrément, appelé(s) régime(s) PSAN, visant principalement à écarter les risques d'arnaques, de blanchiment de capitaux et de financement du terrorisme. Ce cadre légal orchestré par l'autorité des marchés financiers (AMF) et l'autorité de contrôle prudentiel et de résolution (ACPR) implique un coût global de mise en conformité conséquent et souvent hors de portée, pour des acteurs aux ressources et à la taille souvent modestes. Parallèlement, certains acteurs étrangers et prestataires de services sur crypto-actifs qui dominent le marché n'ont commencé à se conformer à ses nouvelles règles qu'à partir de 2021, tout en continuant leurs activités à destination du marché national et européen, sans avoir fait l'objet d'un enregistrement PSAN auprès de l'AMF à cette époque. En d'autres termes, cette poignée d'acteurs étrangers a été autorisée à poursuivre des activités non enregistrées bien après d'autres acteurs français confrontés aux obligations de mise en conformité. Le régime juridique actuel, récemment renforcé par la loi DDADUE[713], a permis une libre concurrence entre les acteurs PSAN enregistrés en France, et ceux étrangers non enregistrés mais opérants tout de même illégalement en France pendant plusieurs années pour certains. Il semble aujourd'hui que le régime PSAN n'a pas particulièrement atténué les effets secondaires des récents scandales internationaux relatifs aux crypto-actifs (arnaques, fautes de gestion, défauts de liquidité en chaîne). Après presque cinq années de recul (2019-2023), le législateur national semble en partie responsable de cette situation d'après les acteurs nationaux de cet écosystème représenté par l'association pour le développement des actifs numériques (ADAN), proactive sur le sujet. En réalité, il semble que le législateur ait créé ce régime de règles

[710] Proposition de Règlement du parlement européen et du conseil concernant les marchés des crypto-actifs et modifiant la directive (UE) 2019/1937, disponible à l'adresse suivante, *v.* également la partie dédiée ci-dessous au Règlement MiCA
[711] Proposition de refonte du Règlement (UE) 2015/847 « Transfer of Funds Regulation », disponible à l'adresse suivante, *v.* également la partie dédiée plus loin au Règlement TFR
[712] *Op. cit.* GASSER A, MOULIN J-M, QUINIOU M., et al., « La Finance Numérique – Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs », p. 146, « L'AMF manque de moyens pour faire appliquer le dispositif des *Prestataires de Services sur Actifs Numériques (PSAN)* instauré par la *loi Pacte* en 2019. Le délai minimum pour le traitement d'une demande d'enregistrement PSAN est de six mois, un temps pendant lequel le futur PSAN ne peut pas exercer son activité conformément à ce régime juridique ».
[713] Loi n°2023-171 du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture. JORF 10 mars 2023, v. Cabinet avocats Gide Loyrette Nouel, « Loi DDADUE : renforcement du régime applicable aux futurs PSAN enregistrés », 2023, disponible à l'adresse suivante

spécifiques sans doter les instances concernées (AMF et ACPR) de moyens de contrôle et de vérification suffisants lors de l'entrée en vigeur de la loi PACTE, qui introduit cet enregistrement obligatoire en plus d'un agrément optionnel pour certaines activités relatives aux crypto-actifs (listées dans le CMF). Sans moyens adéquats pour faire appliquer ces règles, une nouvelle règlementation peut se trouver source de perte de compétitivité pour certains acteurs de cet écosystème[714]. Les paragraphes suivants tentent d'expliquer dans quelles mesures ces règles en cours d'adoption ou récemment adoptées par l'UE restent nécessaires face aux atteintes aux libertés individuelles des internautes. Il est exploré comment le concept de neutralité technologique est consacré par ces textes relatifs aux crypto-actifs et à leurs écosystèmes de prestataires, c'est-à-dire principalement concernant les blockchains publiques à vocation financière. Nous constatons que si règlementer les acteurs de ces écosystèmes est essentiel en l'état actuel des technologies et de leurs usages, tenter de les interdire (par des règles de droit et/ou par principe politique) représente un contresens technologique et social, et entraînerait également une contre productivité économique. La règlementation nationale sur les crypto-actifs, elle-même en partie inspirée du droit helvétique[715], a été une source d'inspiration pour le législateur européen pour la création du Règlement MiCA et de la proposition d'amendement du Règlement TFR, bien que certaines considérations d'ordre financier[716] et énergétique (*v.* Annexe 6) semblent conduire à une volonté politique de limiter l'adoption des crypto-actifs. Les deux parties suivantes visent à déterminer si les Règlements MiCA et TFR sont réellement des tentatives institutionnelles dont l'objectif politique serait d'interdire en droit et/ou en pratique certains protocoles informatiques ou prestataires de ces écosystèmes 3.0, jugés trop complexes à règlementer en raison de leur importante décentralisation (*v.* Annexe 7). Dans ses premières versions, le Règlement MiCA avait pour objectif politique de limiter considérablement l'exploitation et l'utilisation des crypto-actifs les plus décentralisés (émission, achat et vente, détention et transferts), allant parfois jusqu'à proposer de les interdire. Le législateur européen s'est finalement orienté vers l'adoption de règles plus précises, incitatives et juridiquement perçues comme étant proportionnelles, tout en faisant bénéficier le marché commun de plus d'une année d'adaptation entre l'adoption et l'entrée en application de ces textes. Ce long laps de temps permettra ainsi la préparation d'un second texte « MiCA-2 » et d'autres textes relatifs à la DeFi, aux NFT ou encore au minage de crypto-actifs[717]. Sans doute, l'adoption de cette constellation de Règlements et textes aura des impacts significatifs sur l'évolution du marché des technologies blockchains, et tout particulièrement pour ses applications financières et juridiques. Pourtant, il semble qu'il s'agit de ne pas favoriser les

[714] Sauf pour les acteurs les plus importants, qui sont principalement des entités étrangères disposant des ressources nécessaires pour se conformer aux règles le plus tardivement possible - souvent à travers de longues négociations politiques pour éviter les sanctions - les règles déjà en vigueur sont soit appliquées de façon minimale, soit contournées pour éviter les sanctions.
[715] LANGLOIS-BERTHELOT Thibault, BOUILLET-CORDONNIER Ghislaine, « Tour d'horizon du droit financier Suisse : Crowdfunding - ICO – STO », in *Albatross Legal*, pp16, disponible en ligne
[716] FLEURET Faustine, 2 mai 2022, « Règlementation kaMICAze en Europe ? », « Depuis des années, perdurent une croyance importante [persiste chez le législateur européen] que les actifs numériques représentent un véhicule préféré de blanchiment et de financement du terrorisme, alors même que de récentes études démontrent le contraire », in *Grand Angle Crypto*, YouTube, 2022, disponible à l'adresse suivante
[717] V. Annexe 6, Focus 1.

amalgames avec des discours politiques reposant sur la lutte contre le blanchiment et le financement du terrorisme, et le caractère énergivore de certaines blockchains[718], afin de ne pas entraver certaines libertés comme l'innovation et l'entrepreneuriat, au risque d'engendrer une perte de droits fondamentaux voire une fuite massive à l'étranger des talents et des capitaux.

2.5.1 Proposition du Règlement Markets in Crypto-Assets (MiCA)

Issu d'une série de mesures relatives au paquet législatif sur la finance numérique en Europe ou « *Digital finance package* »[719], le Règlement européen sur les marchés de crypto-actifs ou « *Markets in Crypto-Assets – MiCA* » a été présenté le 24 septembre 2020 par la Commission européenne[720]. Il s'inscrit dans une volonté plus large et européenne de soutien politique concernant la technologie blockchain[721]. Ses neuf titres visent à encadrer les crypto-actifs en créant un cadre règlementaire européen qui favorise le développement technologique tout en assurant la stabilité financière et la protection des consommateurs au sein de l'UE. Si certains pays membres de l'UE possèdent déjà un cadre national encadrant les crypto-actifs, MiCA a vocation à se substituer à ces derniers, y compris concernant le régime français encadrant les offres au public de jetons (« ICO ») ainsi que les prestataires de services sur actifs numériques PSAN[722] précités. Si certaines règles sont destinées à s'appliquer sans difficulté en droit interne, d'autres nécessiteront des adaptations au regard de ce nouveau dispositif d'application stricte. L'objectif du Règlement MiCA est d'encadrer à l'échelle de l'UE les prestataires de services sur crypto-actifs[723], y compris pour des segments spécifiques et non régulés de ce marché (certains jetons non fongibles et crypto-actifs stables[724]). Pour cela, il s'agit d'enregistrer tous les acteurs de cet écosystème et ce quel que soit le pays de l'UE visé d'où ces derniers opèrent. Cela implique de catégoriser chaque type d'actif et d'acteur associé, dans un cadre juridique harmonisé en termes de protection des consommateurs et de concurrence européenne[725]. Ainsi, l'ambition de ce Règlement peut être résumée en plusieurs objectifs :

---

[718] FLEURET Faustine, *op. cit.*, « Il y a encore beaucoup d'institutions qui pensent que la crypto est un véhicule préféré pour le blanchiment et le terrorisme ; pour l'écologie c'est le même constat », in *Grand Angle Crypto*, YouTube, 2022 à l'adresse suivante

[719] European Council. « Digital finance package: Council reaches agreement on MiCA and DORA », 2021, disponible à l'adresse suivante

[720] *Op. cit.*, « Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets amending Directive (EU) 2019/1937 COM/2020/593 ». MiCA fait partie du « Digital Finance Package » qui entend transformer l'économie européenne au cours des prochaines décennies. Disponible à l'adresse suivante

[721] *Ibid.* Traduction libre de l'anglais : « cette initiative est étroitement liée à des politiques plus larges de la Commission concernant la technologie de la chaîne de blocs, étant donné que les crypto-actifs, en tant que principale application de cette technologie, sont inextricablement liés à la promotion de la technologie de la chaîne de blocs dans toute l'Europe. La présente proposition soutient une approche globale de la chaîne de blocs et de la DLT, qui vise à placer l'Europe à l'avant-garde en ce qui concerne l'adoption des chaînes de blocs et l'innovation en la matière ».

[722] *Op. cit.*, BOUILLET-CORDONNIER Ghislaine et al., « La Finance Numérique, aspects juridiques et fiscaux du crowdfunding et des cryptoactifs », *op. cit.*, p.146.

[723] *Op. cit.* MiCA, art. 3.1. (8) : « prestataire de services sur crypto-actifs : toute personne dont l'occupation ou l'activité consiste à fournir un ou plusieurs services sur crypto-actifs à des tiers à titre professionnel ».

[724] V. *supra*, II, Titre 2, 2.4

[725] Mise en place d'une obligation d'un seuil minimum de fonds propres pour ces plateformes, de requis techniques et de transparence et contrôle de leur gouvernance. Ces règles impliquent des ressources coûteuses et recentralise progressivement les écosystèmes des blockchains publiques, ce qui est à la fois souhaitable sur le plan légal, et néfaste sur le plan informatique.

harmoniser les législations nationales au profit d'une approche communautaire au sujet de ces actifs[726], assurer une sécurité juridique, assurer la protection des consommateurs, prévenir la fraude et garantir la stabilité financière au sein de l'UE. En pratique, le Règlement MiCA prévoit un agrément obligatoire pour les prestataires de services sur crypto-actifs (PSCA) pour « *Crypto-Asset Service Providers – CASP* » en anglais. Ses exigences sont proches de l'agrément optionnel du régime PSAN français mentionné précédemment. Grâce à ce nouveau Règlement qui s'inspire donc des régimes juridiques helvétique et français, les PSCA agréés bénéficieront d'un « *passeport européen* »[727] leur permettant de fournir et d'opérer leurs services dans tous les pays de l'UE et non plus de se conformer obligatoirement à chaque législation nationale (ce qui est actuellement complexe et coûteux pour les plateformes/bourses de crypto-actifs). A ce titre, ils auront besoin en France d'une autorisation délivrée par les autorités nationales compétentes (l'AMF) dans un délai de trois mois, afin d'exercer librement leurs activités au sein de l'UE grâce à ce passeport normatif. Pour assurer une traçabilité et une transparence de ces acteurs 3.0, un registre public[728] des PSCA enregistrés auprès de l'Autorité européenne des marchés financiers (AEMF)[729] sera disponible sur Internet. MiCA introduit d'autres mesures comme le fait que les crypto-actifs des clients devront être séparés des fonds appartenant au PSCA et protégés en cas d'insolvabilité. Parallèlement, ces acteurs feront l'objet d'une transmission régulière d'informations entre les autorités compétentes, notamment l'autorité bancaire européenne (ABE) qui sera responsable de la tenue d'un registre public des PSCA non conformes avec les propositions du GAFI en matière de risques de blanchiment de capitaux et de financement du terrorisme[730]. A ce sujet, nous soulignons que ces échanges d'informations sensibles et inter-organisations entre de multiples instances nationales, communautaires ou internationales peuvent recourir à des solutions d'identité numérique décentralisée (IND), étudiée plus loin, afin de garantir la confidentialité et l'intégrité des données échangées. De même, les émetteurs de jetons[731] peuvent utiliser ces mécanismes d'identité numérique 3.0 en vertu de leur obligation de disposer d'un « *solide mécanisme de contrôle interne et d'évaluation des risques,*

[726] *Op. cit.* MiCA, (Contexte de la proposition) : « si [avant l'adoption de MiCA] certains crypto-actifs peuvent entrer dans le champ d'application de la législation de l'Union, il n'est pas toujours simple de leur appliquer cette législation dans les faits », disponible à l'adresse suivante

[727] Gide Loyrette Nouel, avocats, « Agreement reached on European crypto-assets regulation (MiCA) under the aegis of the french presidency of the European Union », in *gide.com*, 1er juillet 2021, disponible à l'adresse suivante

[728] *Op. cit.* Proposition du Règlement 2019/1937 (MiCA). Art. 57 : « L'AEMF tient un registre de tous les prestataires de services sur crypto-actifs. Ce registre est accessible au public sur le site web de l'AEMF et mis à jour régulièrement, *v.* également considérant (53) : Afin de favoriser la transparence pour les détenteurs de crypto-actifs en ce qui concerne la prestation de services sur crypto-actifs, il y a lieu pour l'AEMF de constituer un registre des prestataires de services sur crypto-actifs, lequel devrait contenir des informations sur les entités agréées pour fournir ces services dans l'ensemble de l'Union. Ce registre devrait également inclure les livres blancs notifiés aux autorités compétentes et publiés par les émetteurs de crypto-actifs », disponible à l'adresse suivante

[729] L'Autorité Européenne des Marchés Financiers, créée en 2011, est une autorité indépendante de l'UE qui vise à améliorer la protection des investisseurs et à promouvoir la stabilité et le bon fonctionnement des marchés financiers, v. le site internet european-union.europa.eu (ESMA en anglais).

[730] A cet égard, il est souligné que le PSCA dont la société mère est située dans des pays figurant sur la liste de l'UE des pays tiers considérés comme étant à haut risque en matière d'activités de lutte contre le blanchiment de capitaux ou encore sur la liste des juridictions fiscalement non coopératives, seront tenus de mettre en œuvre des garanties et contrôles renforcés.

[731] *Op. cit.*, MiCA, art. 3, 1. (6) « émetteur de crypto-actifs : une personne morale qui offre au public tout type de crypto-actifs ou demande l'admission de ces crypto-actifs sur une plate-forme de négociation de crypto-actifs ».

ainsi que d'un système propre à garantir l'intégrité et la confidentialité des informations reçues. »[732]. A ce propos, nous suggérons que l'identité décentralisée devienne la règle cryptographique pour répondre à ces nouvelles contraintes institutionnelles et commerciales qu'impose le Règlement MiCA. En effet, appliquer une identité numérique 2.0 à ces échanges d'informations hautement sensibles et à une échelle industrielle peut poser des problèmes d'ordre informatique (risque connu de fuite massive des données), et également d'ordre géopolitique (souveraineté numérique non respectée si ces échanges de données s'effectuent via des identités numériques de type fédérées qui dépendent des GAFAM/BHATX comme nous l'avons évoqué). En matière de sanctions, MiCA prévoit dans son article 92 que les autorités compétentes de chaque pays puissent conformément à leur pouvoir de surveillance, sanctionner toutes infractions. Il est prévu à cet égard de lourdes sanctions pécuniaires, entre 500 000 et 700 000 euros d'amendes en cas du non-respect de ses dispositions. Pour les personnes morales, les sanctions peuvent être fixées entre 5 et 15 millions d'euros et/ou 5 à 15% du chiffre d'affaires annuel total consolidé de la personne morale concernée.

Le 14 mars 2022 est une date symbolique pour l'écosystème européen des crypto-actifs, et par extension pour tous les écosystèmes adjacents du Web 3.0. Cette date est en effet le jour du rejet in extrémis par des députés européens de certaines propositions d'amendements alarmants relatives à la version initiale de la proposition de Règlement MiCA[733]. Ces propositions d'insertion d'articles antérieures au sein de ce projet de Règlement étaient avancées par certains membres et députés européens de la Commission des affaires économiques et monétaires du Parlement européen. L'une d'elles, peu pragmatique, suggérait que seuls les crypto-actifs respectant des « *normes minimales de durabilité environnementale* » puissent être émis, proposés ou admis à la négociation au sein de l'Union européenne[734]. Avec cette disposition, il aurait été exigé que certaines infrastructures de crypto-actifs déjà émis et accessibles au public comme bitcoin[735] depuis 2009 et l'ether[736] depuis 2015, mettent en place et maintiennent un plan de déploiement progressif[737] afin de garantir le respect de certaines exigences environnementales minimales. Si cela avait été possible pour la blockchain Ethereum et son écosystème en réalité semi-décentralisé (en référence à sa fondation)[738], le degré de décentralisation pure de Bitcoin et de son mécanisme de la Preuve de travail (« *Proof of Work - PoW* »)[739], étudié en Annexe

[732] *Ibid*. Considérant (34).
[733] European Parliament News, , « Econ Voting Sessions 14 March 2022 », 24 voix pour et 32 voix contre, disponible à l'adresse suivante
[734] Art *2a* et *(5aa)* de la version rejetée, accessible en ligne à l'adresse suivante
[735] Mempool - Bitcoin Explorer, consulté le 24 octobre 2022. Consultez le premier bloc de la blockchain bitcoin à l'adresse suivante
[736] Le lancement de la blockchain Ethereum se constate à la création et validation de son premier bloc : « Blocks #0 », disponible sur Etherscan à l'adresse suivante
[737] Il s'agissait concrètement de publier des PDF (Livre Blanc) expliquant comment ladite blockchain compte réduire ses émissions de CO2 (une documentation que Bitcoin ne peut pas produire en l'état actuel de son fonctionnement et de sa communauté).
[738] V. Annexe 7 & Annexe 6, Focus 2.
[739] V. Annexe 5.

6 (Focus 1), n'aurait pas pu satisfaire de telles exigences légales. Finalement rejetée[740], l'adoption de cette proposition aurait de facto conduit à une interdiction partielle, voire totale, du minage et de l'acquisition et de la conservation de bitcoins ou d'ethers. La motivation de cette proposition venait du fait que le mécanisme de la Preuve de travail consommerait inutilement trop d'énergie, un postulat partiellement inexact comme cela est démontré au cours de cette étude[741]. D'autres tentatives d'ordre politique visant à restreindre l'industrie du minage de bitcoins se feront probablement jour au motif d'une consommation d'énergie perçue comme étant disproportionnée pour cette industrie, bien que seulement 0,04% de l'électricité consommée en Europe en 2022 provienne en réalité du minage de bitcoins[742]. Une interdiction de ce mécanisme informatique historique et spécifique à la première blockchain en date, mettrait probablement fin à une partie significative de l'écosystème blockchain européen qui se déplacerait donc probablement dans des pays dotés de juridictions plus favorables. Toujours d'après l'Annexe 6 de cette étude, il semble que depuis plusieurs années déjà, l'industrie manufacturière du minage, spécifique à certaines blockchains publiques étudiées en Annexes, se mobilise pour améliorer leurs empreintes énergétiques respectives. D'ici quelques années, chaque mécanisme et fonctionnement informatique de blockchains ouvertes et/ou fermées sera désormais analysé dans une « *taxonomie verte européenne* »[743], incitant ainsi les acteurs concernés à améliorer leur empreinte énergétique par l'utilisation d'énergies renouvelables, sans pour autant les interdire comme plusieurs scientifiques le proposaient dans une tribune commune en juin 2022[744]. A ce titre, il est souligné que cette tentative d'interdiction ne concerne pas seulement la consommation énergétique de Bitcoin, mais également son utilité sociale, car les deux sont en réalité indissociables comme l'évoquait dès 2010 Satoshi Nakamoto en réponse à une critique similaire sur un blog[745]. En fin de compte, la version actuelle du Règlement MiCA est le résultat de compromis entre la Commission européenne et le Parlement européen qui avait l'intention d'inclure les crypto-actifs dans la taxonomie européenne pour une finance durable. Si le bon sens a finalement gagné une majorité des députés européens en éliminer l'interdiction initialement envisagée du mécanisme de la Preuve de travail, cela ne suffit pas à dissiper les préoccupations concernant les PSCA et leur nouvelle obligation d'information environnementale.

[740] À la suite du vote le lundi 14 mars 2021 de la Commission des Affaires Economiques et Monétaires (ECON) sur le texte de compromis final du Parlement européen, le texte ne sera pas contesté en plénière.
[741] *Ibid*.
[742] STACHTCHENKO Alexandre, « C'est donc 0,04% de la production électrique […] européenne [que consommerait Bitcoin] », 2022, disponible sur Twitter, *v*. également Annexe 6, Focus 1.
[743] FLEURET Faustine, « Régulation et innovation dans le domaine des cryptoactifs - Table ronde », disponible sur videos.senat.fr
[744] Institut Rousseau et al, tribune de chercheurs qui estiment qu'« Il est urgent d'agir face au développement du marché des cryptoactifs et de séparer le bon grain de l'ivraie […] ne pas autoriser les cryptoactifs dont l'impact sur l'environnement est inutilement nocif », consulté le 1 juin 2022, à l'adresse suivante
[745] NAKAMOTO Satoshi, « Bitcoin minting is thermodynamically perverse », 7 août 2010, traduction libre de l'anglais « C'est la même situation que pour l'or et l'extraction de l'or. Le coût marginal de l'extraction de l'or tend à rester proche du prix de l'or. L'extraction de l'or est un gaspillage, mais ce gaspillage est bien moindre que l'utilité de disposer d'or comme moyen d'échange. Je pense que le cas sera le même pour le bitcoin. L'utilité des échanges rendus possibles par le bitcoin dépassera de loin le coût de l'électricité utilisée. Par conséquent, ne pas avoir de bitcoin serait un gaspillage net. », accessible en ligne à l'adresse suivante

Ces préoccupations persistent jusqu'à la publication des projets de normes techniques règlementaires[746] que l'ABE et l'AEMF doivent élaborer dans un avenir proche. En outre, il est remarqué que l'obligation d'information environnementale imposée aux PSCA ne s'applique pas aux acteurs et institutions financières traditionnels, une obligation incombant seulement aux PSCA[747]. Outre les nouvelles règles précitées, le Règlement MiCA introduit des régimes ad hoc pour (i) les jetons non fongibles (NFT/JNF), et (ii) les crypto-actifs stables (« *stablecoin* »)[748].

(i) En principe, les jetons numériques qui sont uniques et non interchangeables, c'est-à-dire non fongibles (JNF), sont exemptés du champ d'application de MiCA d'après ses annexes (notamment pour les NFT dits artistiques ou de collection qui en sont exclus). En pratique, les superviseurs nationaux (AMF, ACPR) pourraient requalifier au cas par cas certains types de JNF si leurs caractéristiques ou utilisations s'apparentent à la qualification d'instruments financiers ou de crypto-actifs au sens du présent Règlement. En d'autres termes, la non-fongibilité d'un NFT peut être remise en question et requalifiée lorsqu'il est émis en grande quantité à destination du public ou lorsqu'il peut être fractionné.

(ii) Face à l'utilisation progressive de crypto-actifs dont la valeur est stable ou « *jetons de monnaie électronique* » au sens de MiCA[749], plus communément désignés par le terme de « *stablecoins* »[750], MiCA distingue (a) les « *jetons se référant à des actifs* », (b) des « *jetons de monnaie électronique* »[751]. Il encadre tout d'abord les

[746] European Parliament, « News Cryptocurrencies in the EU: deal struck between Parliament and Council », 30 juin 2022. Disponible à l'adresse suivante, (5a), p.8, traduction libre de l'anglais, « les mécanismes de consensus utilisés pour la validation des transactions en crypto-actifs pourraient avoir des impacts négatifs principaux sur le climat et d'autres impacts liés à l'environnement. Ces mécanismes de consensus devraient donc déployer des solutions plus respectueuses de l'environnement et veiller à ce que tout impact négatif principal qu'ils pourraient avoir sur le climat et tout autre impact négatif lié à l'environnement soit identifié et divulgué de manière adéquate par les émetteurs et les fournisseurs de services de crypto-actifs. Pour déterminer si les effets négatifs sont principaux, il convient de tenir compte du principe de proportionnalité ainsi que de la taille et du volume des crypto-actifs émis. L'AEMF, en coopération avec l'ABE, devrait donc être chargées d'élaborer des projets de normes techniques réglementaires afin de préciser davantage le contenu, les méthodologies et la présentation des informations relatives aux indicateurs de durabilité en ce qui concerne les effets négatifs liés au climat et à l'environnement, et de définir les principaux indicateurs énergétiques ».

[747] *Op. Cit.*, « les CASP doivent mettre à la disposition du public, dans un endroit bien visible de leur site web, des informations sur leur impact environnemental et climatique ». Si ces exigences pouvaient en théorie être respectées par la blockchain Ethereum et sa Fondation, la blockchain Bitcoin ne pourrait pas, car aucune 'Fondation Bitcoin' ou tiers de confiance ne l'administre significativement.

[748] V. *infra*, II, Titre 2, 2.4

[749] *Op. cit.*, MiCA, Art. 3, 1. (4), « 'jeton de monnaie électronique' : un type de crypto-actif dont l'objet principal est d'être utilisé comme moyen d'échange et qui vise à conserver une valeur stable en se référant à la valeur d'une monnaie fiat qui a cours légal ».

[750] CARRIER Anna, « Member States continue MiCA review », 2020, in *Regulation Tomorrow*, disponible à l'adresse suivante, art. 3, traduction libre de l'anglais, « les crypto-actifs principalement destinés à servir de moyens d'échange et censés conserver une valeur stable par référence à d'autres formes de capital. ». Notons que « La Commission s'abstient expressément d'utiliser le terme 'stablecoins', considérant qu'il s'agit d'un 'concept marketing' plutôt que d'un terme reflétant précisément la nature des crypto-actifs en question. », *v. infra*, II, Titre 2, 2.4

[751] *Op. cit.*, art. 3 et 1. Contexte de la proposition, 3. 4. Incidence budgétaire : « jeton se référant à un ou des actifs : un type de crypto-actif qui vise à conserver une valeur stable en se référant à la valeur de plusieurs monnaies fiat qui ont cours légal, à une ou plusieurs matières premières ou à un ou plusieurs crypto-actifs, ou à une combinaison de tels actifs ; jeton de monnaie électronique : un type de crypto-actif dont l'objet principal est d'être utilisé comme moyen d'échange et qui vise à conserver une valeur stable en se référant à la valeur d'une monnaie fiat qui a cours légal », disponible à l'adresse suivante

stablecoins qui revêtent une « *importance significative* », c'est-à-dire ceux largement accessibles et à destination du public. Ainsi, il semble à ce jour qu'une majorité des stablecoins du marché (USDT, Tether)[752] entrent dans cette seconde catégorie au sens du Règlement. MiCA impose à cet égard des plafonds d'émission ainsi que certaines conditions non exhaustives pour l'émission de ces deux typologies de crypto-actifs stables[753]. Certaines règles standard comprennent l'obligation de notifier par le biais d'un livre blanc (« White paper ») le projet d'émission d'un stablecoin à l'ABE, la nécessité d'être domicilié légalement dans l'Union européenne afin de soumettre tous les acteurs étrangers aux règles communautaires et l'exigence de constituer des réserves importantes pour prévenir tout risque d'insolvabilité. Toutefois, ces règles ne sont pas valables pour les quelques « *stablecoins algorithmiques* »[754], dont le degré de décentralisation informatique est élevé grâce à l'utilisation puis à l'imbrication de contrats intelligents. Toutefois, le législateur européen ne reconnaissant pas ce caractère partiellement décentralisé, ces stablecoins algorithmiques ne bénéficient pas des exemptions en outre octroyées aux solutions de la Finance Décentralisée (DeFi) et pour partie aux NFT non significatifs. En fin de compte, l'émetteur d'un stablecoin sera tenu de rembourser à tout moment et gratuitement tout utilisateur conformément aux dispositions MiCA. L'ABE peut à cet égard sanctionner les émetteurs de jetons se référant à des actifs revêtant une importance significative[755] avec des amendes et/ou astreintes en cas de non-respect de certaines dispositions (*v.* Annexe V du présent Règlement).

Le 30 juin 2022, la phase de consultation, de négociation et de discussion ayant duré plus de deux ans a pris fin pour cette proposition d'adoption du Règlement MiCA[756]. Sa publication au JOUE est attendue en milieu d'année 2023 pour une entrée en application 15 à 18 mois plus tard, c'est-à-dire entre

[752] CoinMarketCap, « Top Stablecoin Tokens by Market Capitalization », consulté le 24 octobre 2022. Consultez la liste en temps réel des *jetons stables* disponibles sur le marché des crypto-actifs à l'adresse suivante
[753] V. *infra*, II, Titre 2, 2.4
[754] CANT Tim, RICE Bradley, « 10 things you need to know about MiCA: Europe's proposals for regulating crypto assets ». 2020, in *www.ashurst.Com*, traduit de l'anglais, « les 'stablecoins algorithmiques' ne doivent pas être considérés comme des 'jetons de monnaie électronique', bien qu'ils puissent être soumis aux exigences applicables aux cryptoactifs de manière plus générale. Les stablecoins algorithmiques sont désignées comme ceux qui visent à maintenir une valeur stable, via des protocoles, qui prévoient l'augmentation ou la diminution de l'offre de ces cryptoactifs en réponse aux changements de la demande. », disponible en ligne, *v.* également Partie II, Titre 2, 2.4
[755] *Ibid.* MiCA. Titre III, chapitre 5, art. 39, traduction libre de l'anglais, « les critères que l'ABE doit appliquer pour déterminer si un jeton se référant à des actifs est d'importance significative. Ces critères sont les suivants : la taille de la clientèle des promoteurs de jetons se référant à des actifs, la valeur de ces jetons ou de leur capitalisation boursière, le nombre et la valeur des transactions, la taille de la réserve d'actifs, l'importance des activités transfrontières des émetteurs et l'interconnexion avec le système financier. L'article 39 habilite également la Commission à adopter un acte délégué afin de préciser les circonstances dans lesquelles et les seuils au-delà desquels un émetteur de jetons se référant à des actifs sera considéré comme d'importance significative. ».
[756] European Parliament News, « Cryptocurrencies in the EU: deal struck between Parliament and Council », 2022, disponible en ligne à l'adresse suivante

septembre et décembre 2024. Il est à noter qu'une période transitoire supplémentaire de 18 mois est octroyée aux acteurs qui ont déjà obtenu un enregistrement ou un agrément PSAN, leur permettant ainsi de continuer à fournir leurs services au public français en attendant d'obtenir l'agrément et le passeport européen de « PSCA » mentionné au visa de MiCA. Finalement, avec ce Règlement, l'Union européenne deviendra pionnière dans la mise en place d'un cadre règlementaire complet dédié aux crypto-actifs et à leurs écosystèmes de prestataires. MiCA ouvre également la voie à de nombreux autres textes en cours de rédaction visant les cas d'application susvisés des technologies 3.0[757]. Il est en effet prévu une clause de révision du Règlement aux fins d'envisager si de nouvelles dispositions complémentaires[758] étaient nécessaires, ce qui serait bienvenu compte tenu du contexte précédemment exposé. Comme avec le RGPD, ces règles établissent des normes européennes et essaimeront probablement de nombreuses règlementations internationales. Si la rédaction puis les amendements du Règlement MiCA ont été confrontés à plusieurs tentatives politiques de déstabilisation économique et juridique des acteurs de la crypto-économie, son adoption finale fournira indéniablement un socle de confiance pour les consommateurs ainsi que pour les acteurs de ces écosystèmes. Néanmoins après son entrée en vigueur, l'une des conséquences de ce Règlement concerne la mise en place d'innombrables échanges d'informations multilatérales entre les plateformes d'échange et les institutions de contrôle nationales ou internationales. Le transit de ces informations comporte un risque de fuite de données, car il n'est pas prévu d'audit indépendant des systèmes de sécurité informatique de chaque PSCA. Seule leur responsabilité est invoquée, ce qui est insuffisant, car tous les prestataires ne disposent pas de niveaux de sécurité informatique équivalents selon la culture informatique de chaque État membre comme mentionné dans les parties précédentes. Par conséquent, c'est ici que l'identité numérique décentralisée[759] semble incontournable pour répondre à ces obligations de transmission d'informations prévues également par le Règlement TFR en matière de LCB-FT[760].

2.5.2 Amendement du Règlement Transfer of Fund Regulation (TFR)

D'après certains juristes et acteurs du secteur des crypto-actifs[761], une seconde tentative d'encadrement juridique relativement excessif de ce secteur est identifié en parallèle du Règlement MiCA, car issue de motivations politiques similaires à celles mentionnées précédemment. Le *paquet anti-blanchiment*[762] de

[757] Une seconde version de MiCA, surnommée « *MiCA-2* », encadrera les *NFT* ainsi que la *Finance décentralisée* (*DeFi*).
[758] *Ibid.* MiCA. 5. Autres éléments. Disponible à l'adresse suivante, Il est important de noter que la Commission peut adopter des actes délégués afin de préciser certains éléments techniques des définitions et d'adapter ces dernières aux évolutions du marché et de la technologie.
[759] V. *infra*, II, Titre I, Chap. 1
[760] V, partie suivante.
[761] *Ibid.* FLEURET Faustine, Grand Angle Crypto, « Réglementation kaMICAze en Europe ? », 2022, « Les derniers débats [MiCa et TFR concernant la lutte contre la PoW] sont assez inquiétants », disponible à l'adresse suivante,
[762] CE, Anti-money laundering and countering the financing of terrorism legislative package. Consulté le 26 octobre 2022, à l'adresse suivante

la Commission européenne comprend une révision du Règlement sur les transferts de fonds (« *Transfer of Funds – TFR* »)[763] qui étend aux PSCA l'obligation traditionnelle des institutions financières d'accompagner les transferts de fonds et d'informations sur les bénéficiaires effectifs de fonds en crypto-actifs. Le 31 avril 2022 certaines propositions d'amendements (article 15[764] et article 16[765]) de ce Règlement ont été adoptées. Le TFR s'appliquera dès l'application de MiCA, c'est-à-dire dans les mêmes délais à compter de sa publication au JOUE. Certains de ces nouveaux articles relatifs aux PSCA et aux crypto-actifs sont étudiés dans cette partie. Le 20 juillet 2021[766], la Commission a adopté un paquet législatif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), comprenant une proposition de révision du Règlement 2015/847/UE[767] relatif aux informations accompagnant les virements de fonds y compris avec des crypto-actifs. Depuis 2021, Interpol[768], ainsi que la Commission européenne avec la présente proposition d'amendement de ce Règlement[769], estime que le pseudo-anonymat et la portée mondiale des crypto-actifs entraînent des risques d'utilisation à des fins criminelles comme mentionné précédemment. Le cadre règlementaire européen visant à prévenir le blanchiment d'argent et le financement du terrorisme, qui englobe maintenant les crypto-actifs, repose sur plusieurs recommandations datant de 2012 (n°15[770] et 16[771])[772] proposées et mises à jour par le groupe d'action financière (GAFI). Cette « *Règle de Voyage* [de fonds] »[773] concerne des informations minimales obligatoires qui doivent accompagner un transfert financier, ici en crypto-actifs. Ces

[763] Cette proposition prend comme point de départ et modifie le règlement existant (UE) 2015/847 du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) nº1781/2006, tel que modifié par le règlement (UE) 2019/2175 du 18 décembre 2019.V. Proposition de règlement du parlement européen et du conseil sur les informations accompagnant les transferts de fonds et de certains crypto-actifs (refonte), accessible à l'adresse suivante

[764] Relatif aux PSCA bénéficiaires et les nouvelles obligations de vigilance pour tout bénéficiaire de crypto-actifs.

[765] Relatif aux PSCA émetteurs d'actifs et enregistrés (MiCA), sur lesquels pèsent de nouvelles obligations renforcées de collecte d'informations lorsqu'ils envoient des fonds à destination de *portefeuilles d'actifs numériques non hébergés*, voir les pages suivantes. *Op. cit.* Selon une étude du 24 mars 2023, 80% des détenteurs de crypto-actifs les hébergent et les stockent au sein d'une plateforme et chez un tiers de confiance et seulement 30% les détiennent cryptographiquement sur un ou plusieurs portefeuilles non hébergés. in *CoinGeco*, « Where People Store Their Crypto, Post-FTX Collapse », 2023, disponible à l'adresse suivante

[766] CE, Press corner, 2021, consulté le 5 avril 2022, à l'adresse suivante

[767] Règlement (UE) 2015/847 du 20 mai 2015 sur les informations accompagnant les transferts de fonds (TFR) et abrogeant le Règlement (CE) n°1781/2006.

[768] EUROPL, « Europol's Internet Organised Crime Threat Assessment », p.15, accessible à l'adresse suivante

[769] *Op. cit*., TFR, Exposé des motifs, 1. Contexte de la proposition, « Étant donné que les transferts d'actifs virtuels s'accompagnent de risques de blanchiment de capitaux et de financement du terrorisme similaires à ceux entourant les transferts de fonds électroniques, c'est à des exigences de même nature qu'il convient de les soumettre, et il semble donc logique d'utiliser un même instrument législatif pour régler ces problèmes qui leur sont communs ».

[770] CE, Note interprétative de la recommandation nº 15 du GAFI : « Les pays devraient s'assurer que les [PSCA] émetteurs obtiennent et détiennent les informations requises et exactes sur le donneur d'ordre ainsi que les informations requises sur le bénéficiaire pour les transferts d'actifs virtuels, soumettent les informations ci-dessus au [PSCA] ou à l'institution financière du bénéficiaire (le cas échéant) immédiatement et de manière sécurisée, et les mettent, sur demande, à la disposition des autorités appropriées » et que « les [PSCA] bénéficiaires obtiennent et détiennent les informations requises sur le donneur d'ordre ainsi que les informations requises et exactes sur le bénéficiaire pour les transferts d'actifs virtuels, et les mettent, sur demande, à la disposition des autorités appropriées. », disponible à l'adresse suivante

[771] FATF, Recommendation 16 du GAFI, 2021, « updated guidance for a risk-based approach - virtual assets and virtual asset service providers ». p.58, disponible à l'adresse suivante

[772] *Ibid*. Recommandations du GAFI (« FATF » en anglais).

[773] *Op. cit*., TFR, 3. Résultats des évaluations ex post, des consultations des parties intéressées et des analyses d'impact, TFR, art. 4, disponible à l'adresse suivante, « les transferts de fonds pour lesquels le prestataire de services de paiement du bénéficiaire de fonds est établi en dehors de l'Union, dont le montant n'excède pas 1 000 EUR et qui ne semblent pas liés à d'autres transferts de fonds dont le montant, cumulé avec celui du transfert en question, excède 1 000 EUR, sont au moins accompagnés des informations suivantes: a) les noms du donneur d'ordre et du bénéficiaire de fonds; et b) les numéros de compte de paiement du donneur d'ordre et du bénéficiaire de fonds ou l'identifiant de transaction unique ».

transactions sont réalisées entre des portefeuilles virtuels[774] contenant des crypto-actifs, étant désignés comme appartenant à des PSCA (personnes morales) ou à des particuliers (personnes physiques)[775]. Cette Règle de Voyage consacre ce principe d'identification obligatoire des bénéficiaires de crypto-actifs, dès lors qu'il s'agit d'un transfert crypto-financier d'un montant supérieur à 1000 euros[776]. En pratique, cela signifie que certaines informations obligatoires (nom, prénom, adresse, identifiant unique) du bénéficiaire effectif des fonds seront systématiquement associées à ce type de transactions cryptographiques. L'élargissement de cette recommandation vise à permettre le partage d'informations entre d'une part les PSCA soumis au régime de LCB-FT, et d'autre part lesdits bénéficiaires de transactions en crypto-actifs. A l'origine, bien que cette recommandation proposée par le GAFI ne présente pas de caractère obligatoire puisque le GAFI émet des recommandations sans caractère coercitif, force est de constater que de nombreux pays développés, dont la France, transposent systématiquement en droit interne ces recommandations pour une application stricte par l'AMF ou l'ACPR.

Pour recontextualiser, le 9 février 2022, deux Commissions de la politique économique de l'UE (LIBE et ECON)[777] composées de deux factions du Parlement européen (Les Verts[778] et les Conservateurs et Réformistes européens[779]) présentent un projet de règlementation visant à lutter contre le blanchiment d'argent et le financement du terrorisme aux moyens de crypto-actifs. Ce projet d'amendement suit l'avis officiel et déterminant du GAFI. Dans sa version consolidée par un vote de ces comités, il vise à appliquer une « *Règle de Voyage renforcée* »[780], initialement pensée comme un outil de traçabilité et de contrôle efficace pour des systèmes informatiques et sociaux centralisés, ceux des institutions financières. La transposition de cette Règle de Voyage à des écosystèmes et technologies décentralisées semble inadaptée comme le suggèrent les propos suivants. En réalité, les deux propositions initiales à savoir la Règle de Voyage renforcée précitée et la réduction du seuil de tolérance (ci-après) visaient à aligner la crypto-économie sur les mêmes normes que les réseaux financiers traditionnels, tel que SWIFT. En principe, cette règle serait donc applicable pour chaque crypto-transfert d'un montant supérieur à 1 000 euros[781], les PSCA étant tenues d'informer les autorités compétentes afin d'enregistrer ces informations d'identification minimales considérées comme indispensables pour la LCB-FT. Il est

[774] V. *infra*, II, Titre 1, 1.3.1.3
[775] *Op. cit.*, TFR, voir les considérants et définitions (12) à (20) : « 'adresse de portefeuille', un numéro de compte dont la conservation est assurée par un prestataire de services sur crypto-actifs ou un code alphanumérique relatif à un portefeuille sur une chaîne de blocs » ; « 'transfert de crypto-actifs entre particuliers', une transaction entre personnes physiques agissant, en tant que consommateurs, à des fins autres que commerciales ou professionnelles, sans recours à un prestataire de services sur crypto-actifs ou à une autre entité assujettie ni intervention de l'un ou de l'autre », etc.
[776] *Op. cit.*, TFR, art. 5.
[777] Le 25 novembre, le dossier a été assigné conjointement à LIBE et ECON, Ernest Urtasun étant le rapporteur pour la Commission ECON et Assita Kanko pour la Commission LIBE.
[778] Wikipedia contributors. « Groupe des Verts/Alliance libre européenne », 2022, disponible à l'adresse suivante
[779] Wikipedia contributors. « Conservateurs et réformistes européens », 2022, disponible à l'adresse suivante
[780] Dont les modifications spécifiquement applicables aux crypto-actifs sont plus strictes que celles qui concernant le secteur bancaire et financier.
[781] Art. 4 et 5 du Règlement TFR, disponible à l'adresse suivante

souligné que le 31 mars 2022[782], la Commission de l'UE, souhaitant aller au-delà de ce seuil de tolérance de 1000 euros en dessous duquel le GAFI estime qu'une exonération d'identification est possible, a tenté de renforcer cette identification en essayant de le supprimer. Si cette tentative manifestement disproportionnée avait été un succès, cela aurait entraîné la collecte et la vérification d'innombrables données personnelles pour chaque transfert de crypto-actifs réalisé au sein de l'UE, dès un euro. Ainsi, cette même Commission souhaitait instaurer l'identification de tous les portefeuilles de crypto-actifs non hébergés[783] (indispensables pour tout transfert P2P)[784], une obligation également disproportionnée aux objectifs de LCB-FT poursuivis, puisque non visée dans les recommandations du GAFI. En dernier ressort, cette tentative de contrainte d'identification de chaque transfert P2P entre des particuliers (cas sans PSCA), a été rejetée, toujours grâce aux efforts des acteurs du lobby 3.0 mené par l'association pour le dévelopement des actifs numériques (ADAN). Selon Stéphane Berger, l'un des membres du Parlement européen et rapporteur du Règlement MiCA : « *mettre en application les* (…) *règles* [susvisées] *du TRF serait comme demander un passeport pour un paiement de 20€ en cash lors d'un achat au Supermarché* »[785]. En effet, en amont du vote du Parlement européen pour confirmer ces amendements, de nombreux acteurs (re)connus de cet écosystème[786] ont interpellé dans une lettre ouverte en avril 2022 les gouvernements européens[787] concernant les risques de telles propositions, tandis que certains acteurs français ont plus radicalement annoncé qu'ils quittaient le territoire national face à cette seconde tentative de restriction politico-juridique ciblant leur secteur et leurs activités[788].

Finalement, l'identification obligatoire et renforcée dès le premier euro de transfert a été abrogée puis substituée par un autre amendement dont l'effectivité juridique et informatique est sujette à

[782] Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, voir notamment les amendement 68 sur l'art. 18 bis, 15 sur l'art. 27 ter et 52 sur l'art. 14 et 5, disponibles à l'adresse suivante

[783] Un *portefeuille non hébergé de crypt-oactifs*, également appelé « *unhosted wallet* » ou « *cold wallet* » en anglais, permet à un utilisateur de maintenir seul un solde de crypto-actifs en dehors de tout tiers de confiance (plateformes d'échanges, dits « *portefeuilles hébergés* », « *hosted wallet* » ou « *hot wallet* »), grâce à sa propre clé cryptographique privée, comme s'il avait des billets de banque dans son propre portefeuille. Selon une étude du 24 mars 2023, 80% des détenteurs de crypto-actifs les hébergent et les stockent chez une plateforme et un tiers de confiance et seulement 30% les détiennent cryptographiquement sur un ou plusieurs portefeuilles non hébergés, *op.cit.*, « Where People Store Their Crypto, Post-FTX Collapse », 2023, disponible à l'adresse suivante

[784] V, *supra*, I, Titre 1, 2.3.1.1.c

[785] BERGER Stephan, « EU Parliament's MiCA Rapporteur, talks about crypto regulation in the EU », 2022, in *Cryptolaw* [Vidéo]. YouTube

[786] Créée en 2019, l'ADAN est une association professionnelle qui fédère les acteurs du secteur des crypto-actifs et de la blockchain pour imposer la France et l'Europe comme des innovateurs dans cet espace. Notons que l'ADAN a joué un rôle essentiel dans la définition en France des divers cadres règlementaires dédiés aux crypto-actifs. Son positionnement d'association professionnelle permet entre autres de former le législateur aux nombreuses innovations et enjeux de l'écosystème des crypto-actifs.

[787] RAYMOND Gregory, « Exclusif MiCA : l'industrie crypto interpelle les gouvernements européens », 2022, in *www.thebigwhale.io*. Consulté le 3 mai 2022, à l'adresse suivante

[788] PLANCADE Jean, « Durcissement régulatoire dans l'UE - L'exode de la crypto européenne vers la Suisse s'accélère », 2022, in *Bilan*, disponible à l'adresse suivante. Parmi eux, l'entrepreneur Sébastien Gouspillou, président de la société *BigBlock Datacenter*, qui annonce poursuivre sa levée de fonds de 200 millions de dollars dans le canton Suisse de Neuchâtel, au détriment de la France.

interprétation[789]. Si en principe, tout transfert inférieur à 1000 euros n'oblige donc pas un PSCA à identifier le bénéficiaire effectif de fonds comme mentionné, cela est sans compter l'exception qui infirme cette règle, c'est-à-dire lorsque de multiples transactions de faibles montants sont réalisées et dont le cumul total dépasse ce montant de 1000 euros (ce qui déclenche l'obligation d'identification). En effet, ce montant et plafond déclenche une identification au plus tard en trois jours, par les PSCA concernés. Ce montant de 1000€ est extrêmement faible lorsque rapporté au montant médium de 5000€ détenus par les crypto-investisseurs français d'après un sondage de 2021 « *la valeur médiane du portefeuille crypto se situe autour de 5.000 euros, si 29% des sondés gèrent entre 5.000 et 25.000 euros, ils sont 6,4% à gérer plus de 100.000 euros* »[790]. Dès lors, cette exemption d'identification en deçà de 1000€ ne concernera pas à moyen terme la majorité des utilisateurs de crypto-actifs qui pourraient détenir des montants supérieurs à l'avenir. Ce constat semble ainsi écarter l'écosystème des crypto-actifs et ses utilisateurs de leur volonté initiale d'utiliser un cash électronique[791] pair à pair et respectueux de leur vie privée. A titre de comparaison, les espèces n'imposent pas de telles obligations d'identification, aussi strictes et automatisées. Parce que la temporalité de ce seuil de 1000 euros n'est pas définie dans le Règlement TFR, cela signifie que tous les internautes qui posséderont plus de 1000 euros en crypto-actifs seront nécessairement identifiés et leurs fonds surveillés, un principe ayant pour effet à long terme une recentralisation des crypto-actifs qui seront alors censurables au moindre soupçon de non-conformité (avéré ou non). Pour certains observateurs et spécialistes engagés dans cet écosystème 3.0, juristes y compris, cela risque d'introduire une forme de surveillance active et généralisée qui pourrait être contraire à la libre circulation des flux financiers au sein de l'UE[792]. Concernant la possibilité de disposer en toute autonomie d'un portefeuille de crypto-actifs non hébergé[793], cela est toujours considéré par beaucoup d'utilisateurs comme le moyen le plus sûr de les stocker et les détenir cryptographiquement, en comparaison aux solutions centralisées dépendantes de PSCA, régulièrement en proie à des attaques informatiques ciblées ou à des escroqueries massives. A cet égard, il est soutenu qu'empêcher ou à freîner l'utilisation de ces portefeuilles crypto-monétaire (P2P et non hébergés) revient à empêcher ou freiner certaines libertés associées aux crypto-actifs (liberté de propriété

[789] *Op. cit.*, TFR, Section 2, art. 7, 4. « Pour les transferts de fonds dont le montant n'excède pas 1 000 EUR et qui ne semblent pas liés à d'autres transferts de fonds dont le montant, cumulé avec celui du transfert en question, excède 1 000 EUR, le prestataire de services de paiement du bénéficiaire de fonds n'est pas tenu de vérifier l'exactitude des informations sur le bénéficiaire de fonds ».

[790] ARMANDET Pauline, « Les crypto-investisseurs français sont presque exclusivement des hommes », 2022, in *agefi.fr*

[791] *Op. cit.* « Bitcoin: A Peer-to-Peer Electronic Cash System », disponible à l'adresse suivante

[792] Parlement européen, « La libre circulation des capitaux », Fiches thématiques sur l'Union européenne, « Toutes les restrictions aux mouvements de capitaux entre les États membres et entre les États membres et les pays tiers doivent être levées, sauf circonstances exceptionnelles. La libre circulation des capitaux est la pierre angulaire du marché unique et complète les trois autres libertés. Elle contribue également à la croissance économique [...] », 2021, consulté en ligne

[793] Pour quelques centaines d'euros il est par exemple possible de mettre en place son propre système de gestion et de stockage de ses cryto-actifs, directement chez soi. Pour plus d'informations, consultez la solution de la société « Umbrel ». *Op. cit.* Selon une étude du 24 mars 2023, 80% des détenteurs de crypto-actifs les hébergent et les stockent chez une plateforme et un tiers de confiance et seulement 30% les détiennent cryptographiquement sur un ou plusieurs portefeuilles non hébergés. Disponible à l'adresse suivante

cryptographique[794], liberté de communication[795], liberté de circulation des capitaux). La nouvelle version du Règlement TFR aura donc pour effet d'identifier massivement tous les utilisateurs de crypto-actifs, tout en favorisant l'utilisation de portefeuilles hébergés chez des PSCA, que l'histoire de ce secteur démontre comme moins sécurisés pour les utilisateurs les moins avertis. Cet effet juridique informatiquement indésirable forme ainsi un paradoxe au détriment des bénéficiaires effectifs de crypto-actifs[796]. En complément des propos précédents, l'ADAN a identifié puis insisté plusieurs dangers qu'il convient de souligner concernant les impacts des présentes propositions d'amendements du Règlement TFR :

(i) Dangers concernant la protection des données personnelles, de la vie privée des personnes et de la souveraineté numérique européenne. La *Règle de Voyage* doit en principe respecter un équilibre entre une LCB-FT[797] essentielle, et une protection de la vie privée des utilisateurs de crypto-actifs, dont la majorité est de bonne foi (peu de transactions impliquent en réalité des signes de blanchiment de capitaux d'après des sociétés spécialisées qui collaborent avec Interpol[798]). Dès lors, il est primordial que les PSCA se conforment au RGPD et ne transfèrent des informations sur leurs utilisateurs que si la protection de ces données est assurée, ce qui ouvre - comme pour MiCA - le champ au marché de l'identité décentralisée pour répondre avec efficience à cette nouvelle exigence[799] que certains PSCA estiment à juste titre complexe à mettre en œuvre. Jusqu'à présent, les PSCA n'ont pas encore mis en place de solutions techniques répondant aux exigences du TFR concernant l'accompagnement des transferts de données personnelles. Pour remédier à ce manque, l'utilisation de solutions d'identité décentralisée est recommandée pour garantir une identification fiable et éviter certains risques liés à la non-conformité du RGPD, aux vols de données personnelles, aux usurpations d'identité, entre autres. Bien que ces solutions 3.0 soient particulièrement adaptées aux contraintes imposées par ces propositions

[794] V, *infra*, II, Titre 1, 2.2.6
[795] V, *infra*, II, Titre 1, 2.2, *v*. également Annexe 3, Focus 6.
[796] Même si un utilisateur est protégé en cas de perte de ses actifs en raison de la négligence d'un prestataire de services de conservation d'actifs (PSCA), il est souvent difficile et laborieux de prouver cette négligence, comme l'illustre l'affaire de la plateforme Mt. Gox (PSCA) qui a duré plus de sept ans devant les tribunaux. V. ICHBIAH Daniel, « Les victimes du piratage de Mt. Gox dédommagés 7 ans après la disparition de leurs Bitcoins », 2021, in *Futura-sciences.com*, disponible à l'adresse suivante
[797] CE. Parlement européen, « Crypto-actifs : de nouvelles règles pour stopper les flux illicites dans l'UE », 2022, consulté à l'adresse suivante
[798] La société *Chainalysis* leader et spécialisée dans la lutte contre le blanchiment de capitaux a constaté que seulement 0,15% des transactions en crypto-monnaies en 2021 comportaient un élément de criminalité, « Le blanchiment d'argent n'a représenté que 0,05 % du volume total des transactions en crypto-monnaies en 2021 », « The 2022 Crypto Crime Report », 2022, in *chainalysis.com*, p.5.
[799] *Op. cit*., TFR, « La mise en œuvre de la 'règle de voyage' introduit […], de nouvelles exigences spécifiques qui les obligent [PSCA] à obtenir, conserver et partager les informations requises et exactes sur les utilisateurs de transferts d'actifs virtuels et à les mettre à disposition à la demande des autorités concernées. De telles obligations soulèvent diverses difficultés techniques, du fait de la nécessité pour les prestataires de services sur actifs virtuels de mettre au point des solutions technologiques et des protocoles permettant de recueillir et de partager ces informations aussi bien entre eux qu'avec les autorités compétentes. […] il s'agit de l'introduction de nouvelles normes internationales du GAFI qui doivent être appliquées simultanément dans plusieurs pays dans le monde […] », disponible à l'adresse suivante

d'amendements, il est important de s'assurer que leur implémentation informatique ne soit pas dépendante d'acteurs étrangers, mais plutôt européens.

(ii) Risques concernant la compétitivité économique européenne. En matière de souveraineté économique, il peut être risqué de mandater des acteurs étrangers, notamment des plateformes dont le siège social n'est pas situé au sein de l'UE, afin de transmettre automatiquement des informations d'identité civile aussi sensibles et à forte valeur ajoutée (comme cela est déjà le cas pour la majorité des réseaux sociaux qui sont Chinois ou Américains comme précédemment constaté). A ce titre, un PSCA étranger – souvent soumis à une législation moins contraignante - pourrait exploiter ces données dans son propre intérêt stratégique ou économique, c'est pourquoi il est préconisé un chiffrement de bout en bout grâce aux standards informatiques de l'identité décentralisée. Comme l'appréhendent certains PSCA[800], leur compétitivité pourrait être réduite face à l'obligation d'implémenter cette exigence de règle de voyage renforcée concernant les mouvements de fonds en crypto-actifs. La compétition pour attirer les acteurs internationaux s'intensifie, comme en témoigne une annonce récente du gouvernement britannique visant à instaurer une règlementation souple et avantageuse pour ces acteurs[801], à l'instar des États-Unis[802].

En définitive, à la lumière des articles 263 et 264 du TFUE[803], et des articles 7 et 8 concernant la libre circulation des capitaux protégée par la Charte des droits fondamentaux de l'UE[804], il convient de se poser la question suivante : les atteintes à ces libertés fondamentales sont-elles proportionnées et justifiées aux simples motifs de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme ? La collecte de données personnelles des bénéficiaires de fonds en crypto-actifs pourrait demeurer déclarative et réalisée au cas par cas, et non pas reposer sur un principe de soupçon généralisé certes plus efficace, mais partiellement disproportionné voire liberticide face à l'objectif poursuivi (créant d'une part des institutions « *pots de miel* » pour les pirates informatiques, et d'autre part, contribuant à une forme de surveillance de masse des contribuables[805]). En réalité, il s'agit pour le législateur de trouver un véritable équilibre entre les procédures LCB/FT et certains droits fondamentaux

[800] *Ibid.* « certains représentants des prestataires de services sur actifs virtuels dans l'Union européenne 27 ont affirmé que l'absence de solution technique globale normalisée, libre et gratuite, pour la règle de voyage pourrait entraîner l'exclusion des petits acteurs du marché des cryptoactifs, seuls les grands acteurs du marché ayant les moyens de se conformer aux règles. ».
[801] HM Treasury, « Government sets out plan to make UK a global cryptoasset technology hub », in *GOV.UK*, consulté le 4 avril 2022, à l'adresse suivante
[802] The White House, « Fact sheet: President Biden to sign executive order on ensuring responsible development of digital assets », 2022, consulté le 12 avril 2022, à l'adresse suivante
[803] Art. 263 du Traité sur le fonctionnement de l'UE (aussi appelé Traité de Rome) : « La Cour de justice de l'UE contrôle la légalité des actes législatifs, des actes du Conseil, de la Commission et des actes du Parlement européen destinés à produire des effets juridiques à l'égard des tiers (…) » et v. art. 264 « Si le recours est fondé, la Cour de justice de l'Union européenne déclare nul et non avenu l'acte contesté (…) ».
[804] Art. 7 du Traité sur le fonctionnement de l'UE : « Toute personne a droit au respect de sa vie privée et familiale et de ses communications », *v.* également art. 8 « Toute personne a droit à la protection des données à caractère personnel la concernant ».
[805] SEZNEC Erwan, « Comment Bercy a tenté d'accéder à nos données bancaires », 28 septembre 2022, in *Le Point*, disponible en ligne

(protection des données personnelles des utilisateurs et droit au respect de leur vie privée), un processus complexe lorsque lobby politique et manque de connaissances techniques et commerciales se côtoient. En pratique, les crypto-actifs sont un vecteur peu efficace et non privilégié pour blanchir les fruits d'activités illégales. En effet, il existe une trace permanente de chaque transaction sur ces blockchains publiques dont l'analyse et le suivi sont à ce jour quotidiennement effectués par des sociétés spécialisées. En 2022, selon le rapport « Chainanalysis Crypto Crime Report »[806], la part des activités illicites dans le volume des transactions en crypto-actifs n'a jamais été aussi faible (elle ne représente qu'environ 0,15 % de toutes les transactions identifiées). Dès lors, avec l'augmentation de ces outils d'analyse des blockchains publiques et du nombre d'enquêteurs, les criminels écartent progressivement ce vecteur pour opacifier l'origine illicite de leurs fonds. Notons que selon Europol, environ 1 % du produit intérieur brut annuel de l'UE est identifié comme étant impliqué dans une activité financière suspecte, les crypto-actifs ne représentant donc qu'une fraction infime de ce chiffre (~0,15%), démontrant ainsi la questionnable proportionnalité de cette Règle de Voyage renforcée imposée par l'amendement prochain du Règlement TFR.

2.6 La blockchain et l'identité décentralisée au regard de la propriété intellectuelle

La diffusion du progrès et des savoirs est l'un des fondements du développement de la propriété intellectuelle comme le soulignent plusieurs chercheurs de l'Institut Mines-Telecom « *les objectifs de protection de la propriété intellectuelle* (…) *consistent à accorder un monopole temporaire à l'inventeur pour l'exploitation industrielle et commerciale de son invention en échange duquel l'inventeur est tenu de dévoiler les principes de son invention, favorisant ainsi la diffusion des savoirs techniques dans le tissu industriel* »[807]. Dans cette partie, les technologies blockchains ainsi que les solutions d'identité décentralisée, étudiées dans la seconde partie de cette étude, sont principalement appréhendées sous l'angle de la propriété intellectuelle et du droit des marques, des brevets et du droit d'auteur sur les logiciels[808]. Le tableau suivant propose d'introduire et d'identifier les relations entre la notion de propriété intellectuelle (PI) en droit et celle d'application 3.0 (usages) en informatique :

[806] Chainalysis, « Crypto Crime Report », *op. cit.*, disponible à l'adresse suivante
[807] VALERIAN François, COMBY Gérard, KAPPELMANN Alexia, GIMON Magali, et al. « Annales des mines n°18 sur les enjeux numériques : propriété et gouvernance du numérique », série trimestrielle - N°18 - Juin 2022, Institut Mines-Télécom, p.72, disponible à l'adresse suivante
[808] Un logiciel peut être défini comme un ensemble de programmes destinés à effectuer un traitement particulier sur un ordinateur. Un logiciel est protégé par le droit d'auteur au visa de l'article L.112-2 du Code de la propriété intellectuelle qui vise : « (…) 13° Les logiciels, y compris le matériel de conception préparatoire (…) ».

La PI s'applique-t-elle aux technologies 3.0 ?		
Droit des marques	Droit des brevets (Logiciels)	Droit d'auteur (Logiciels et autres)
Oui	Oui	Oui

Le droit d'auteur sur les logiciels trouve son origine dans la protection nécessaire des nouvelles technologies et de leurs besoins concurrentiels et commerciaux. Avec l'avènement de la technologie blockchain et de son innovation constante, notamment en matière d'identité numérique décentralisée, de nouvelles possibilités techniques émergent, créant ainsi de nouvelles opportunités sociales, mais également des défis d'ordre juridique. En 2020, le contexte international est tel que la Chine et les États-Unis étaient en tête de la répartition par pays des 100 premières entreprises dans le monde déposant des demandes de brevets relatifs aux technologies blockchains[809]. La France ne figure pas dans ce classement, peut-être en raison d'une visibilité ou de contraintes règlementaires initialement moins accommodantes pour innover par rapport à d'autres juridictions, comme étudié précédemment. Notons toutefois que les dispositifs du crédit impôt recherche (CIR) et le crédit d'impôt pour la compétitivité et l'emploi (CICE) des entreprises dont bénéficie un très grand nombre d'entre elles du secteur en France, tend à nuancer ce constat. Comme mentionné précédemment, l'écosystème des crypto-actifs et de la technologie blockchain a été initialement créée de manière ouverte et transparente, avec des programmes informatiques « open source »[810], car développés par des communautés de développeurs. Appréhender un service décentralisé pose la question du titulaire des droits de propriété intellectuelle, et l'étendue de ces droits inhérents à ces nouveaux écosystèmes (brevets, marques ou droits d'auteur). Les logiciels sont majoritairement protégés par les droits d'auteurs attachés aux programmes informatiques, car ces derniers sont créés et maintenus par des personnes physiques opérant dans le cadre du Web 3.0 et de son périmètre conceptuel contenant de multiples briques technologiques (AEC, DAO, protocoles blockchains, etc.). La propriété intellectuelle trouve ici application, tandis que les tiers de confiance qui interagissent avec ces derniers disposent d'une licence d'utilisation étendue, généralement fournie par défaut par des sites tels que GitHub, hébergeant une grande partie de ces programmes informatiques[811]. En matière de droits d'auteur, la technologie blockchain présente de nombreux avantages, comme la facilitation de la preuve d'acquisition de droits antérieurs, la divulgation ou l'horodatage d'œuvres ou encore de preuves numériques[812]. La traçabilité et l'intégrité supposément offertes par une blockchain permettent de retracer chaque étape du processus de création d'une œuvre littéraire ou artistique, ce qui

[809] Statista, « Global blockchain patents major applicants ; country distribution 2020 », consulté le 7 mars 2022, à l'adresse suivante
[810] V, *infra*, II, Titre 1, 1.5.3.1
[811] Plateforme disponible à l'adresse suivante
[812] V. *infra*, Partie I, Titre 2, 2.8

est particulièrement pertinent en cas de collaborations multiples, notamment pour les régimes de co-auteurs[813]. Dans ce contexte, l'utilisation d'une blockchain publique peut offrir des micro-paiements proportionnels à la cession de certains droits patrimoniaux associés à une œuvre, telle qu'une œuvre musicale, à la fois pour l'auteur et pour le bénéficiaire de l'œuvre. En août 2022, la Commission européenne a annoncé qu'elle développera un système qui utilisera la blockchain et les contrats intelligents[814]. L'Office de l'Union européenne pour la propriété intellectuelle « World Intellectual Property Organization - WIPO » prévoit de développer un système permettant aux détenteurs de propriété intellectuelle de créer des AEC adossés à des produits afin de prouver leur authenticité. Pour utiliser ce système de suivi sur la blockchain, les détenteurs d'éléments de propriété intellectuelle devront être préalablement enregistrés en tant que signataires approuvés. L'Office européen de la propriété intellectuelle vise à disposer d'un système opérationnel d'ici la fin 2023. Pourtant, la technologie blockchain n'empêche pas certaines infractions courantes et avérées[815] comme la contrefaçon ou la copie de logiciel sans respecter le droit moral de ses auteurs et développeurs. Ainsi, il est envisageable que l'adoption croissante de ces applications, souvent à la fois centralisées et décentralisées (DAO, DeFi, AEC), entraîne inévitablement des litiges concernant la violation de droits de propriété intellectuelle. De plus, si les protocoles des blockchains sont open source[816], certains services sur crypto-actifs développés par des prestataires et entreprises demeurent néanmoins la propriété exclusive et fermée de ces entités commerciales. En conséquence, il est possible de constater que si les blockchains publiques sont open source depuis leur conception et accès jusqu'à leur (ré)utilisation, leurs écosystèmes sociaux deviennent progressivement moins ouverts[817], comme pour les blockchains hybrides et surtout privées, étudiées précédemment. En particulier, les blockchains publiques liées à des solutions d'identité numérique auto-souveraine (INAS)[818] peuvent être à l'avenir source d'inquiétudes et de complexité, notamment en raison de la publicité et de l'imuabilité de leurs transactions numériques. En effet, des violations de droits d'auteurs, de licences de marque, de brevets ou encore de dessins et modèles fleurissent d'ores et déjà pour les applications les plus décentralisées de ces technologies. Par exemple, de nombreuses applications blockchains prônent une décentralisation de bout en bout, c'est-à-dire l'incapacité pour un tiers de revendiquer un droit sur les informations déployées par ces dernières. Cela est notamment le cas du service « Ethereum Name Service - ENS »[819] qui propose la fourniture de noms de domaine décentralisés, car reliés à des portefeuilles de crypto-

[813] Art. L.113-3 du Code de la propriété intellectuelle, dans sa version en vigueur depuis le 3 juillet 1992, dispose : « L'œuvre de collaboration est la propriété commune des coauteurs. Les coauteurs doivent exercer leurs droits d'un commun accord. En cas de désaccord, il appartient à la juriddiction civile de statuer (…) ».
[814] WIPO (contributions prepared by the European Union and the Tencent Group), « Advisory Committee on Enforcement – fifteenth session - new technologies in ip enforcement », WIPO/ACE/15/10, 2022, disponible à l'adresse suivante, *v.* également *supra*, Partie I, Titre 1, 2.3.1.1.d
[815] MALONEY Conor, « Researchers Allege Tron Plagiarized Code from other Crypto Projects », 2022, in *Yahoo Finance*, disponible à l'adresse suivante
[816] V. *infra*, II, Titre 1, 1.5.3.1
[817] V. Annexe 7 et Annexe 6, Focus 3.
[818] V. *infra*, II, Titre 1, 2.2.1
[819] Pour plus d'informations consultez le service de création et gestion de *noms de domaine – supposés - décentralisés* à l'adresse suivante

actifs (pour faciliter l'identification et les crypto-paiements entre des sites internet et leurs propriétaires). Si en théorie, le fonctionnement de ces noms de domaine est décentralisé, il s'avère dans les faits que plusieurs de ses composantes techniques et légales demeurent centralisées[820]. Cependant, le fait que certains protocoles soient tout de même partiellement décentralisés engendre des complications de nature administrative et informatique concernant l'identification des personnes morales et physiques responsables, ce qui rend parfois impossible toute poursuite judiciaire. Il est possible de constater en navigant sur l'application ENS mentionnée[821] que cette dernière a permis à un utilisateur (anonyme) d'enregistrer le nom de domaine « *banquedefrance.eth* », très probablement sans l'autorisation de cette institution (en tant que titulaire de la marque « Banque de France » déposée auprès de l'INPI). C'est ici probablement un cas de contrefaçon (certes sans utilisation commerciale à ce jour), parmi de nombreux autres encore ignorés en raison de la modeste taille de ce service (~800 000 ENS enregistrés en 2022).

Par ailleurs, il convient de noter que la règlementation des PSCA en vertu des Règlements MiCA et TFR, étudiés en amont, pourrait par voie de conséquence réduire le nombre de violations de ces droits de propriété intellectuelle. Cela s'explique par le fait que ces infractions seront liées à des crypto-actifs dont les propriétaires seront identifiés, ce qui facilitera ainsi l'identification des responsables en cas d'utilisation d'un PSCA pour faire transiter – en contrefacteur - ces noms de domaine et leurs fonds associés. Il convient de distinguer les composantes de propriété intellectuelle préexistantes de celles nouvellement générées dans le cadre d'une application décentralisée. Cette première distinction doit s'effectuer au regard du degré de décentralisation de chaque application 3.0. La responsabilité de l'intégration de logiciels libres ou de tiers doit également être prise en considération aux prémices de toute activité de développement. A cet égard, cette étude suggère qu'au sein des blockchains privées et hybrides, il est communément admis que la propriété intellectuelle soit contractuellement encadrée préalablement à tout développement informatique[822]. Ainsi, deux considérations et certains compromis sont nécessaires au sein de ces consortiums d'acteurs :

(i) Le régime d'indivision (au sens du Code civil) est en principe à proscrire en raison de la nature constamment évolutive des développements logiciels réalisés au sein de ces consortiums 3.0.

(ii) Le régime de co-propriété au sein duquel tout membre du consortium possède des connaissances et des droits antérieurs est à privilégier, chaque membre étant libre de fournir ou non certaines briques technologiques au consortium et de bénéficier de licences d'utilisation le cas échéant.

[820] Notamment par le biais d'une fondation immatriculée aux îles Caïmans ou encore par le biais d'une organisation décentralisée (DAO) dont la gestion et répartition des jetons numériques dédiés (nommés « ENS ») demeurent sous l'influence de ladite fondation et ses propriétaires.
[821] Pour consulter cette probable contrefaçon de marque en ligne, visiter l'adresse suivante consultée le 28/08/2021.
[822] Un logiciel, même standard, est une œuvre de l'esprit qui, si elle est originale, accède à la protection par le droit d'auteur (reproduction, utilisation, adaptation, représentation). L'exploitation d'un logiciel peut prendre plusieurs formes selon certains types de contrats de licence pour son exploitation.

En fin de compte, il apparaît que la technologie blockchain et plus largement les briques technologiques du Web 3.0 qui la composent, s'intègre sans opposition au(x) cadre(s) juridique(s) des droits de propriété intellectuelle, certes au bénéfice des développeurs de ces solutions informatiques 3.0, mais qui demeurent paradoxalement en constante évolution, et parfois particulièrement ouvertes et décentralisées, c'est-à-dire défiant partiellement le droit de la propriété intellectuelle.

2.7 Les métiers du droit au regard des technologies décentralisées

Les juristes représentent une « *caste sociale et intellectuelle* »[823] de la même façon que les technophiles, comme les crypto-anarchistes, possèdent la leur[824]. Internet et ses multiples technologies, anciennes comme récentes, n'échappent donc pas à ce principe social et communautaire auquel les juristes se confrontent progressivement dans l'univers numérique. Les technologies décentralisées ont un impact croissant sur le monde du droit et les métiers qui y sont liés, tout particulièrement au regard de l'adoption des crypto-actifs. Entre 2016 et 2021 régnait une forme d'inquiétude chez de nombreux juristes (avocats, notaires), celle de voir leur rôle et métier disparaître dans une vague de décentralisation informatique. L'opposition entre les techno-anarchistes de la décentralisation d'une part et la centralisation administrative et intellectuelle des juristes d'autre part, est en effet intrinsèque comme le suggèrent certains auteurs « *on voit à quel niveau de profondeur se situe la rivalité possible entre le droit et la blockchain : celle-ci prétend faire de manière plus scientifique et infalsifiable le même travail vis-à-vis des transactions dans le monde ordinaire que celui qu'accomplit le droit, c'est-à-dire de qualifier et donc, ipso facto, de juger* »[825]. Cependant, le postulat d'un droit entièrement algorithmique et décentralisé ne semble qu'une utopie au regard de la construction de nos sociétés où une décentralisation sociale ne semble généralement avoir que peu de place et de chance pour s'introduire. Face à ce besoin de confiance inné et à cette réalité sociale et comportementale, les limites des technologies 3.0 apparaissent. En effet et paradoxalement, nouer des ponts entre ces solutions décentralisées et les acteurs centralisés de notre société nécessite davantage l'intervention d'un professionnel du droit, c'est-à-dire d'un tiers de confiance dont l'identité et la responsabilité sont clairement établies pour réaliser des transactions juridiques (civiles, contractuelles, fiscales et financières, immobilières, judiciaires). Selon le journaliste et auteur Marc Bousquet : « *les blockchains obligent à réinventer les métiers de légiste et de juriste, tandis que les codeurs sont appelés à faire du droit – plus ou moins consciemment.* »[826]. Finalement, il apparaît que tout service décentralisé (quel que soit son degré/échelle de décentralisation)

[823] *Op. cit.* LASSEGUE Jean, GARAPON Antoine, « Justice digitale », pp.102-103, « Les avocats ont l'habitude de croiser le fer avec les notaires, les avoués, les experts-comptables, les juristes d'entreprise, mais à chaque fois, tous restent dans la grande famille des juristes ».
[824] *Op. cit.* GIRARD, Guillaume, « A Tale of Chaos vs Order: The ideological war between Bitcoin and Ethereum doesn't need to happen », Medium, consulté le 21 juin 2022, à l'adresse suivante, *v.* également Annexe 3 et 6
[825] *Op. cit.*,, « Justice digitale », p.140. Éd. Kindle.
[826] *Op. cit.*, BOUSQUET Marc, « Tout savoir sur le Bitcoin et les cryptomonnaies », Dossiers Science Hors-Série, in édition *du Sens*, ISSN : 2802-1843, novembre 2022, p. 41.

ne pourra se passer de l'intervention *ante* ou *post* d'un professionnel du droit, d'autant plus face à la recentralisation qu'impliquera l'application des Règlements MiCA et TFR. Cela s'explique également par l'histoire, l'expérience, la garantie des droits des justiciables ou encore la qualité des juristes au sein de notre société. Si le point de vue neutre du juriste permet indéniablement de prendre du recul sur l'objet technique dont il est question, il l'éloigne parfois de sa bonne compréhension et donc de son appréhension juridique[827]. Ainsi, un subtil équilibre entre acculturation technique des juristes et prise de recul (éducation)[828] sera nécessaire pour faire émerger de plus en plus de juristes 'augmentés' à l'avenir. Tout code décentralisé doit mettre en place un système de gouvernance (informatique et social) : telle est la règle informatique qui s'applique par essence aux blockchains, selon son extrapolation et acceptation juridique. Par exemple, dès lors que les diverses applications techniques et juridiques de la blockchain sont comprises par l'esprit des praticiens du droit, ces derniers doivent tenir compte des tensions potentielles entre le droit actuel de la propriété intellectuelle et de la protection des données personnelles appliquées au Web 3.0. En effet, les lois et les règles applicables dans les juridictions concernées sont des connaissances essentielles pour les professionnels du secteur 3.0, notamment afin de comprendre les restrictions concernant, pour illustration, le contenu, les formats et le lieu de stockage des informations et des preuves des blockchains. Face à ces évolutions parfois radicales, comme avec les blockchains publiques et les crypto-actifs, l'univers du droit et ses praticiens constatent parfois que le fond (législatif) et la forme (métiers) de leurs pratiques évoluent, sans toujours en comprendre ou en accepter les origines et les raisons. Par voie de conséquence, le corps législatif[829] a tendance à vouloir encadrer tout objet juridique non identifié, parfois avec le soutien de certains juristes[830], mais également parfois avec un manque de connaissance et par conséquent de capacité d'anticipation technologique. En réalité, une ouverture des esprits et des champs de compétences semblent intimement liés. Par conséquent, il semble important que les juristes collaborent avec les développeurs pour comprendre les effets juridiques des programmes décentralisés et leur relation avec chaque branche du droit et chaque texte de loi. En pratique, la blockchain va impacter les professionnels du droit, comme cela est déjà le cas pour les directeurs en conformité (KYC, LCB-FT). A ce titre, le rôle de certains juristes sera de réidentifier certains bénéficiaires et détenteurs de crypto-actifs, conformément à l'instauration du nouveau cadre règlementaire mentionné précédemment. Principalement en raison de son origine financière provenant de Bitcoin[831], les principaux cas d'usage actuels demeurent financiers. Néanmoins, de nombreux autres font déjà leurs preuves, comme le cas d'usage de la certification blockchain (des

[827] *Op. cit.* JEAN Aurélie, « Les algorithmes font-ils la loi ? », « […]es prochains textes ne pourront être articulés correctement que s'ils sont pensés et construits sur la base de connaissances et de savoirs scientifiques et technologiques approfondis », position de lecture dans le livre : 10%.
[828] V. *infra*, II, Titre 1, 1.5.3.2
[829] GAYTE Aurore, « Les sénateurs ne comprendraient rien aux cryptos et une sénatrice veut changer ça », 2022, in *Numerama*, article disponible à l'adresse suivante
[830] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, « L'identité numérique ; quelle définition pour quelle protection ? », 2020, p.162, « L'appréhension du numérique par le droit est source d'indéniables défis pour le juriste. Celui-ci, en quête de rationalisation et de clarification, se trouve confronté à des techniques et des concepts souvent obscurs pour une personne qui n'est pas experte dans le domaine de l'informatique. ».
[831] V. Annexe 3 & 6, Focus 1.

diplômes[832], des dessins industriels, des attestations ou encore des extraits KBIS[833]). Par exemple, cette dernière implique dans son sillon les professionnels de la propriété intellectuelle, amenés à retravailler la technique du droit d'auteur, des marques ou encore des brevets, face à la technique de la blockchain. Finalement, tous les juristes ne seront pas directement impactés par les divers cas d'usage des technologies blockchains, mais avec certitude et par ricochet, ils le seront probablement via leurs clientèles qui utiliseront probablement des blockchains publiques, privées ou hybrides. Dès lors, il ne s'agit pas de considérer une recentralisation totale des services décentralisés par les tiers de confiance que sont les notaires, avocats, commissaires de justice[834] les greffiers ou encore les experts-comptables, mais plutôt de ne pas renier leurs qualités, expériences et nécessités pour la société. En effet, leur présence et leur action garantiront la sécurité de toute opération technique ou juridique liée à une ou plusieurs transactions sur la blockchain, au bénéfice des parties prenantes concernées. A ce titre, il convient de citer plusieurs services pseudo-décentralisés (une blockchain privée) que propose actuellement l'ordre des Commissaires de justice, en partenariat avec la société IBM, faisant ainsi figure d'exemple industriel en la matière dans le monde du droit[835]. De même, le projet « *MonIdenum* »[836] est un service proposé par le Conseil National des Greffiers des tribunaux de Commerce et Infogreffe qui permet aux dirigeants d'entreprise de se connecter rapidement et de manière sécurisée sur les sites partenaires d'Infogreffe (système d'identité numérique fédérée). Ce système recourt aussi à une blockchain privée pour renforcer la sécurité des informations échangées entre les greffes et accélérer l'actualisation des registres des commerces et des sociétés (RCS), tout en empêchant la fraude documentaire, la création d'entreprises fictives ou l'usurpation d'identité de dirigeants d'entreprises.

2.7.1 Le rôle des juristes renforcé par l'identité décentralisée

De manière générale, l'identité numérique décentralisée (IND)[837] permettra aux juristes de certifier de manière plus fiable et transparente l'identité civile des parties impliquées dans une transaction commerciale. Cela permet non seulement de réduire les risques d'escroquerie, mais aussi de renforcer la confiance entre les parties prenantes. Le cas échéant, les juristes peuvent également utiliser la blockchain pour stocker de manière sécurisée certaines informations juridiques relatives à une transaction, ce qui réduit les risques de falsification de documents et facilite la vérification de l'authenticité des contrats.

[832] BC Diploma et Université de Lille, « Attestations numériques blockchain de réussite au diplôme de l'Université de Lille », Livre Blanc du projet « Dem-Attest-ULille », février 2023, disponible à l'adresse suivante
[833] En référence à un projet mené par la société Blockchain Partner, en 2018, avec l'Etat de Genève concernant l'émission d'extrais *KBIS* grâce à l'ancrage de *métadonnées* (d'empreintes numériques) infalsifiables et durables. Plus d'informations à l'adresse suivante
[834] Décret n° 2021-1625 du 10 décembre 2021 relatif aux compétences des commissaires de justice, disponible à l'adresse suivante, *v.* également Chambre nationale des commissaires de justice (CNCJ), disponible à l'adresse suivante
[835] Notamment pour réaliser des constats par des commissaires de justice directement en ligne ou encore pour horodater des données ou document de façon similaire à l'enveloppe Soleau, consultez l'adresse suivante www.legide.paris
[836] Pour plus d'informations consultez le site monidenum.fr
[837] V. *infra*, II, Titre I, Chap. 1

Pour l'instant, l'IND demeure un marché de niche par rapport à celui des crypto-actifs, bien que ces deux briques technologiques soient conceptuellement regroupées dans le Web 3.0 au sens de cette étude. L'impact de l'IND sur les professions du droit est donc à ce jour méconnu et anecdotique, mais il est suggéré qu'au fil de son adoption les métiers du droit seront impactés, notamment pour articuler ces nouvelles normes informatiques avec les règles de droit et par ruissèlement avec la vie progressivement numérisée des juristes. En renfort des propos de la partie précédente, il est possible d'identifier et regrouper en quatre grands métiers du droit les domaines qui seront impactés par l'IND dans la décennie qui vient : (i) les avocats[838], (ii) les notaires, (iii) les institutions judiciaires et (iv) les commissaires de justice. Premièrement, les tiers de confiance et représentants du système judiciaire peuvent utiliser des attributs d'identité numérique décentralisée (DID, VC) [839] pour émettre ou endosser des actes[840]. Les mises à jour de ces actes pourraient être suivies en temps réel et retracées si nécessaire, en utilisant une ou plusieurs blockchains dédiées (privées ou consortiums pour garantir la conformité légale). Ces possibilités permettraient une organisation plus transparente et efficace des interactions entre les acteurs du système judiciaire, renforçant ainsi la confiance numérique des justiciables. A titre d'illustration, la technologie blockchain commence d'ores et déjà à être utilisée dans le cadre de leurs (crypto)activités[841] par certains juristes et dans certaines juridictions. En 2022, un pirate informatique a par exemple reçu une ordonnance restrictive temporaire (« TRO »)[842] de la part d'un cabinet d'avocats. Cette ordonnance lui a directement été envoyée sous la forme d'un NFT[843] sur son portefeuille de crypto-actifs, permettant a posteriori le gel de ces fonds frauduleux en vertu d'une autre ordonnance d'un tribunal du Liechtenstein[844]. Cette situation pourrait marquer un tournant pour le législateur, qui pourrait prendre conscience de la valeur ajoutée technique de l'inscription directe et de la transmission d'actes juridiques ou de preuves procédurales via une blockchain. Loin de l'a priori des crypto-actifs comme facilitateurs d'activités illicites, ils peuvent également être un moyen efficace d'identifier des criminels et de protéger des internautes ou victimes. Les blockchains fermées représentent un segment du Web 3.0 à fort potentiel pour les juristes, bien que cela soit moins sensationnel sur le plan de l'innovation informatique. Cependant, ces cas d'utilisation génèrent des besoins importants en matière de contractualisation plutôt classique, seule l'approche commerciale paraissant innovante. Par exemple, la traçabilité des biens dans le secteur du transport (médicaments, aliments) implique un important besoin de contractualisation. Néanmoins, contrairement aux crypto-actifs qui soulèvent actuellement des problèmes juridiques

[838] SUN Mengqi, « Crypto Industry Can't Hire Enough Lawyers », 2022, in *The Wall Street Journal*, Consulté le 28 avril 2022, à l'adresse suivante
[839] V, *infra*, II, Titre 1, 1.3.1
[840] Concrètement, ces acteurs pourraient accuser réception d'un acte juridique, le modifier et le renvoyer de façon cryptographiquement sécurisé et vérifiable par d'autres parties.
[841] Voir aussi la décision de justice d'un tribunal mexicain dans la partie suivante.
[842] District de Columbia Courts, définition disponible en ligne à l'adresse suivante, traduction libre de l'anglais, « Un ordre restrictif temporaire (TRO) fait partie d'un procès civil et dure environ 14 jours. Un juge peut ordonner à une partie de faire ou de ne pas faire quelque chose pour cette courte période, y compris rester loin de et / ou n'ayant aucun contact avec vous ».
[843] V. *supra*, I, Titre 1, 2.3.1.1.f
[844] LCX, « Law firm serves anonymous hacker a restraining order via NFT. BTC PEERS ». Consulté le 23 juin 2022, à l'adresse suivante, traduction libre de l'anglais, « Le lien du 'Service NFT' mène à des documents juridiques, dont l'ordonnance TRO, à l'adresse suivante : https://www.hklaw.com/en/general-pages/lcx-ag-v-doe ».

complexes, notamment en pénétrant de nouveaux secteurs avec de nouvelles fonctionnalités, les blockchains fermées ne suscitent que peu ou pas de problèmes juridiques nouveaux. A l'inverse, dans des secteurs tels que les jeux vidéo[845] ou même celui du droit des sociétés, l'introduction des crypto-actifs (blockchains publiques) entraîne régulièrement une nouvelle approche juridique, car elle implique une tokenisation des actifs, c'est-à-dire l'utilisation de la technologie blockchain pour transposer les caractéristiques intrinsèques d'actifs tangibles (biens immobiliers, biens meubles) ou intangibles (parts sociales, caractéristiques d'un personnage dans un jeu vidéo) à des représentations virtuelles uniques. Cette extension et/ou duplication depuis l'univers physique vers l'univers numérique permet en théorie à chaque personne de transférer, d'immobiliser ou diviser ces représentations virtuelles uniques. Dans ce contexte de recherche et avec cette volonté désormais affichée de tokenisation, l'identité numérique pourrait également être sujette à une tentative de tokenisation, c'est-à-dire à une forme de traçabilité ou de valorisation financière de certains attributs d'identité[846]. En matière de protection des données au visa du RGPD, il est important de rappeler que celui-ci est neutre envers les technologies utilisées et ne cherche pas à limiter une technologie en particulier, mais plutôt à responsabiliser la personne qui l'administre, à savoir le responsable de traitement des données. Il est rappelé que le RGPD ne s'applique pas à l'ensemble d'Internet, mais uniquement aux personnes en charge du traitement des données de leurs applications, et de même, il ne cible pas directement la technologie blockchain, mais plutôt les titulaires et les opérateurs de celle-ci. Par conséquent, l'identité numérique décentralisée[847] peut aider les « Data Protection Officer – DPO » à remplir leur mission en renforçant la sécurité des données personnelles. En effet, l'identité numérique décentralisée permet de regrouper les informations d'identification de manière sécurisée et de les partager uniquement avec les parties prenantes autorisées. Les DPO pourront également utiliser une blockchain fermée pour stocker des preuves d'activités de traitement de données personnelles, ce qui peut faciliter des audits de conformité.

2.7.2 Perspectives d'une justice alternative et décentralisée avec le protocole Kleros

La montée en puissance des transactions numériques sur diverses blockchains publiques a conduit inévitablement à une hausse des conflits entre les utilisateurs, à la suite de fraudes, de vols et de pertes de crypto-actifs. Pour cette raison, de nouvelles plateformes alternatives et expérimentales de règlement des litiges ont vu le jour sur certaines blockchains ouvertes, comme le système « *Kleros* » en 2018[848] ou

[845] V. *infra*, II, Titre 2, 1.4
[846] Pour étayer ces propos, le dirigeant de la société Ledger (spécialisée dans la sécurisation physique et logicielle des crypto-actifs), Pascal Gauthier, explique : « L'identité tokenisée, c'est votre prochain marché ? Oui, la combinaison de l'argent et de l'identité, c'est le futur du portefeuille physique, le hardware wallet dans le jargon crypto. Nous voulons fournir une solution qui sera une sorte de compagnon de tous les jours pour les utilisateurs. » ; « Notre ambition va bien au-delà de la crypto », TELLIER Louis, 2022, in *AGEFI*, consulté le 17 octobre 2022, à l'adresse suivante
[847] V. *infra*, II, Titre I, Chap. 1
[848] V. pour plus d'informations le site internet du projet disponible à l'adresse suivante

« *Aragon Network Jurisdiction* »[849] en 2020. Cette partie étudie la solution Kleros, objet également de l'Annexe 8 qui lui est spécifiquement dédiée, afin de déterminer si une blockchain publique représente une infrastructure viable pour héberger une justice en ligne alternative, expérimentale et décentralisée. Il s'agit de comprendre pour quelles raisons l'adhésion à une telle proposition est aussi ambitieuse et innovante pour certains pays en voie de développement, qu'incertaine et marginale à court et moyen termes dans les pays développés. Le 31 juillet 2018, la naissance du protocole Kleros propose une nouvelle application décentralisée à la sphère numérique et judiciaire[850]. Kleros, une société coopérative d'intérêt collectif (SCIC)[851], s'engage à concrétiser la promesse d'un « *système judiciaire décentralisé à l'ère de l'internet* »[852]. Bien que la justice représente une prérogative régalienne tout comme la délivrance d'une identité légale, Kleros cherche à émanciper et à démocratiser cette pratique grâce au numérique. Le protocole Kleros souhaite ainsi apporter une nouvelle réponse efficace à l'augmentation des litiges de la sphère numérique due à l'augmentation du nombre d'internautes qui interagissent et consomment en ligne[853]. En 2020, Kleros a reçu un prix du Conseil européen de l'innovation avec un financement à hauteur d'un million d'euros pour développer une justice numérique décentralisée[854]. Au regard des sciences sociales, Kleros compte sur l'intelligence collective – sur une « *sagesse d'une foule de participants* »[855] - pour résoudre des litiges via un espace numérique supposé décentralisé et incensurable. Avec Kleros, chaque décision prise par un jury d'internautes pseudo-anonymes et détenteurs de crypto-actifs reflète la sagesse collective de cette crypto-communauté. Ces jurés sont incités à agir honnêtement lorsqu'ils tranchent des conflits, car ils sont économiquement contraints en cas de décisions contraire à la morale collective. Ce système alternatif permet, en théorie, d'aboutir à une forme de vérité collective. Il est issu de l'expérience sociales de « *La Sagesse des foules* »[856] puis a été transposé par Kleros dans le Web 3.0. Cet écosystème distribué considère que cette approche de sagesse communautaire permet effectivement d'atteindre un jugement moralement juste, voire impartial[857]. En pratique, le modus operandi proposé par Kleros est de mettre à disposition de tout internaute un nouveau protocole de résolution des litiges permettant à ses utilisateurs de trancher

[849] « Aragon Network Jurisdiction Part 1: Decentralized Court », 2021, in *Aragon's Blog*, disponible à l'adresse suivante
[850] *Op. cit.* « (…) la blockchain porte dans ses blocs et ses chaînes une véritable théorie de la justice (…) », « Justice digitale », p. 157.
[851] Pour en savoir plus concernant la *SCIC Kleros* consultez l'adresse suivante
[852] Présentation d'une page de Kleros, p. 2, consulté en ligne le 21 avril 2021.
[853] Avec la digitalisation progressive de notre société, la contractualisation numérique est en plein essor et, par effet de ruissellement, de nombreux litiges numériques naissent. En ce sens, et parce que le nombre d'acheteurs en ligne augmente (via le commerce en ligne), alors une augmentation proportionnelle des litiges numériques devrait continuer à s'amplifier à l'avenir. Statista, « Digital buyers worldwide 2021 », consulté en ligne le 22 avril 2021.
[854] CE, Shaping Europe's digital future. « The Commission's European Innovation Council awards 5 million € to blockchain solutions for social innovations. », 30 juin 2020, disponible à l'adresse suivante
[855] SUROWIECKI James, « The Wisdom Of Crowds », 2005, in *Anchor Books*, ISBN: 0-385-72170-6, consulté en ligne le 21 novembre 2021, p. 53.
[856] *Ibid.* Traduction libre de l'anglais, « Ce sont toutes des tentatives d'exploiter la sagesse de la foule, et c'est la raison pour laquelle elles fonctionnent. Il s'avère que la véritable clé n'est pas tant de perfectionner une méthode particulière que de remplir les conditions - diversité, indépendance et décentralisation - dont un groupe a besoin pour être intelligent. ». Lire pp.119-121 l'expérience sociale du Professeur Thomas C. Schelling.
[857] En référence à une série de journées et d'ateliers sur le sujet de Kleros : « Atelier – Justice décentralisée » – EHESS – 18 novembre 2022 10h30-17h, organisateurs : Katrin Becker (Univ. Luxembourg) et al. Lieu : EHESS, 54 boulevard Raspail 75006 Paris - salle A06_51.

équitablement - grâce à des contrats intelligents sur la blockchain Ethereum[858] - des litiges de tous ordres, également soumis par des internautes. Concrètement, le protocole Kleros articule ainsi la technologie blockchain à une collaboration communautaire en ligne (« *crowdsourcing* »[859]), pour résoudre en ligne des réclamations et des litiges. Cette coordination innovante caractérise une forme de tentative de judiciarisation en ligne, qui vante son ouverture et sa transparence au service d'un Internet plus juste et ouvert. Ce projet est ainsi en phase avec une certaine volonté et idée de réinventer la justice sociale, depuis l'Etat de droit et ses institutions, vers une justice pour les internautes et par les internautes. Pour fonctionner, cette architecture décentralisée s'appuie sur des incitations économiques pour motiver des internautes pseudo-anonymes – les *jurés* précités - à statuer au plus proche de la vérité en fonction de chacun des litiges soumis directement sur le site internet et la plateforme maintenue par Kleros[860]. Le système se fonde sur plusieurs principes de sélection en théorie aléatoire de ces citoyens-jurés, un univers emprunté aux Athéniens et à la Grèce antique tant sur le plan conceptuel et démocratique, que mercatique[861]. Dans ce contexte, le recourt à la technologie blockchain et à un crypto-actif propose de résoudre une problématique déjà soulevée par Aristote il y a plusieurs siècles « *celui qui contrôle les tribunaux, contrôle l'État* »[862]. En d'autres termes, la transparence juridique est essentielle à tout système judiciaire, et les justiciables doivent pouvoir avoir confiance dans l'intégrité du processus judiciaire, y compris la sélection des juges et l'authenticité des preuves présentées. Pour répondre à ce défi, Kleros utilise les incitations de la « *théorie des jeux* »[863] ainsi que le crowdsourcing pour que les jurés puissent juger les affaires de manière juste et impartiale. La blockchain publique Ethereum enregistre de manière vérifiable et permanente tous les processus de règlement en ligne des litiges soumis à Kleros. Dès lors, cette blockchain publique permettrait-elle de répondre de manière optimale aux exigences de transparence d'un nouveau système judiciaire 3.0 ?[864]. A ce stade, il semble qu'en partie seulement. En effet, des compromis au détriment d'autres composantes sociales et légales surviennent, il est en effet pertinent de se pencher sur quatre questions fondamentales et défis que Kleros doit relever[865] : est-ce que le système est vraiment décentralisé sur le plan informatique ? Comment peut-on avoir confiance

[858] V. Annexe 6, Focus 2.
[859] Le *crowdsourcing* consiste à tirer profit des connaissances d'une communauté et d'une foule d'internaute pour obtenir un résultat social donné.
[860] Consultez la plateforme de Kleros à l'adresse suivante, *v.* également Annexe 8.
[861] En grec, « Kleros » signifie « chance ». Dans la Grèce antique, une « clérouquie » (« klêroukhía » en grec ancien) était l'attribution de lots de terre civique (« kleros ») à des soldats-citoyens par tirage au sort. Ces soldats-citoyens étaient appelés des « clérouques » (qui étaient présents à Athènes aux Ve et IVe siècles avant J.-C). Le terme « kleros » désignait donc le lot de terre attribué par tirage au sort à un citoyen. C. Vial, *Lexique de la Grèce ancienne*, A. Colin, 2008.
[862] MIRHADY David C., « Aristotle and the Law Courts », Polis J. Anc. Greek Polit. Thought, 2006, consulté le 22 avril 2021.
[863] Pour comprendre ce concept en informatique, il est possible de se référer à l'explication suivante suivante : « Satoshi Nakamoto nous a appris qu'un certain nombre d'ordinateurs anonymes qui ne se font pas confiance peuvent néanmoins parvenir à un consensus, à condition que des mécanismes d'incitations économiques soient correctement structurées. Kleros étend ce principe à la prise de décision humaine. Un certain nombre de jurés anonymes qui ne se font pas confiance peuvent *parvenir à* un consensus sur une bonne décision, à condition que les incitations soient correctement structurées. », AST Federico, « Kleros : Frequently Asked Questions about Peer-to-Peer Justice », 2017, in *Medium*, disponible à l'adresse suivante
[864] En évoquant le chiffre *3.0*, il est fait référence à une comparaison entre les *LegalTech* qui proposent des services numériques centralisés *(2.0)*, à la différence de la technologie blockchain qui propose, certes, aussi des services en ligne, mais, décentralisés *(3.0).* Ainsi, parce que le degré informatique requis pour une blockchain semble plus important que pour une *LegalTech 2.0*, le terme *3.0* devient pertinent tout en étant technologiquement distinctif.
[865] V. Annexe 8.

dans cette pseudo-institution qui se substitue aux tribunaux, étant donné une incertitude technologique omniprésente ? En fin de compte, Kleros rend-il réellement justice au sens du droit ou plutôt au sens de sa communauté d'internautes ?

La plateforme exige des utilisateurs-jurés qui détiennent et utilisent un jeton numérique d'utilité[866] appelé « *PNK* »[867]. Il est souligné que les utilisateurs de Kleros ne sont pas tenus de maîtriser la programmation informatique pour utiliser les contrats intelligents développés par la plateforme, car ceux-ci sont conçus pour être relativement accessibles facilement via sa plateforme. Les cas d'usage et litiges ciblés par ce service innovant sont en théorie nombreux[868], mais semblent pour l'instant plutôt marginaux et circonscrits à l'univers des crypto-actifs et tout au plus certains autres domaines du Web 3.0 (Métavers[869], NFT). Kleros a en effet trouvé un ancrage solide dans l'univers des crypto-actifs au sein duquel il peut déployer ses fonctionnalités de manière optimale en créant une conception philosophique de la justice toutefois différente du système juridique conventionnel. La Finance Décentralisée (DeFi) est également un écosystème composé de multiples protocoles pseudo-décentralisés, où les utilisateurs régulièrement lésés peuvent désormais se tourner vers Kleros pour obtenir une forme de justice en cas de perte ou d'extorsion de leurs crypto-actifs, ou pour contester des informations trompeuses fournies par des plateformes d'échange de crypto-actifs[870]. Néanmoins, la faillite de la plateforme et crypto-bourse « FTX »[871], qui a défrayé la chronique en 2022, a entraîné une augmentation de la demande pour les protocoles décentralisés, bénéficiant par voie de conséquence à Kleros. Du point de vue des sciences de l'informatique, Kleros répond à la problématique dite « *Sybil* »[872], qui consiste à éviter la duplication de fausses identités par des jurés, qui pourraient ainsi manipuler les décisions collectives de cette crypto-communauté en ligne. Il existe de nombreux mécanismes de blockchains publiques qui résolvent plus ou moins parfaitement cette problématique informatique de l'attaque Sybil, notamment grâce à des mécanismes d'incitation (crypto)économique[873] d'efficacité inégale, telles la Preuve de travail (« PoW »), la preuve d'enjeu (« PoS ») ou la preuve d'autorité (« PoA »), étudiées dans l'Annexe 6. Il convient de dresser le portrait de Kleros en ce qui concerne son potentiel et ses limites. Les méthodes

[866] Comme nous l'avons expliqué dans la partie dédiée aux crypto-actifs, le *PNK* est un *jeton d'utilité* ou *utility token* et son incitation économique vise à encourager son utilisation sur le protocole et les applications de Kleros.
[867] Il y a plusieurs milliers d'années en Grèce antique, un *pinakion* était une petite plaque de bronze qui permettait d'identifier le citoyen d'une ville en affichant son nom. C'était une forme de *jeton citoyen*. Les candidats à un poste politique ou à un poste de juré inséraient leur *pinakion* dans une machine appelée *klérotèrion*, pour procéder à un tirage au sort manuel. Le projet Kleros tire ainsi son nom et son jeton numérique (PNK) de cette outil et époque emblématique de la Grèce antique, parfois considérée comme le berceau de la démocratie.
[868] Jeux en ligne, conflits en matière de propriété intellectuelle, soins de santé, médias sociaux, financement participatif, travailleurs indépendants, etc.
[869] V. *infra*, II, Titre 2, 1.4
[870] Kleros permet à tout utilisateur de soumettre un litige, ce qui signifie que si un protocole décentralisé ou une plateforme d'échange centralisée fourni des informations incomplètes ou erronées à ses utilisateurs, ces derniers pourront se retourner contre eux via Kleros. Cela est tout à fait possible concernant les « *preuves de réserves* [de crypto-actifs] » (« *proof of reserve - PoR* ») de ces entités qui peuvent être plus ou moins exactes et pourtant essentielles pour créer et assurer la confiance des crypto-utilisateurs.
[871] Contributeurs aux projets Wikimedia, « Faillite de FTX », 2023, disponible en ligne
[872] V. Annexe 6, Focus 1.
[873] V. Annexe 6, Focus 1 à 3.

alternatives de règlements des différends (MARD)[874] qui connaissent un développement croissant aujourd'hui sont un exemple de décentralisation qu'intéresse Kléros, que les litiges soient d'ailleurs d'ordre judiciaire (ordonné par un tribunal) ou d'ordre conventionnel[875], c'est-à-dire convenu entre les parties d'un litige. À mesure que le protocole Kleros et sa blockchain sous-jacente Ethereum[876] évoluent, il semble que ce système de justice décentralisée puisse un jour permettre de résoudre des litiges de plus en plus complexes. Une mise à jour de Kleros est ainsi en cours de déploiement courant 2023. Pour l'heure, Kleros permet d'ores et déjà de généraliser l'utilisation des contrats intelligents dans un nombre restreint, mais croissant, d'activités crypto-économiques. Cependant, la proposition de Kleros comporte certaines limites qu'il convient d'évoquer. Par exemple, ses (crypto)frais soit son coût d'utilisation est assez important, car plus le nombre d'utilisateurs de la blockchain Ethereum augmente, plus les frais payés par les utilisateurs de Kleros augmentent mécaniquement[877] se traduisant par une augmentation du prix à payer pour devenir juré sur Kleros[878]. Cela représente une conséquence économique difficile à accepter pour les juristes qui estiment que la justice doit être accessible et gratuite[879]. Kleros tente déjà de déploier certaines solutions face à ces problématiques de volumétrie et de mise à l'échelle limitée de la blockchain sur laquelle il fonctionne[880]. L'incitation économique relatvie au PNK, représente également un frein au fonctionnement de Kleros en raison d'une centralisation économique d'une majorité des jetons auprès de quelques personnes physiques et morales[881]. En 2023, la solution de Kleros fonctionne à petite échelle et pour quelques centaines ou milliers d'individus, mais demeure inaccessible pour un nombre plus important d'internautes. En dépit de son efficacité dans de nombreux cas, il convient de reconnaître que Kleros a une limite majeure : il demeure un système mathématiquement binaire et par conséquent peu adaptable à la complexité des litiges qui nécessitent des connaissances professionnelles en droit et en procédure. Ces compétences ne peuvent être apportées que par des juristes issus de professions réglementées, ce qui limite la portée de Kleros dans certaines situations. Il semble

[874] ROLLAND Paul, doctorant, « Les Modes Alternatifs de Règlement des Différends (MARD) », in *Village de la Justice*, consulté le 23 avril 2021, *v.* également les dispositions des articles 131-1 à 131-15 du Code de procédure civile régissant les médiations ordonnées par un tribunal (dites judiciaires) et celles des articles 1530 et s. du même code pour les médiations dites conventionnelles.

[875] Conseil d'Etat, Étude annuelle 2014, Le numérique et les droits fondamentaux, consulté le 20 novembre 2021, *v.* également la recommandation n°3 du Conseil d'État : développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques.

[876] V. Annexe 6, Focus 2.

[877] Pour devenir juré au sein d'une Cour de Kleros, un montant minimal de *1000 PNK* doit y être séquestré.

[878] La variation des frais de transaction sur une blockchain est automatique et protocolaire. C'est la loi de l'offre (les ordinateurs qui valident les transactions) et la demande (les utilisateurs souhaitant effectuer des transactions) qui s'applique. Ainsi, plus il y a de demande de transaction des utilisateurs, plus les ordinateurs qui valident les transactions deviennent en incapacité – temporaire – à répondre à cette demande, ce qui fait mécaniquement augmenter les frais de transaction. V. Annexe 3, Focus 1 à 4 et Annexe 6, Focus 1.

[879] La justice est un bien commun qui peut certes avoir un coût, mais ne devrait pas avoir de prix : dans le système judiciaire traditionnel un juge est payé pour rendre un verdict en vertu de ses compétences et de son pouvoir, le fait que Kleros fasse payer des jurés pour rendre justice est donc en opposition fondamentale avec notre fonctionnement judiciaire actuel.

[880] La blockchain Ethereum a connu une mise à jour majeure de son protocole en 2022 (« The Merge » aussi connu sous le nom « d'ETH 2.0 »), permettant à terme de réduire ses frais de transactions. Nous pouvons entre autres évoquer la solution XDAI ou encore Polygon qui permettent d'effectuer des transactions à moindre coût, bien que ces solutions soient informatiquement centralisées (recentralisation informatique), *v. supra*, I, Titre 1, 2.3.2

[881] A ce titre, Vitalik Buterin estime que « Pour faire confiance à un service tel que Kleros, il semble nécessaire qu'il n'y ait pas un seul individu détenteur de plus de 25% des jetons dans l'une de ces courts numériques. », « DAOs are not corporations : where decentralization in autonomous organizations matters », 2022, *op. cit.*, disponible à l'adresse suivante

que Kleros manque actuellement d'un espace politique permettant l'expression de la parole, à l'instar d'un système de justice traditionnel. Cela signifie que cette plateforme ne parvient pas encore à recréer certains éléments humains essentiels propres au monde physique. Bien que la solution Kleros permette une démocratie directe partiellement fiable grâce à ses votes communautaires, elle reste une alternative qui ne permet pas l'expression de la parole sous forme de vidéos en temps réel, de messages vocaux, etc. Par conséquent, il semble que Kleros doit implémenter un espace politique où la parole de ses jurés ou des parties d'un litige puisse s'exprimer – par des témoignages, conclusions, plaidoiries - afin d'assurer plus d'humanité et moins de déterminisme par le calcul (qu'implique les AEC). Les juristes qui étudient Kleros remarquent l'utilisation d'un vocabulaire mercatique similaire à celui du droit, bien que Kleros ne soit aucunement un tribunal judiciaire, même s'il vise à en reproduire les effets[882]. Selon Aurélie Jean, la justice et l'exercice de la loi sont avant tout une affaire d'êtres humains, de personnes physiques qui sont jugées, plaignantes, victimes ou défenderesses[883]. De plus, les juges doivent prendre en compte ce que le collectif considère comme juste dans un litige et en fonction des preuves présentées par les jurés, car ces derniers perdent leurs fonds séquestrés lorsque leur décision est minoritaire lors d'un vote dédié. Il n'y a donc pas de loi commune à exécuter, mais plutôt une morale collective qui juge chaque litige au cas par cas. En réalité, cette morale collective repose sur la mentalisation (consciente ou non) des lois propres à chaque juré, car ces derniers se basent en pratique sur le droit en vigueur pour rendre leur verdict. Il convient également de relever que seuls les litiges contractuels pour lesquels une clause compromissoire a été prévue pourraient bénéficier d'une reconnaissance et d'une valeur légale lorsqu'ils sont résolus par le protocole Kleros. En revanche, les autres litiges qui n'ont pas été préalablement contractualisés ne reposent sur aucun fondement juridique autre que moral, excepté sur l'échange de jetons PNK entre les parties, ce qui pourrait être considéré comme une forme de contractualisation tacite. Il est noté par exemple conformément à la Convention de New York que la plateforme Kleros ne peut être considérée comme une forme d'arbitrage juridiquement valide[884]. A ce titre, il est identifié quatre éléments qui font que Kleros est en rupture avec le système judiciaire actuel : (i) sa décentralisation, (ii) l'immuabilité des transactions effectuées, (iii) le quasi-anonymat des jurés et (iv) la binarité de son code informatique mentionnée au préalable. En pratique, la nature décentralisée de Kleros est relative puisque des intermédiaires et des opérateurs sont facilement identifiables sur les réseaux sociaux, un constat que le législateur européen mettra probablement en application si Kleros ne s'enregistre pas en tant que PSCA conformément à l'entrée en application du Règlement MiCA ainsi que TFR comme

[882] LEQUESNE-ROTH Caroline, « Metavers, Web3 : la révolution juridique en trompe-l'œil », in *Receuil Dalloz*, 2022, « La communauté du droit est attendue dans les batailles judiciaires qui seront conduites, et plus largement les arbitrages juridiques conclus qui cristalliseront des choix civilisationnels. Si la révolution juridique annoncée est un trompe-l'œil, l'inscription du droit numérique dans nos valeurs démocratiques et le respect de nos droits fondamentaux est l'un des enjeux majeurs du juriste du XXIè siècle. », disponible en ligne, p.5.

[883] JEAN Aurélie, « Les algorithmes font-ils la loi ? », *op. cit.*, position de lecture dans le livre : 82%.

[884] FERREIRA L.C., « La résolution des litiges blockchain : Vers un arbitrage décentralisé ? », Mémoire de Master de l'Université de Neuchâtel, 2021, p. 96, « Même si, en fonction des circonstances du cas d'espèce, une décision de Kleros peut théoriquement être qualifiée de sentence arbitrale étrangère au sens de l'art. I ch. 1 CNY, la procédure souffre de plusieurs anomalies empêchant d'opérer une telle qualification. » ; « Lorsque la procédure de Kleros est délocalisée, en ce sens qu'elle n'est pas liée à un ordre juridique, la Convention de New York ne trouve pas application. ».

précédemment étudiés. De même, le caractère immuable des transactions et de certaines informations relatives aux litiges (documents et pièces justificatives) qui sont publiées en non-conformité sur la plateforme de Kleros méconnaît pour l'instant les principes du RGPD[885]. Au regard de la territorialité du droit applicable concernant les litiges gérés par Kleros, sa nature décentralisée et sans frontière, couplée au pseudo-anonymat des transactions de ses utilisateurs, complexifie la localisation réelle du litige[886]. Sur le plan procédural, la création des procédures alternatives sur Kleros ne respecte pas certaines dispositions imposées par les règlements d'arbitrage internationaux (témoignages physiques des parties[887], droit à un procès équitable)[888]. Aussi, si la théâtralité des procédures est parfois critiquée, voire moquées (robes, jargons juridiques), elle est en réalité essentielle pour garantir la neutralité des rôles, l'équité et l'impartialité des décisions de justice. L'adoption généralisée de Kleros risquerait de progressivement effacer l'humanité des procédures judiciaires, tels que les plaidoiries et l'humanisme des juristes. Pour remédier à cela, il semble que le protocole Kleros puisse intégrer son propre Métavers[889] à l'avenir, ce qui permettrait d'organiser des délibérations avec des avatars (les jurés pouvant décider de rester pseudo-anonymes). L'utilisation des Contrats Ricardiens déjà évoqués, semblerait également pertinente pour le protocole Kleros aux fins notamment d'optimiser l'articulation entre les contrats intelligents et les contrats en langage naturel éventuellement associés. En quelque sorte, Kleros applique les principes de jeu et de spéculation au système juridique en permettant aux utilisateurs de gagner de l'argent sous la forme de crypto-actifs tout en rendant actuellement des pseudo-jugements au regard des systèmes juridiques occidentaux. Cependant, pour assurer la viabilité à long terme de ce système, il est essentiel que son fonctionnement communautaire et ses mécanismes d'incitation économique soient transparents et équitablement distribués entre les utilisateurs[890]. Il est probable que dans un conflit entre le système Kleros et le système juridique traditionnel, le droit considérera l'utilisateur-juré comme un simple investisseur sans compétence judiciaire en raison de son pseudo-anonymat. Ce pseudo-anonymat pourrait être une faiblesse en cas de défaillance technique ou démocratique du protocole Kleros et l'implémentation d'une identification grâce aux standards de l'identité numérique décentralisée (IND) semblerait pertinente (implémenter une forme de pseudo-

[885] En 2023, il est possible de trouver en quelques clics des données personnelles de « justiciables » de la plateforme Kleros, car les documents sont accessibles à tout internaute. Ainsi, la conformité au RGPD n'est pour l'instant pas assurée par ce service 3.0.
[886] Le protocole KLEROS ne prend pas en compte les différences de territorialité et de culture juridique des juges qui ne se connaissent pas en raison de leur pseudo-anonymat respectif.
[887] *Ibid*. « […] le langage écrit ou oral était une étape essentielle au travail d'élaboration de la vérité. La transcription écrite ou le témoignage oral avaient pour but d'articuler un texte juridique à une réalité extra-légale. », p. 175.
[888] « […] aux côtés d'un raisonnement logique de la part du représentant de la loi venait s'asseoir une certaine intelligence émotionnelle pour envisager le justiciable comme un être unique avec une histoire et un passé qui lui appartiennent et qui sont, par définition, uniques et irreproductibles. », *op. cit*., JEAN Aurélie, « Les algorithmes font-ils la loi ? », position de lecture dans le livre : 81%.
[889] V. infra, II, Titre 2, 1.4
[890] Au 11 novembre 2022, seulement dix adresses Ethereum (sur plus de 9000) détiennent plus de 50% du total des PNK en circulation, ce qui signifie que la distribution des jetons PNK est relativement centralisée à ce jour. « *Pinakion Token Contract and Distribution Chart* », informations disponibles et vérifiables à l'adresse suivante

anonymat hybride)[891]. Cependant, il convient de souligner que le système judiciaire actuel n'est pas non plus parfait[892] et que les technologies et les concepts utilisés dans Kleros, tels les DAO et l'AEC, pourraient être utiles en impliquant des professionnels du droit. Kleros offre une nouvelle définition de la justice en ligne, mais cette redéfinition ne doit pas être au détriment des notions d'intégrité et d'honneur qui sont à la base du système juridique actuel et pourtant absentes de Kleros pour le moment.

En résumé, Kleros est un concept novateur qui présente l'avantage de proposer une alternative imparfaite au système traditionnel, comme celle par exemple d'une résolution alternative des différends (MARD) via ce protocole. Ce tiers de confiance décentralisé et expérimental permet à sa communauté de résoudre certains litiges financiers relatifs à l'utilisation de contrats intelligents déjà utilisés dans l'écosystème des crypto-actifs, notamment dans le domaine de la Finance Décentralisée. Bien que Kleros soit en partie en opposition avec le système judiciaire traditionnel et dépendant de sa reconnaissance dans les pays développés, il est important de considérer ce projet comme une alternative juste et pertinente dans les pays où la justice est affaiblie. En pratique, Kleros est déjà devenu le système de justice décentralisée privilégié pour résoudre des litiges au sein de la crypto-économie, comme le prouve une première décision de justice rendue au Mexique[893]. La solution proposée par Kleros est aussi pertinente, car elle nous amène à s'interroger sur la structure actuelle de notre propre système judiciaire. En d'autres termes, Kleros représente un symptôme du malaise actuel concernant certaines limites de notre système de justice qui souffre, entre autres, d'un manque de ressources humaines et de débouchées numériques. Il reviendra aux juristes de s'emparer ou de rejeter ces systèmes expérimentaux de justice alternative 3.0, mais il semble d'ores et déjà important d'explorer et d'approfondir les synergies possibles avec ce système en cours de maturation. Comme le propose justement le juriste suisse Léonel Constantino Ferreira « *dans une perspective de co-régulation, l'État pourrait se limiter à fixer un cadre procédural général à la résolution des litiges blockchains, tout en laissant aux participants à la technologie le soin de développer des normes précises et des mécanismes permettant de mettre celles-ci en œuvre* »[894]. Kleros n'opère pas pour autant dans un cadre juridique inexistant, ce qui signifie qu'une reconnaissance juridique lui est nécessaire sur le long terme pour survivre. Il doit mettre en place une solution hybride afin que sa forme de jurisprudence morale et collective devienne conforme aux lois et règlements en vigueur (RGPD, MiCA, TFR, eIDAS, Data Act). Selon un groupe de travail de l'EHESS consacré à ce phénomène de justice décentralisée, ce système de quasi-justice est déjà viable pour rendre justice dans certains pays en voie de développement où les États ne sont pas des États de droit en raison d'une

[891] Les *jurés* pourraient demeurer pseudo-anonymes tout en désignant des *jurés-référents* (titulaires d'un diplôme en droit) en support si besoin.
[892] Malheureusement, on redécouvre que sans une société unie autour des valeurs qui fondent un droit, sa dimension fondamentale et universelle peut être remise en cause, en une journée, par une poignée de personnes (constitutionnalistes, parlementaires), alors que cette décision en impactera des millions.
[893] Kleros, « How to enforce Blockchain dispute resolution in court? The Kleros Case in Mexico », 2022, disponible à l'adresse suivante, traduction libre de l'anglais, « C'est ainsi que, pour la première fois, un tribunal mexicain a reconnu et exécuté une sentence arbitrale dont la substance n'était pas régie par le seul jugement de l'arbitre, mais par un outil technologique conçu pour le règlement décentralisé des litiges : le protocole Kleros ».
[894] *Op. cit.* FERREIRA L.C., « La résolution des litiges blockchain : Vers un arbitrage décentralisé ? », p.95.

corruption importante des instances judiciaires[895]. Ainsi, cette justice décentralisée pourrait être considérée comme plus fiable dans certains pays d'Amérique latine ou d'Inde où se situent d'ores et déjà de nombreux utilisateurs de Kleros. Il est également probable que la croissance et le succès de Kleros dépendront de la croissance globale du Web 3.0 qui comprend de multiples technologies en phase (crypto-actifs, réalité virtuelle, Métavers, IND). Il semble que pour réussir à atteindre leur ambition théorique affichée ouvertement - « *Decentralized Justice as a Service* » - Kleros devra attirer d'autres communautés physiques et virtuelles, en particulier les juristes, pour assurer un soutien structurel à son déploiement. En ce qui concerne l'identité numérique, si le protocole Kleros a réussi à proposer avec succès un système de justice décentralisée dont le degré d'identification est relativement faible (niveau 1 ou 2)[896], il ne fait guère de doute que la mise en place d'une identité numérique auto-souveraine (INAS) propre au protocole Kleros, semble imminente. Grâce à cette identité numérique sur une blockchain, Kleros pourrait devenir un fournisseur d'identité décentralisée non seulement pour son propre service de justice décentralisée, mais également pour des tiers et services en ligne (PSCA) à la recherche d'identifiants et d'identités numériques vérifiables. À terme, la frontière entre justice décentralisée et identité numérique auto-souveraine pourrait ainsi s'estomper au bénéfice des utilisateurs de Kleros. Peut-être même qu'un jour cette justice en ligne décentralisée alimentera certaines composantes de la justice prédictive (utilisant l'intelligence artificielle).

2.8 La technologie blockchain comme outil au service de la preuve légale

À mesure que la technologie blockchain gagne en adoption au sein de la société, de plus en plus de professionnels du droit sont confrontés à une nouvelle question relative au droit et à l'informatique 3.0 : la technologie blockchain représente-t-elle une nouvel outil probatoire inégalé ? Certains adeptes de cette technologie la décrivent souvent comme un outil privilégié pour une preuve dématérialisée et fiable en raison de son accessibilité, de son coût supposé abordable, de son caractère programmable et de sa relative immuabilité. Par conséquent, il est important de se demander comment le droit français de la preuve encadre et reconnaît cette technologie perçue comme source de preuves numériques ultimes. D'abord, il convient de rappeler les deux principes directeurs du droit français de la preuve, dans lesquels la technologie blockchain doit s'inscrire pour être considérée comme un moyen de preuve admissible. En effet, le système civil et probatoire français repose sur le principe de la preuve légale, qui est légalement organisé et encadré, par opposition à la preuve morale qui admet tous les moyens de preuve possibles. Le système de preuve légale présent dans le droit français repose sur plusieurs aspects juridiques essentiels, parmi lesquels figurent cinq catégories de modes de preuve différentes consacrées

[895] Dans un pays corrompu, une justice décentralisée est probablement mieux qu'un système judiciaire corrompu. Elle représente un contre-pouvoir permettant de contourner la censure.
[896] Consultez le schéma dédié, *v, supra*, I, Titre 2, 1.4.1

par le Code civil[897] : (i) la preuve littérale ou par écrit, (ii) la preuve testimoniale ou par témoignage, (iii) les présomptions judiciaires, (iv) l'aveu judiciaire et enfin (v) le serment décisoire. À ce titre, chacune possède une admissibilité ainsi qu'une force probante variable[898]. En principe, le système de preuve légale régissant les actes juridiques impose que ceux-ci soient prouvés par des écrits, qui sont considérés comme des preuves parfaites et dont le caractère est irréfragable. En revanche, les faits juridiques sont régis par le système de preuve morale et peuvent être prouvés par tous moyens, c'est-à-dire constitutif de preuves dites imparfaites. La valeur probatoire des cinq modes de preuve mentionnés précédemment n'est pas égale. Certaines preuves, telles que la preuve par écrit (i), l'aveu judiciaire (iv) et le serment décisoire (v), sont considérées comme parfaites et probantes, et s'imposent au juge sans qu'il puisse remettre en question leur existence ou fondement. En revanche, d'autres preuves, telles que le témoignage (ii) et les présomptions judiciaires (iii), sont imparfaites et laissent le pouvoir de conviction à la libre appréciation souveraine du juge. De ce fait, sauf à amender le Code civil pour créer une sixième catégorie de preuve propre au caractère probatoire de la technologie blockchain, il semble dans un premier temps préférable de rattacher les informations contenues dans une blockchain à l'une de ces cinq catégories de la preuve légale dont il est question. Bien qu'en principe, la valeur probatoire et l'admissibilité des différents modes de preuve énumérés soient fixées par la loi, tous ne sont pas admissibles pour faire preuve de tous les éléments relatifs à des actes ou à des faits juridiques. En ce sens, une analyse décomposée en deux temps doit être effectuée à propos de l'article 1358 du Code civil. Ce dernier dispose que la preuve est libre : « (…) *la preuve peut être apportée par tous moyens* », ce qui laisse penser que tous les modes de preuve sont librement admissibles. Cependant, il dispose et précise tout d'abord que « *or les cas où la loi en dispose autrement* (…) » la preuve libre est confrontée à certaines exceptions citées par le Code civil. L'une de ces exceptions légales concerne justement la preuve des actes juridiques d'une valeur excédant 1500€, qui doit nécessairement être administrée au moyen d'une preuve littérale, c'est-à-dire par un écrit[899] dont la valeur probante est parfaite comme mentionné (dès lors que son intégrité peut être retracée et établie). Selon le mode de preuve utilisé, l'effet sur le juge peut varier dans les cas où la preuve est libre. Il est donc essentiel de classer la technologie blockchain dans l'une des catégories existantes en droit de la preuve français afin de déterminer la force probante d'une preuve numérique sur une blockchain. Si une 'preuve blockchain' est considérée comme une preuve parfaite, le juge sera tenu de la prendre en compte. Toutefois, si elle est considérée comme une preuve imparfaite, le juge pourrait décider de ne pas la prendre en compte en fonction des circonstances[900]. Il convient de souligner que le droit français a été précurseur en admettant la preuve

[897] Art.1363 à 1386-1 du Code civil, modifié par l'Ordonnance n°2016-131 du 10 février 2016.
[898] Art. 9 du Code de procédure civil : « Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention ».
[899] Cet écrit doit nécessairement constituer un acte authentique (art. 1369 du Code de procédure civil), un acte sous signature privé (art. 1372 du Code civil) ou bien un acte sous seing privé contresigné d'un avocat (*v.* l'Acte d'avocat).
[900] Un juge (ou un expert judiciaire) se doit de comprendre la gouvernance d'une blockchain afin d'interpréter la valeur probatoire d'une inscription de donnée(s) en son sein. Cette même gouvernance qui est propre à chaque catégorie de blockchain est en mesure d'affecter l'intégrité d'une inscription, d'en modifier son contenu et son existence.

dématérialisée[901] depuis plus de vingt ans[902]. Cette avancée législative et technologique a permis d'accorder une force probante équivalente entre une preuve sur un support matériel (signature manuscrite) et une preuve sur un support dématérialisé (signature numérique). A cet égard, la dématérialisation également possible grâce à la blockchain ne représente pas une limite en matière d'admissibilité en tant que mode de preuve, conformément à l'article 1316-1 de la loi du 13 mars 2000 sur l'adaptation du droit de la preuve aux technologies de l'information. Pourtant, la reconnaissance de la preuve électronique est soumise au respect de certaines spécificités irréductibles[903], qui peuvent influencer la force et la conviction d'une preuve électronique et intangible par rapport à une preuve matérielle et tangible. Parce que la preuve d'une information inscrite sur une blockchain est électronique, elle doit en principe être recevable par toute juridiction, mais cette recevabilité juridique ne doit pas être confondue avec l'assurance d'une reconnaissance juridique. Pour qu'un document électronique puisse produire efficacement ses effets juridiques, le juge doit nécessairement être convaincu de l'intégrité du système informatique utilisé et donc comprendre en premier lieu les mécanismes et les rouages[904]. Parce que ces débats sur le fond ainsi que sur la forme d'une preuve électronique sur blockchain sont complexes, le règlement eIDAS stipule qu'une présomption de validité de ladite preuve existe, dès lors que l'horodatage sous une forme électronique satisfait aux exigences d'un horodatage électronique dit qualifié[905].

En complément des propos précédents, il semble légitime de s'attarder sur le rôle du notaire qui est un officier ministériel indispensable à la production de preuves parfaites grâce aux actes authentiques qu'il délivre. La force probante d'un acte notarié ne concerne que les actes que le notaire a personnellement accomplis ou bien personnellement constatés. En pratique, le notaire est un tiers de confiance étatique, qui régit les relations entre l'État et les contribuables. Les actes notariés ont une force probante irrésistible pour un juge et ne s'appliquent qu'aux actes que le notaire a personnellement accomplis ou constatés. En tant que tiers de confiance étatique, les notaires régissent les relations entre l'État et les citoyens, formant en quelque sorte une 'infrastructure humaine et institutionnelle' en raison de leur rôle règlementé. Cependant, contrairement à une infrastructure blockchain, les notaires garantissent l'équilibre social et juridique des conventions entre des parties, ce qui confère une valeur probante supérieure aux actes associés. Même en comparaison avec une preuve imparfaite basée sur une blockchain et associée à une convention sur la preuve, un acte notarié authentique reste la preuve la plus

[901] Au visa de l'art. 46 du Règlement européen eIDAS dispose que « L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique ».
[902] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *v*. Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[903] Art. 1366 du Code civil dispose que « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».
[904] Grâce à un expert judiciaire ou un Commissaire de justice qui intervient pour soumettre un rapport technique détaillé et simplifié au juge le cas échéant.
[905] V. *infra*, II, Titre 1, 2.1.1.1

fiable, car il ne peut être contesté qu'en cas d'inscription en faux, tandis qu'une convention sur la preuve n'a qu'une présomption de fiabilité simple qui peut être contestée. Ce type de convention reste ainsi limité dans ses conditions et sa portée[906]. Par exemple, lorsqu'il y a l'intervention d'un juriste dont la profession est règlementée (notaire, commissaire de justice, avocat)[907], une convention sur la preuve numérique peut paraître excessive et disproportionnée face à la force authentique d'un acte délivré par un notaire. Néanmoins, l'origine des litiges impliquant des transactions et preuves sur blockchain concerne aujourd'hui principalement des évènements qui n'impliquent souvent pas de notaires, mais pour l'instant plutôt des avocats. Ainsi, l'utilisation de conventions sur la preuve pour ces actes courants et sous seing privé semble une solution temporaire que les utilisateurs des blockchains publiques peuvent privilégier en attendant que certains législateurs reconnaissent éventuellement la présomption de fiabilité de certaines blockchains publiques.

Par conséquent, le notaire restera en monopole de la preuve parfaite, un « Graal probatoire »[908] que la technologie blockchain ne peut pas atteindre en raison de son caractère binaire et peu flexible. Pour certains technophiles avisés, quelques blockchains publiques comme Bitcoin voire Ethereum représentent pourtant des sources de vérités numériques jugées inalénables et donc proche de ce « Graal probatoire », dans son acceptation en réalité surtout informatique. Dans cette perspective, la blockchain ne vise pas à remplacer les rôles clés des notaires, mais plutôt à fournir une nouvelle infrastructure informatique que les notaires peuvent utiliser pour certifier certains actes de manière plus efficace. Pour donner une valeur probante à une information disponible sur une blockchain, un fait juridique peut être couplé à une convention sur la preuve numérique[909], à condition que ce mode d'inscription en blockchain soit celui retenu dans cette convention. Cependant, ce cadre juridique est assez paradoxal : si la technologie blockchain nécessite toujours une convention sur la preuve, cela suggère ainsi qu'elle ne possède pas intrinsèquement, c'est-à-dire cryptographiquement, une valeur probante au regard de ces textes. Depuis le 16 juin 2020[910], les Notaires du Grand Paris (les Présidents des 5 Chambres des Notaires franciliennes) ont signé une « Politique de Confiance de la Blockchain Notariale - BCN » et mis en place l'Autorité de Confiance numérique notariale des Notaires du Grand Paris afin de permettre la fourniture de services notariaux basés sur une technologie blockchain fermée. Une blockchain privée

[906] Art. 4 de l'ordonnance n°2016-131 du 10 février 2016 : « 1°Art. 1356. - Les contrats sur la preuve sont valables lorsqu'ils portent sur des droits dont les parties ont la libre disposition. 2° Néanmoins, ils ne peuvent contredire les présomptions irréfragables établies par la loi, ni modifier la foi attachée à l'aveu ou au serment. Ils ne peuvent davantage établir au profit de l'une des parties une présomption irréfragable. », v. également art. 6 du Code civil : « On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs. ».
[907] L'HERMITE Marie et STENNE Paul, « La preuve, la blockchain et les professions réglementées », *Op. cit.*, p. 8, « Ainsi l'AMF a considéré que l'intervention d'un tiers tel qu'un avocat, huissier ou notaire pouvait constituer une garantie de fiabilité, d'opérabilité et d'efficacité pour assurer le suivi et la sauvegarde de fonds issus d'ICO ».
[908] Cour de cassation, Colloques sur la blockchain et la Preuve, 27 février 2020, Augustin AYNES (modérateur), Bertrand BONNEAU (intervenant), Didier FORNONI (intervenant) et al.
[909] Art. 1356 du Code civil : « Les contrats sur la preuve sont valables lorsqu'ils portent sur des droits dont les parties ont la libre disposition. Néanmoins, ils ne peuvent contredire les présomptions irréfragables établies par la loi, ni modifier la foi attachée à l'aveu ou au serment. Ils ne peuvent davantage établir au profit de l'une des parties une présomption irréfragable. ».
[910] Notaire du Grand Paris, « Présentation de la Blockchain Notariale (BCN) », Dossier de presse du 7 juillet 2020, consulté le 27/04/2021.

a ainsi été intégrée à la plateforme IntraNotaires[911] pour permettre à la profession de se familiariser avec cette technologie et à ses différents cas d'usage concrets pour la profession[912]. Parallèlement, d'autres initiatives hybrides portées par des commissaires de justice existent, comme la solution développée par la société Smart Preuve[913] qui permet de générer puis d'horodater des attestations ou bien des constats[914] en ligne réalisés par des Commissaires de justice grâce à une application mobile intuitive et reliée à une blockchain également fermée. Toutefois, les constats en ligne (avec ou sans une blockchain) peuvent souffrir de certaines lacunes en matière de reconnaissance et de valeur juridique. Un Commissaire de justice ne va en effet pas constater sur une application numérique comme Smart Preuve le contenu d'une photo en ligne, mais seulement sa bonne réception et son existence. Effectivement, pour qu'un constat réalisé par un Commissaire de justice soit valable, ce dernier doit impérativement être présent physiquement lors dudit constat[915]. Bien que cette solution développée par la société SmartPreuve ne bénéficie pas d'un Graal probatoire, elle contribue toutefois à rendre accessible et intuitif le droit auprès du grand public, tout en représentant une alternative parfois bénéfique en matière de précontentieux et pour certains litiges du quotidien. Pour le moment, il semble que les informations enregistrées dans une blockchain publique soient considérées nativement comme des preuves imparfaites, c'est-à-dire dont la valeur probatoire peut être simlement remise en question en apportant une preuve contraire[916]. En effet, selon les textes en vigueur, ces informations ne peuvent pas être considérées comme un aveu judiciaire ou comme un serment décisoire, ce qui laisse comme seul moyen de preuve parfaite possible la preuve écrite sous la forme d'un acte authentique ou d'un acte sous seing privé (convention sur la preuve). Selon l'article 1316 du Code civil, la preuve par écrit est constituée d'une suite de signes ou symboles ayant une signification intelligible, quel que soit leur modalité de transmission ou leur support. Cependant, en utilisant la technique de hachage cryptographique[917] couramment utilisée pour la certification de

[911] Pour plus d'informations, consultez cette plateforme à l'adresse suivante

[912] L'HERMITE Marie, STENNE Paul, « La preuve, la blockchain et les professions réglementées », consulté en ligne le 28/12/2021, p.2., « les notaires et les huissiers ont choisi d'innover et se présentent ainsi tel un notaire ou huissier 'augmenté' (par la blockchain) ».

[913] Cette solution est à l'initiative de 70 Commissaires de justice français, pour plus d'informations consultez l'adresse suivante

[914] Il convient ici de faire la distinction entre un constat et une attestation qui est réalisée par un commissaire de justice, car leur valeur juridique respective diffère. Contrairement à une attestation, un constat permet d'obtenir un procès-verbal soit une preuve irréfutable et incontestable.

[915] LAHER Rudy., « La numérisation des activités de l'huissier de justice », in *Cah. Droit Sci. Technol.*, PUP, 2020, consulté en ligne le 15 janvier 2022, « La protection des droits des justiciables de même que l'impératif pratique d'une présence physique justifient cet état de fait. ». Un constat doit donc impérativement être réalisé sur place par un commissaire de justice.

[916] En référence au caractère irréfragable d'une preuve parfaite dont la charge ne peut être renversé, *v.* Art.1354 du Code civil : « La présomption que la loi attache à certains actes ou à certains faits en les tenant pour certaine dispense celui au profit duquel elle existe d'en rapporter la preuve. Elle est dite simple, lorsque la loi réserve la preuve contraire ; elle est dite irréfragable lorsqu'elle ne peut être renversée. ».

[917] Cette empreinte cryptographique (*hash*) peut être issue d'un « *arbre de Merkle* » ou « *arbre de hachage* » (« *Merkle Root* »), inventé par *Ralph Merkle* en 1979. Un *arbre de Merkle* est un outil cryptographique qui permet de consolider de grandes quantités de données en un seul *hash* unique. Ce *hachage* unique (*Merkle Root*) agit comme un sceau cryptographique qui résume un ensemble de données saisies. Les *arbres de Merkle* permettent à des utilisateurs de vérifier si des contenus spécifiques ont été inclus dans un ensemble particulier de données « *scellées* ». Dans le cas de Bitcoin ils permettent de réaliser un *hash* unique qui contient l'ensemble des transactions d'un bloc. Dans le cas d'une blockchain, le processus de *hachage* est effectué à partir du contenu du bloc, c'est-à-dire le *hash* du bloc précédent qui contient un certain nombre de transactions et permet un horodatage automatique de chacune de ces dernières. Le *hash* d'un ensemble de données peut ainsi être comparé à une *empreinte numérique* précise et unique. Une *fonction de hachage* est dite **«** *à sens unique* **»** : elle est conçue de sorte que

documents avec la technologie blockchain, il semble que cette méthode ne réponde pas à la notion « *d'intelligibilité* » requise par cet article. En d'autres termes le caractère dématérialisé de la technologie ne pose pas de problème, la difficulté réside dans la capacité d'une blockchain à répondre à ce critère d'intelligibilité, bien qu'elle puisse être interprétée par un juge ou par un expert judiciaire, comme supposé précédemment. Pour rappel, en informatique, la finalité d'une blockchain n'est pas de stocker des documents directement en son sein (dans ses blocs de transactions)[918], mais plutôt de les certifier avec une empreinte numérique unique, inviolable et non répudiable. Ainsi, un identifiant numérique ou « hash »[919] ancré dans une transaction blockchain ne peut pas être considéré comme un document électronique, c'est-à-dire se voir doté d'une valeur juridique. En droit, la blockchain ne constitue donc pas un registre de preuves juridiques, mais un outil de preuves cryptographiques, imparfait au regard du droit sans une convention sur la preuve. Également, si une inscription dans une blockchain n'est pas réalisée conformément aux conditions requises par la loi[920], elle ne s'imposera pas au juge en raison de sa libre appréciation souveraine. En pratique, les actes sous seing privé contiennent généralement les signatures électroniques et cryptographiques des parties impliquées[921]. À l'avenir, il est possible que les blocs de transactions contenant la signature électronique des parties et respectant la formalité du double original et de la mention manuscrite soient considérés comme des actes constitutifs d'une preuve littérale sous seing privé, à condition que cela soit conforme aux règles en vigueur[922]. Pour l'heure, une inscription blockchain ne peut donc ni constituer un acte sous seing privé ni un acte authentique, il s'agit donc d'une preuve imparfaite qui pourrait être l'équivalent d'un témoignage[923]. En effet, ce rapprochement semble pertinent dans le sens où une transaction blockchain s'inscrit informatiquement dans un bloc, dont les témoins ici des nœuds validateurs ont la charge de la validation de nouveaux blocs, de telle sorte que chaque transaction soit validée individuellement puis communément par ces

l'empreinte et le *hash* produits soient impossibles à inverser pour retrouver son information initiale (du moins avec les puissances de calcul disponibles aujourd'hui). En conséquence, modifier le contenu d'un bloc suppose de recalculer les *hash* de tous les blocs qui le suivent. Cette caractéristique des fonctions de hachage rend toute modification du contenu d'un bloc immédiatement visible dans les blocs suivants, même si cette modification est minime : cette empreinte numérique constitue une preuve cryptographique – et non légale – d'intégrité pour la donnée initialement « *hachée* » par cet algorithme. V. également Annexe 6, Focus 1.

[918] V. Annexes 3 et 6.

[919] Pour rappel, le « *calcul des sommes de contrôle* » ou « *hashing* » est une technique qui consiste à créer une empreinte unique reliée à une information/donnée. De cette façon, une donnée correspond strictement à une suite de chiffres et de nombres uniques, et un nombre correspond strictement à cette information (consultez le site internet suivant pour transformer une donnée telle qu'un ou plusieurs mots en un ou plusieurs *hash uniques*). En partageant ces *hash* et identifiants numériques pseudo-anonymes à travers un réseau informatique, la blockchain assure leur résilience au changement : toute modification de l'information changerait la somme associée, et serait rejetée par les validateurs dudit réseau blockchain.

[920] Art. 1367 du Code Civil : « […] Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. […] ».

[921] Art. 1367 du Code civil : « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire. ».

[922] Art. 1367 du Code civil : « […] Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie […] ».

[923] Art. 10 du Code civil : « Chacun est tenu d'apporter son concours à la justice en vue de la manifestation de la vérité. […] ».

témoins informatiques automatisés[924]. Il semble important de souligner qu'une blockchain permet de certifier l'intégrité d'une donnée et d'une information, en aucun cas sa véracité, qui nécessiterait une vérification formelle et parfaite, entre autres par un professionnel de droit comme susvisé. En ce sens, la réalité du fait dont il est rendu compte dans une blockchain dépend ex ante de celui qui l'a inscrit, c'est-à-dire de celui qui la dépose en son sein. Nous pouvons en conclure que la valeur probante qu'accordera un juge à une information inscrite dans une blockchain dépendra ultimement de ses conditions de dépôt, d'inscription, mais aussi de restitution[925]. Plus spécifiquement au regard des attributs d'identité numérique décentralisée (IND) étudiés en seconde partie[926], l'utilisation d'une solution d'identité numérique auto-souveraine (INAS)[927] ne semble pas pouvoir garantir la production de preuves parfaites en raison du principe d'autonomie de la preuve. Selon ce principe, la validité d'une preuve ne peut dépendre d'éléments non vérifiables, même si ces éléments sont supposés par une communauté numérique comme cela est le cas pour une INAS, ce qui n'est pas suffisant pour garantir ce principe d'autonomie sur le plan juridique. Par conséquent, une attestation vérifiable peut être considérée comme un début de preuve par écrit en droit civil français, sous réserve que l'identité de la personne émettrice soit clairement établie. À court terme, il est probable que l'identité auto-souveraine devienne hybride[928], c'est-à-dire qu'elle devienne partiellement centralisée par des fournisseurs d'identité. Cette évolution mixte (2.0 et 3.0) vise à garantir que les mécanismes de preuve cryptographiques tels que les attestations vérifiables (VC)[929] et les identifiants décentralisés (DID)[930] soient conformes aux schémas d'identité numérique nationaux et communautaires, en vertu d'eIDAS-1 et d'eIDAS-2[931].

Afin de répondre à notre problématique initiale, il convient tout d'abord de souligner l'intérêt et la pertinence technique d'une blockchain ouverte dans les cas où la preuve est libre : une preuve blockchain constitue un support électronique recevable jusqu'à preuve du contraire. Néanmoins, cet outil au service de la preuve ne caractérisera pas un Graal probatoire sans amendements législatifs adéquats et dédiés.

---

[924] Il est fait référence aux nombreux ordinateurs/validateurs des blocs de transactions de ces réseaux décentralisés, qui dans un certain sens, *témoignent* chacun, des transactions qui leurs sont communiquées, jusqu'à former ensemble un *témoignage commun* et *consensuel*, c'est-à-dire formant un *consensus* concernant les transactions légitimes à enregistrer ou à rejeter dudit réseau. Il est important de souligner que chaque blockchain et chaque consensus peut varier, ce qui remettrait en question cette même interprétation.

[925] Il est fait référence aux différences de restitution qui peuvent exister selon le type de blockchain publique, privée ou hybride dont il est question. Ces variantes technologiques de même que le contexte de leur utilisation peut ainsi faire sensiblement évoluer les techniques d'inscription, de vérification et de restitution des informations ancrée sur ladite blockchain.

[926] V. *infra*, II, Titre I, Chap. 1

[927] V. *infra*, II, Titre I, 1.4

[928] L'identité auto-souveraine (INAS) prône une gestion totale par l'utilisateur de son identité, y compris concernant l'embarquement et l'identification numérique préalable d'une personne. L'INAS est ainsi particulièrement disruptive et sera confrontée – à court et moyen termes - aux schémas d'identité numérique centralisés : elle devra ainsi s'y conformer et donc le concept de *Self Sovereign Identity – SSI* purement décentralisée laissera place au concept d'identité distribuée (plutôt hybride soit à la fois 2.0 et 3.0), privilégié dans cette recherche.

[929] V. *infra*, II, Titre 1, 1.3.1.2

[930] V, *infra*, II, Titre 1, 1.3.1.1

[931] V, *infra*, II, Titre 1, 2.1.1

Dans l'espoir qu'une telle prise de conscience se reproduise[932], une intervention du législateur serait-elle souhaitable et pertinente pour reconnaître le potentiel probatoire d'une information ancrée sur une blockchain publique ? Remarquons que le législateur est déjà intervenu en ce sens pour la propriété des titres de société non cotée, cela résulte d'une ordonnance du 8 décembre 2017[933] et d'un décret du 24 décembre 2018[934] où il a adopté une réforme technique consistant à faciliter la preuve de compte titre enregistré sur une blockchain. Cette réforme a entre autres permis de considérer la technologie blockchain dans son ensemble comme un outil technique au service de la preuve de la propriété des titres, sans pour autant modifier le régime juridique de propriété des titres en vigueur. Grâce à cette intervention législative, la blockchain a une valeur probante égale au registre papier pour ce qui est de la propriété des titres non cotés (et non pas pour d'autres types de transactions blockchains à vocation non financières). En ce sens, cette approche technologiquement agnostique du législateur explique peut-être le statu quo actuel concernant le droit de la preuve à l'aune de la technologie blockchain : afin de ne pas braver cette neutralité technologique le législateur préfère observer si l'adoption technologique de la blockchain concernera plutôt des registres publics, privés ou bien hybrides (tout en sachant que le Règlement eIDAS-2 tranche en faveur des blockchains privées et hybrides comme suggéré plus loin)[935]. Le législateur français n'a donc pas tranché en faveur de spécifications et de garanties techniques précises pour l'une ou l'autre de ces variantes technologiques. En effet, le ministère de la Justice a décidé - en coulisse - de ne pas légiférer pour attribuer une valeur probante à une preuve blockchain. Comme souvent, ce dernier privilégie la formation d'une jurisprudence comme source de droit, ce qui implique que les professionnels du secteur judiciaire méconnaissent cette technologie pourtant au service de la preuve. Certains pays comme Monaco (2017)[936] puis quelques années plus tard l'Italie (2019)[937], ont déjà légiféré sur ce sujet en vue de favoriser l'innovation tout en acceptant le plein potentiel probatoire inhérent aux technologies blockchains (certes relatif dans ses versions publiques mais conformes au droit de la preuve dans ses versions hybrides ou privées). Depuis septembre 2022 un nouveau décret italien permet - en coordination avec les entreprises et les centres de recherche publics ou privés - de solliciter des subventions (enveloppe totale de 45 millions d'euros) pour mener à bien des projets de recherche et d'innovation technologique concernant la technologie blockchain[938]. A ces égards, il s'agit d'œuvrer à une harmonisation européenne de la preuve recourant à la technologie blockchain comme semblent le soutenir progressivement de plus en plus de juristes : « *à partir du moment où il y a un*

[932] Il est fait référence à la clairvoyance législative dont a fait preuve le législateur français concernant loi du 13 mars 2000 portant l'adaptation du droit de la preuve aux technologies de l'information. En effet, le législateur a su anticiper l'importance technique que connaît aujourd'hui la signature numérique et plus généralement le digital dans notre quotidien.
[933] L'Ordonnance n°2016-520 du 28 avril 2016 (art. L.223-12 & L.223-13 du CMF), en application de la loi Macron du 6 août 2015, confère à la technologie blockchain une première reconnaissance légale en droit français, disponible en ligne
[934] Décret n°2018-1225 portant diverses mesures relatives aux contrats de la commande publique.
[935] V. *infra*, II, Titre 1, 2.1.1.1.a
[936] L'Etat de Monaco reconnait une présomption de caractère fiable de toute inscription sur une blockchain.
[937] Loi n° 12/19 du 11 janvier 2019 relative au soutien et à la simplification des entreprises et de l'administration publique, entrée en vigueur en Italie le 13 février 2019. Elle a permis de renforcer le caractère juridiquement contraignant de l'horodatage électronique effectué au moyen de technologies blockchain. V. BARBET-MASSIN Alice, *in Revue Lamy droit de l'immatériel* (Wolters Kluwer), n°157, mars 2019, p. 40-43.
[938] « Blockchain e intelligenza artificiale : da settembre gli incentivi », 5 juillet 2022, in *mise.gov.it*. Disponible en ligne

protocole cryptographique, on considère que la preuve est avancée. Mais tant qu'un législateur français ou européen n'aura pas dit qu'une preuve par blockchain équivaut à une preuve avancée ou une preuve simple, on restera dans le flou. »[939].

2.9 Une identité en ligne universelle 3.0 avec Proof of Humanity (PoH)

Le 16 avril 2021, Kleros s'est engagé sur la voie de l'identité numérique auto-souveraine (INAS), étudiée plus loin[940], avec le lancement d'un autre projet 3.0 nommé « *Proof of Humanity – PoH* ». Il s'agit d'un « *système combinant des réseaux de confiance* (…) *et la résolution de conflits pour créer une liste d'humains à l'épreuve de l'attaque Sybil* »[941]. Le concept de Proof of Humanity vise à établir un système fiable de preuves d'existence numériques pour les utilisateurs en combinant la vérification sociale et la soumission de vidéos sur une plateforme décentralisée. Kleros, qui a développé une expertise dans la justice numérique décentralisée comme mentionné, utilise cette expertise pour offrir une solution de preuve d'identité numérique décentralisée à tous les internautes. La problématique de la vérification d'identité est un enjeu commun dans l'écosystème des crypto-actifs et sur Internet, car certains utilisateurs malveillants peuvent créer plusieurs comptes et portefeuilles numériques de manière pseudo-anonyme pour tenter de recevoir des récompenses plusieurs fois, influencer des votes, écrire de fausses critiques, etc. Proof of Humanity répond à cette problématique (« Sybil »)[942] en offrant une vérification distribuée de l'identité numérique (IND)[943], fiable et sécurisée, que les utilisateurs peuvent utiliser pour s'authentifier auprès de services tiers numériques tels que des réseaux sociaux, des blogs et des plateformes financières. Cette solution tente ainsi de résoudre la difficulté quotidienne qu'ont des personnes physiques à prouver leur identité en ligne. PoH est encore à ses débuts, mais plusieurs cas d'usage ont déjà été envisagés. Tout d'abord (i), la mise en place d'un revenu universel en crypto-actifs est proposé. Une fois qu'une personne a déposé son identité sur la plateforme PoH et qu'elle a été vérifiée par d'autres utilisateurs de confiance, elle reçoit le droit de percevoir un revenu universel sous la forme d'un jeton numérique, l'« *Universal Basic Income - UBI* ». Grâce à cette solution déployée en 2021, chaque être internaute dont « l'humanité » est vérifiée reçoit 1 UBI par heure (soit 720 UBI par mois ce qui est équivalent à environ 108 euros par mois à date de 2021). Bien que les UBI soient échangeables, leur valeur et leur prix restent en phase exploratoire et peuvent donc varier considérablement. Cette distribution de (crypto)revenus est gratuite et partiellement décentralisée. Dans un second temps (ii), la vérification de la solvabilité d'un crypto-investisseur serait possible grâce à la plateforme PoH. En effet, de nombreux utilisateurs et professionnels de la crypto-économie recourent actuellement à l'utilisation

[939] MAGNIER Véronique, « L'Édition de l'université Paris-Saclay été 2021 », éd. 2021, numéro 16, p. 10. Disponible en ligne
[940] V. *infra*, II, Titre I, 1.4
[941] Kleros, « Welcome to Proof of Humanity », traduction libre de l'anglais, 2021, YouTube, disponible à l'adresse suivante
[942] V. partie précédente, *v.* également Annexe 6, Focus 1.
[943] Tout internaute peut d'ores et déjà procéder à son enregistrement sur le site et la plateforme PoH afin d'obtenir une forme d'identité numérique auto-souveraine et percevoir un (crypto)revenu universel. Pour cela, consultez l'adresse suivante

de prêts en crypto-actifs à titre d'investissement ou encore de spéculation (pour se surexposer au marché). Ces crédits en crypto-actifs pour l'instant hautement risqués sont généralement proposés par des plateformes d'échanges spécialisées[944]. Ces dernières ont, comme étudié dans les parties précédentes, des obligations d'identification, mais souhaitent également vérifier de façon systématique que leurs clients et utilisateurs sont bien solvables. Par conséquent, PoH permet à ces bourses et plateformes d'échanges de s'assurer qu'une personne est bien qui elle prétend être (vérification d'identité civile) et qu'elle possède bien ce qu'elle prétend posséder (vérification de solvabilité). Finalement (iii), de nombreuses communautés en ligne revendiquent leurs appartenances numériques, un besoin de reconnaissance sociale en vogue dans la crypto-économie où foisonnent les projets, communautés et crypto-actifs de différentes natures et fiabilités. Pour lutter contre les attaques Sybil, PoH permet aux porteurs de projets d'engager des communautés d'utilisateurs vérifiées[945] et uniques de manière supposée plus ciblée et efficace (que la vérification d'identité numérique 2.0 étudiée auparavant). Le projet expérimental de PoH repose donc sur la vocation d'un haut degré de décentralisation ainsi que sur la volonté d'ouvrir et d'émanciper l'identité numérique des personnes, en proposant une identité universellement accessible sur Internet. Finalement, cette plateforme d'agrégation 3.0 des identités numériques ouvre progressivement à certains droits numériques tels que le revenu universel mentionné ou encore un droit de vote destiné à la gouvernance de ce protocole qui ambitionne de devenir un bien commun numérique. En théorie, le fonctionnement de PoH est directement géré par ses utilisateurs grâce à une DAO qui respecte un principe de démocratie sans tiers de confiance : « *une personne possède un vote* »[946]. En somme, PoH représente l'une des premières solutions informatiques - derrière « DID4ALL » initié en 2019[947] - permettant de générer et de vérifier des preuves d'existences numériques de façon distribuée et au service des internautes et de leurs droits numériques[948]. PoH est un système accessible et ouvert qui repose sur une transparence ainsi que sur un engagement communautaire supposé croissant de ses utilisateurs. Il est possible de résumer le potentiel prospectif de ce système ainsi :

[944] Il est important de différencier les plateformes centralisées des plateformes décentralisées. Les premières agissent simplement en tant qu'intermédiaires financiers centralisés (PSCA), tandis que les secondes fonctionnent de manière autonome et partiellement décentralisée (DeFi), grâce à l'utilisation de technologies telles que des AEC et des DAO

[945] Reposant sur une nouvelle couche technologique nommée « *token curated registry – TCR* » ou « *registre de jeton sécurisé* ». Conceptuellement, le *TCR* est un registre en ligne d'humains (d'informations telles que des photos, des vidéos, des données biométriques comme la voix, etc.) permettant de résister aux attaques *Sybil*. Informatiquement, pour s'inscrire sur une *liste décentralisée*, un demandeur achète le jeton natif (« UBI Tokens ») et dépose une demande en ligne. Les détenteurs de jetons peuvent contester une candidature (grâce à Kleros) s'ils estiment qu'elle n'a pas sa place sur la liste. Lorsqu'une contestation est lancée, les détenteurs de jetons peuvent voter pour accepter ou rejeter la demande (leur vote est proportionnel au nombre de jetons qu'ils possèdent). Si la candidature est rejetée, le dépôt est perdu : il est partagé entre le vérificateur à l'origine d'une demande de vérification et les détenteurs de jetons qui ont voté pour le rejet. Si la demande est acceptée, le principe précité est inversé.

[946] Disponible depuis 2022, cette DAO permet de définir les orientations techniques et sociales de cette solution. Consultez son fonctionnement à l'adresse suivante

[947] V. *infra*, II, Titre2, 2.1

[948] V. *infra*, II, Titre 1, 2.2

Facteurs clés de succès (FCS) pour PoH	Court terme	Moyen terme	Long terme
Conformité juridique et reconnaissance politique	×	× ou ~	~
Reconnaissance puis adoption sociale[949]	✓ ou ~	✓ ou ~	✓
Reconnaissance puis adoption informatique (Ethereum[950], UBI/TCR, DAO)	~	✓ ou ~	✓

Ce tableau prospectif suggère qu'une reconnaissance juridique et politique à moyen terme serait indispensable pour favoriser l'adoption sociale et informatique de la solution d'identité numérique auto-souveraine (INAS) proposée par PoH. Cependant, il convient de noter que PoH n'a actuellement qu'une reconnaissance informatique partielle et aucune reconnaissance légale en raison de son probable non-respect à de multiples dispositions du RGPD, du Règlement TFR et eIDAS, ainsi qu'au DSA et DMA mentionnés en amont. Bien que PoH permette théoriquement de fournir une preuve d'existence numérique à chaque personne, en pratique, cela demeure une utopie phygitale comparée à d'autres systèmes d'identité numérique hybrides (2.0) encadrés par le droit ou par une autorité publique (*v.* projet « DID4ALL »[951]). PoH est pour le moment un système informatique immature et sujet à de nombreuses dépendances économiques et informatiques, pouvant impliquer des failles comme cela a été constaté en 2022 pour son projet voisin Kleros[952]. A ce titre, si les défis informatiques demeurent légions en 2021 pour une telle solution d'identité numérique 3.0, force est de constater que l'imbrication entre la solution Kleros et PoH est informatiquement et surtout commercialement pertinente, même si largement soumise à questionnement et interprétation sur le plan juridique, ne serait-ce que sur la pertinence (crypto)économique de mêler des identités numériques auto-souveraines (INAS) à une justice numérique décentralisée (Kleros).

[949] Le 15 mars 2023, 18.322 internautes sont enregistrés et vérifiés sur la plateforme PoH, accessible à l'adresse suivante. Depuis son lancement PoH dénombre une majorité d'utilisateurs en Amérique du Sud.
[950] V. Annexe 6, Focus 2.
[951] V. *infra*, II, Titre2, 2.1
[952] *Op. cit.* « DAOs are not corporations: where decentralization in autonomous organizations matters », consulté le 20 septembre 2022 à l'adresse suivante : « Le processus décisionnel de la Cour, fondé sur des incitations, est, selon toute apparence, corrompu par un seul développeur qui possédait un intérêt économique trop important et à la hauteur de 25 % dans les tribunaux [Kleros] ».

Conclusion de la première partie

Notre étude de l'identité montre que cette notion a connu de nombreuses définitions en sciences sociales. Ici observée et relativement circonscrite à travers ses champs philosophiques, juridiques et sociaux, l'identité demeure pourtant ductile et le plus souvent insaisissable pour ses observateurs d'attention moyenne. Si le droit contribue à fixer certaines facettes indispensables de l'identité des personnes, l'identité doit en réalité être systématiquement (re)contextualisée pour être appréhendée en fonction des objets et des sujets qu'elle traite autant que ceux qui l'alimentent. En comprenant la chronologie de l'informatique 1.0, puis des services en ligne et des systèmes d'identité numérique 2.0, nous sommes en mesure de déterminer les progrès technologiques et sociaux accomplis ainsi que certains défis informatiques et juridiques à relever, et enfin certaines opportunités et besoins technologiques dernière génération liés à l'émergence de systèmes de gouvernance 3.0, supposés plus transparents qu'auparavant. L'analyse sémantique et segmentée des technologies blockchains publiques, privées et hybrides, ainsi que de leurs principales briques technologiques respectives, met en exergue de nouveaux fondements informatiques, au regard d'un Internet présumé plus souverain, sûr et respectueux des droits des internautes. Dans ce contexte, certaines propositions de règlementations européennes - à l'heure de ces écritures votées mais non promulguées - se concentrent progressivement sur ce phénomène revisité de la décentralisation informatique 3.0. Il revient à tous les acteurs de la société tels que les juristes, les institutions et les gouvernements de prendre connaissance avec patience, pragmatisme et expertise des enjeux, des promesses et des défis liés à ces nouvelles technologies afin de réinventer au moins partiellement certains de nos modèles de gouvernances phygitaux qui manquent parfois de transparence en ligne.

II/ La blockchain et l'identité décentralisée au service du droit et de l'identité

Titre 1 : L'hypothèse d'une identité cryptographique universelle source de droits renforcés

Chapitre 1 : L'émergence d'une nouvelle identité décentralisée voire universelle pour l'humanité

1.1 Introduction contextuelle et sémantique pour une identité numérique de troisième génération

Pour rappel, la notion d'identité n'a jamais été aussi centrale au sein de nos sociétés en raison du fait que plus d'un milliard de personnes éprouvent aujourd'hui des difficultés à prouver leur existence légale[953]. Comme nous l'avons vu, les titres d'identité deviennent digitaux et font progressivement naître une identité régalienne en ligne. L'identité personnelle se compose d'une infinité d'attributs personnels fixes (couleur des yeux, la voix[954]), variables (couleur des cheveux), mais aussi racines (prénom et nom patrimoniaux) et étendus (expérience professionnelle, diplômes). Le cadre de confiance pancanadien (CCP) décrivait en 2016 une distinction entre les identités appelées « *fondatrices* » de celles appelées « *contextuelles* »[955]. Dans le cadre de nos identités numériques actuelles 2.0, ces innombrables attributs et données d'identité se trouvent généralement sous le contrôle d'organisations et de serveurs externes à l'individu auxquels ils se réfèrent. Ainsi, l'identité numérique 2.0 soulève régulièrement diverses problématiques parce que fragmentée entre différentes organisations, bien souvent privées, peu interopérables ou accessibles, onéreuses et complexes à sécuriser. Dans certains cas, sa gestion est opaque au détriment des utilisateurs et de leurs données personnelles parfois commercialisées en toute impunité en ligne ou hors ligne. L'enjeu d'une identité numérique de confiance, partiellement fondée sur certaines technologies blockchains, se fait jour et s'ouvre aux entreprises, aux citoyens ainsi qu'aux États. Elle permet de façon inédite de conférer une valeur légale et cryptographique aux transactions d'identité auxquelles les acteurs feront légitimement confiance, dès lors qu'elles seront initialement dérivées de titres d'identité officiels. Plus qu'une simple technologie sur un marché historique, elle représente un nouveau concept technico-social tant pour l'identité des personnes physiques ou morales que pour l'Internet des objets connectés (IdO)[956]. L'identité décentralisée ne possède pas encore de définition stable, il s'agit pour l'heure d'un ensemble de principes et de concepts. En 2022, cinquante experts du secteur semblent unanimes pour considérer qu'elle se développe plus rapidement qu'Internet

[953] DESAY Vyjayanti, DIOFASI Anna, « The global identification challenge: Who are the 1 billion people without proof of identity? World Bank Blogs », 25 avril 2018, disponible à l'adresse suivante
[954] Cour d'appel de Paris, 28 mai 2014, RG n°12/20952, il existe peu de décision concernant la protection de la voix, un « *attribut de la personnalité* » invoqué en l'espèce à titre de liberté d'expression pour justifier l'enregistrement d'un contrôle fiscal (aff. David Guetta qui a utilisé un site proposant de synthétiser la voix d'une personne).
[955] MONTANA Kent, « L'identité numérique dans le 21ème siècle », 25 juin 2021, série sur la confiance numérique : première partie | Identité numérique, disponible à l'adresse suivante
[956] V. *infra*, II, Titre 2, 1.6

à ses débuts[957], certains auteurs la distinguant néanmoins de la notion d'identité numérique auto-souveraine (INAS) étudiée plus loin[958], un positionnement rejoint dans cette étude. Ce dernier concept anglo-saxon est désigné de façon ambivalente par les termes « *Self-Sovereign Identity – SSI* » ou plus généralement par celui de « *Decentralized Identity* » (ci-après « IND »). Une subtile distinction existe pourtant entre ces deux appelations, comme le confirme en 2021 un collectif de chercheurs européens[959]. Concrètement, l'INAS offre un degré de contrôle par l'utilisateur qui va plus loin que la notion générique d'identité numérique décentralisée (IND) dans laquelle elle s'inscrit. S'il est convenu que l'INAS reprend nécessairement le fonctionnement informatique d'une identité numérique décentralisée, celle-ci n'est pas systématiquement une INAS. Cette distinction est également nécessaire pour bien comprendre le lien existant entre l'INAS et un système de preuve d'identité numérique universelle[960]. A cet égard, il est supposé de ne pas laisser une trop grande liberté aux personnes sur leurs attributs d'identité racine - initialement une prérogative uniquement régalienne - au risque qu'elles en fassent une utilisation partiellement abusive ou décomplexée. Les parties suivantes explorent en quoi l'identité décentralisée propose un nouvel agencement au sein duquel l'utilisateur est souverain, depuis la création en ligne de ses attributs d'identité numérique jusqu'à leur partage à des tiers[961]. L'IND contribue ainsi directement à réduire la frontière qui existe entre les solutions d'identité numérique 2.0 et 3.0 en conférant aux données probabilistes un caractère déterministe, car les données sont 'cryptographiquement' encadrées par un tiers de confiance, tout en offrant une autonomie à leurs utilisateurs. Avec l'IND, les individus peuvent choisir quelles informations peuvent être connues publiquement ou non par des tiers et services en ligne publics ou privés. La granularité de ces informations et attributs numériques varie en fonction de chaque contexte social. Alors qu'une personne peut ne vouloir fournir que le minimum d'informations requis à une autorité publique, elle peut à l'inverse décider de partager des détails très personnels avec certains cercles sociaux de son choix, sa famille ou ses amis. Dans certains cas précis (INAS), l'utilisateur peut avoir besoin de différents profils ou cercles sociaux pour présenter des informations de confiance auprès de services en ligne. Par

[957] PREUKSCHAT Alex, REED Drummond, presentation 2022, « The Future of Self-Sovereign Identity (SSI) », Vidéo YouTube, disponible à l'adresse suivante, *v.* également « Self-Sovereign Identity Decentralized digital identity and verifiable credentials », livre publié en 2021, in *Manning Publications*.

[958] Bien que nombreux chercheurs utilisent l'acronyme « *SSI* » pour désigner le concept d'identité décentralisée, nous écartons l'utilisation de cet acronyme déjà utilisé par les acteurs du secteur informatique qui désigne la *Sécurité des Systèmes d'Information (SSI)*. De plus, l'identité décentralisée et l'identité auto-souveraine diffèrent légèrement en terme de degré de contrôle par l'utilisateur d'après le rapport « Blockchain and Digital Identity » du European Union Blockchain Observatory and Forum, publié le 2 mai 2019, consulté en ligne le 04/10/2021, traduit librement de l'anglais, p.14 : « Il est possible d'aller plus loin dans la décentralisation de l'identité en donnant aux utilisateurs le contrôle non seulement de leurs identifiants mais aussi des données qui leur sont associées. C'est le cœur de ce que l'on appelle l'identité auto-souveraine (SSI) », et *v. infra* II, Titre 1, chap. 1, 1.4

[959] SEDLMEIR Johannes, SMETHURST Reilly, RIEGER Alexander, FRIDGEN Gilbert, « Digital Identities and Verifiable Credentials », 2021, traduit de l'anglais, « L'identité auto-souveraine (SSI) est un nom contesté qui est souvent utilisé pour promouvoir divers projets d'identité numérique décentralisée », consulté en ligne le 08/10/2021, p.4.

[960] V. *supra*, I, Titre 2, 2.9, v. également *infra*, Partie 2, Titre 2, chap. 2, 2.1

[961] Trust Over IP Foundation, consultez le tutoriel suivant pour comprendre et visualiser ce nouveau modèle d'identité numérique.

conséquent, la possibilité d'une identité numérique de troisième génération, informatiquement vérifiable et distribuée, fait naître de nouvelles possibilités phygitales et sociétales inédites.

1.2 Définition informatique et conceptuelle de l'identité numérique décentralisée (IND)

L'identité numérique décentralisée (IND) propose une réinvention de la manière de concevoir, de générer et d'exploiter l'identité en ligne des personnes physiques. Ce nouveau paradigme informatique consiste à positionner l'utilisateur au centre du modèle de gestion de son identité tout en dissipant le besoin d'un tiers de confiance pour l'adiministrer. De façon inédite à l'ère d'Internet, un utilisateur possède désormais la possibilité informatique de devenir acteur, et non plus simplement spectateur, de sa propre existence numérique. En pratique, l'identité décentralisée propose à l'utilisateur de posséder sur une même application numérique certains de ses attributs numériques qui constituent tout ou partie de son identité (preuves de majorité ou de nationalité, attestations de diplômes et/ou cursus professionnels, attestations d'assurances ou financières). L'utilisateur possède ainsi tout ou partie de ses fragments d'identité directement sur une application mobile nouvelle génération : un portefeuille d'identité numérique décentralisé (défini par « PIND »)[962]. Cette application mobile ou web peut être définie comme un tableau de bord numérique permettant à une personne d'avoir un aperçu en temps réel de ses données d'identité, qu'elle peut piloter grâce à cette interface 2.0 ou 3.0. Elle pourra ensuite recevoir ou émettre des attestations et attributs numériques[963] directement depuis cette application pour finalement les partager en ligne ou hors ligne à des tiers choisis. En informatique, ce schéma d'identité de dernière génération, détaillé plus loin, propose à l'utilisateur de gérer ses identités numériques grâce à des identifiants uniques appelés des « identifiants décentralisés (DID) »[964] auxquels sont cryptographiquement associés des « attestations vérifiables (VC) »[965] également étudiées plus loin. Ces quelques définitions soulèvent de nombreuses questions, notamment celles des spécificités informatiques mobilisées pour ces échanges d'attributs d'identité nouvelle génération. Quelles sont les nouvelles opportunités, défis et conséquences informatiques et sociales au regard de l'utilisation de l'IND et/ou de l'INAS ? Comment les droits des personnes seront respectés, encadrés et impactés dans les sphères numériques de la société civile ? L'identité numérique décentralisée est un concept évoqué pour la première fois en 2012[966], s'ensuit une accélération majeure de l'intérêt et de l'adoption de ces nouveaux standards informatiques dans le secteur privé et à partir de 2017. En 2019, ce sont près de 170

[962] V. *infra*, Partie II, Titre 1, chap. 1, 1.3.1.3
[963] V. *infra*, Partie II, Titre 1, chap. 1, 1.3.1.2
[964] Traduit de l'anglais « Decentralized Identity (DID) » qui représente « Des identifiants permanents, uniques, qui ne nécessitent pas d'autorité d'enregistrement centralisée et qui sont souvent générés et/ou enregistrés de manière cryptographique » selon la *Decentralized Identity Founfation (DIF).* Toutefois, de nombreuses méthodes de *DID*, mais pas toutes, utilisent une technologie blockchain ou d'autres types de réseaux décentralisés/distribués. V. *infra*, II, Titre 1, 1.3.1.1
[965] V. *infra*, Partie II, Titre 1, chap. 1, 1.3.1.2, v. également *op. cit*. 2021, hal-03398096
[966] STOKKINK Quinten. POUWELSE Johan, « Deployment of a blockchain-based self-sovereign identity » CoRR, 2018, disponible en ligne

solutions d'identité numérique décentralisée (IND) et d'identité auto-souveraine (INAS) qui ont été recensées selon une étude du ministère de l'Intérieur[967] et environ 90% des solutions de « *Self-Sovereign Identity - SSI* » existantes sont implémentées à date au sein d'une infrastructure blockchain. Parce que l'utilisateur possède un contrôle théorique partiel (IND) ou total (INAS) sur ses attributs d'identité 3.0, une pratique étudiée dans les prochains paragraphes de cette partie, elle permet de nouvelles interactions en ligne. De manière simplifiée, elle implique systématiquement la présence (i) d'un émetteur, (ii) d'un utilisateur et (iii) d'un vérificateur (*v.* schémas suivants). Ces interactions sont telles que le premier émet un ou plusieurs attributs d'identité, le second le(s) reçoit(s) et le dernier le(s) vérifie(nt). Ces rôles peuvent être cumulés par une même entité, selon les cas d'usage de l'identité dont il est question.

De manière courante, les individus utilisent des attestations pour établir leur identité au quotidien. Ces documents peuvent prendre la forme de passeports, de permis de conduire, de certifications, de diplômes, de cartes d'assurance ou encore d'attestations médicales. En général, ces preuves d'identité sont physiques et sont constituées de papier ou de plastique. En appliquant une approche de décentralisation numérique de l'identité d'une personne, ses attestations physiques peuvent être transformées en attestations numériques vérifiables[968]. Pour ce faire, elles doivent être converties en un format numérique standardisé et stockées localement sur le téléphone de l'utilisateur ou de manière distante sur un serveur appartenant à un tiers de confiance (institutions publiques, sociétés privés certifiés). Ces attestations vérifiables (VC), évoquées plus loin, représentent des certificats numériques standardisés qui permettent à leurs détenteurs de partager des informations en ligne de manière autonome et sécurisée. La notion de standardisation informatique indique qu'il existe une méthode conforme pour programmer une attestation vérifiable, un mécanisme en cours de normalisation par le « World Wide Web Consortium - W3C »[969] afin que les fournisseurs d'identité et de services de cet écosystème 3.0 puissent recourir à des normes informatiques communes, interopérables et spécifiquement dédiées aux outils mobilisés par l'identité numérique décentralisée. En associant des attestations vérifiables d'internautes à des autorités reconnues comme des gouvernements ou des sociétés privées, les utilisateurs bénéficient d'homologues numériques[970] qui prolongent leurs attestations régaliennes et physiques. En effet, grâce à une attestation vérifiable, une carte nationale d'identité (CNI) possède en quelque sorte un jumeau numérique tout aussi recevable en ligne et hors ligne que sa version palpable et officielle. Une fois générées, les attestations vérifiables d'une personne peuvent être partagées par l'utilisateur depuis son téléphone, ordinateur ou même navigateur grâce à une

[967] *Op. cit.* HENNEBERT Christine, al., « Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité' », 2020, disponible à l'adresse suivante

[968] La notion d'attestation vérifiable ne possède pas encore de traduction unanime en français. v. *infra,* II, Titre 1, 1.3.1.2

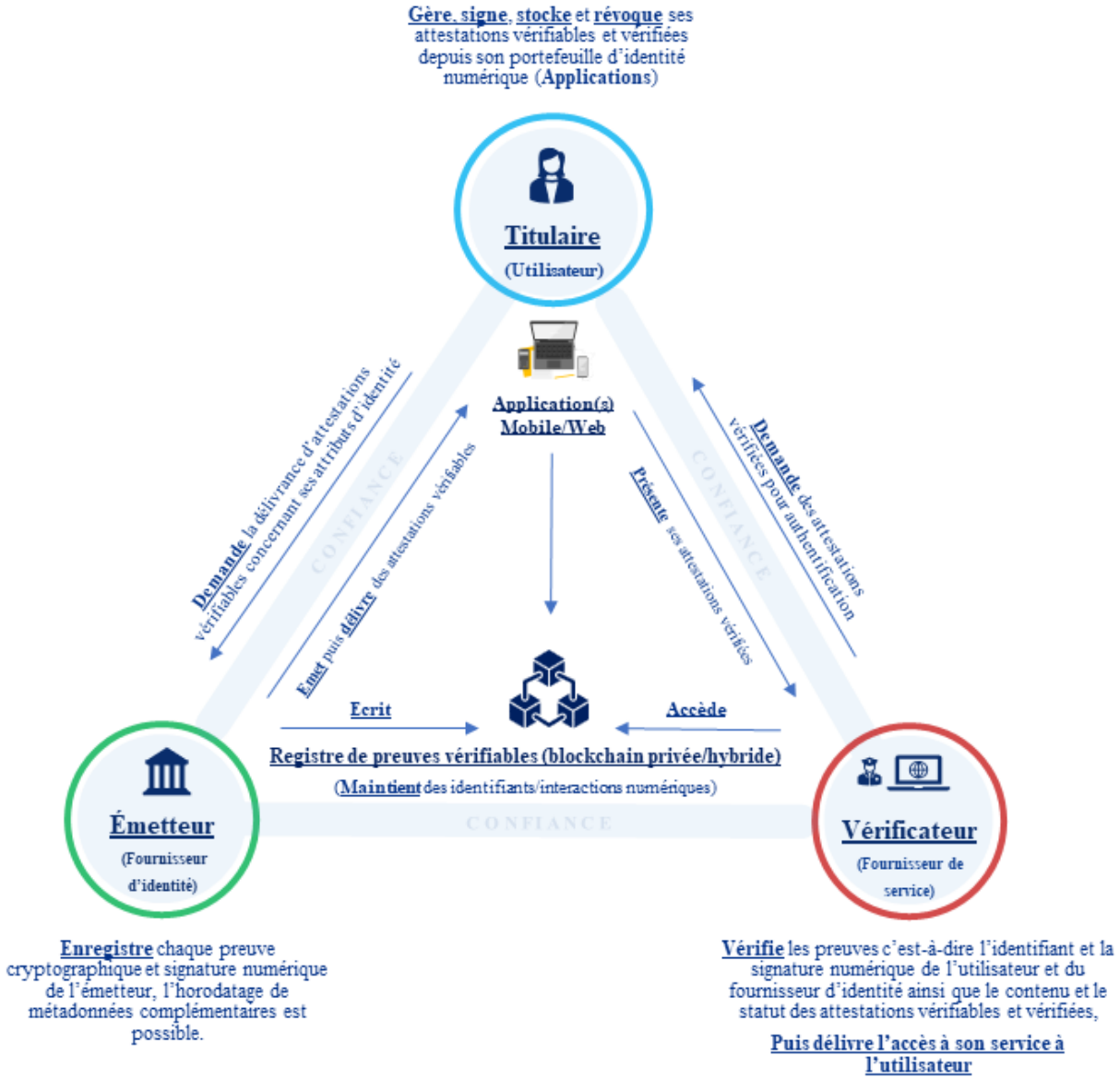
[969] Les attestations vérifiables sont standardisées par le World Wide Web Consortium (W3C), une norme disponible à cette adresse. Le W3C est composé de plus de 450 organisations investies dans les identifiants décentralisés et les attestations vérifiables du W3C afin de garantir un écosystème de partage des données plus décentralisé, respectueux de la vie privée et fondé sur le consentement

[970] Si l'intégrité des informations d'une attestation vérifiable peut être vérifiée, son authenticité ne peut l'être. Bien que le vérificateur soit obligé de faire confiance à l'émetteur de l'attestation, il n'a pas besoin de le contacter directement pour vérifier les informations dès lors qu'il lui fait confiance.

extension web spécifique[971] - par courriel, SMS, QR code ou Bluetooth - afin de prouver certaines informations racines ou étendues rattachées à son identité. La cryptographie mêlée à ces nouveaux standards numériques 3.0 joue un rôle central dans la réalisation technique d'une identité numérique distribuée/décentralisée[972]. Ses implémentations utilisent des preuves cryptographiques - des empreintes numériques persistantes ou jetables - en théorie infalsifiables grâce aux technologies blockchains, aux fins de fournir une certitude mathématique concernant le lien entre une personne physique et ses données numériques. Toutefois, l'identité numérique décentralisée ne requiert pas nécessairement, comme infrastructure numérique sous-jacente, une technologie blockchain. En effet, les standards techniques utilisés permettent d'offrir à tous types d'entités des attestations vérifiables autonomes et partageables quel que soit le registre numérique sur lequel elles évoluent (serveurs centralisés, distribués ou décentralisés). Pourtant, le binôme de ces nouveaux standards avec une technologie blockchain est incontestablement judicieux. Les avantages intrinsèques[973] qu'offre une infrastructure blockchain décentralisée se transposent naturellement à ces standards, dès lors qu'ils reposent sur cette dernière. De fait, de nombreux projets d'identité décentralisée recourent pour l'heure à des technologies blockchains, en réalité plus ou moins immuables et décentralisées sur le plan informatique.

[971] Wikipedia contributors, « Plugin », 2022, disponible à l'adresse suivante
[972] A partir d'ici l'un ou l'autre de ces deux termes sera utilisé pour désigner le même concept – celui d'IND - tout en signifiant une différence de degré concernant ledit niveau de décentralisation dont il est question.
[973] Il est fait référence aux caractéristiques et avantages issus des technologies blockchains : immuabilité, rapidité, sécurité, accessibilité et pseudonymat des transactions du registre.

1.2.1 Le triangle de confiance de l'identité numérique décentralisée



Le « triangle de confiance » est un concept théorique propre à l'identité décentralisée et permet de s'approprier visuellement certaines de ses principales composantes et interactions numériques. Ce schéma - non exhaustif sur le plan informatique - place le détenteur d'une identité au centre des échanges d'informations le concernant. Trois entités possèdent un ou plusieurs rôles[974], participant à l'échange d'informations chiffrées[975] de bout en bout : (i) un émetteur, (ii) un titulaire/utilisateur et (iii) un vérificateur. La relation entre ces rôles est décrite dans ce triangle de confiance :

[974] En théorie, tous les rôles peuvent prendre la place d'un autre rôle, ce qui signifie qu'un émetteur peut également être un détenteur ou un vérificateur. En pratique, un individu en tant que titulaire pourrait ne pas être en mesure de jouer le rôle d'un émetteur puisque certains registres de preuves vérifiables (blockchains publiques) ne permettent pas aux individus d'écrire leurs identifiants décentralisés (DID) pour des raisons de conformité au RGPD.
[975] Le terme « chiffrer » est à privilégier à celui de « crypter » d'après le site en ligne *BlogChiffrer.info*, disponible en ligne

(i) L'émetteur des informations d'identité en tant que tiers de confiance fournit - grâce à un registre électronique centralisé ou décentralisé - la preuve de la validité de l'assertion vérifiable délivrée au détenteur en le signant électroniquement avec sa clé cryptographique privée. La clé publique de l'émetteur peut quant à elle être stockée dans un registre de données vérifiable centralisé (serveur) ou dans un registre décentralisé (blockchain). Cela permet à chaque partie de vérifier de manière indépendante l'exactitude et la validité des attestations vérifiables émises. Une fois la signature cryptographique du titulaire effectuée, son attestation vérifiable (VC) devient désormais une attestation vérifiée (VP), c'est-à-dire possédant la valeur équivalente à une attestation papier et manuscrite comme signalé plus loin. Parce que l'émetteur envoie au titulaire une version signée de cette dernière attestation[976], elle peut ainsi être vérifiée par une entité reconnue (étatique) et/ou vérifiable en ligne par tout tiers (services en ligne).

(ii) Après réception par le titulaire/utilisateur, les informations peuvent être stockées directement sur toute machine connectée ou portefeuille numérique (PIND) comme déjà mentionné, pour recevoir, stocker et partager ses attestations vérifiables (VC) et vérifiées (VP).

(iii) Le processus de vérification est initié par le système informatique d'une organisation vérificatrice qui accepte la mise en œuvre d'identifiants décentralisés (DID) et l'envoi d'attestations vérifiables et/ou vérifiées à un titulaire qui décidera - ou non - de l'envoyer au vérificateur pour prouver ses attributs d'identité. Le registre de données vérifiables (blockchain) permet au vérificateur de s'assurer automatiquement et en temps réel que chaque preuve d'identité fournie par le titulaire a été préalablement validée par l'émetteur.

Ce schéma permet de comprendre que chaque interaction entre ces trois entités est en principe transparente et vérifiable, c'est-à-dire de confiance. Ces mécanismes d'interactions numériques sont nouveaux et pour l'instant déployés à des échelles non industrielles, c'est-à-dire surtout expérimentales. En définitive, si l'un des principaux avantages de l'identité numérique distribuée repose sur la vérifiabilité des informations présentées entre les entités précitées, la confiance repose préalablement sur un émetteur de confiance généralement certifié par l'Etat ou ses institutions publiques. Ainsi, l'identité décentralisée est en réalité hybride et ne tend pas pour l'heure vers un degré de décentralisation important comme le prône en revanche le modèle d'identité auto-souveraine (INAS) étudié plus loin.

[976] Les VC sont signés par leur émetteur. La signature et donc la déclaration peuvent être vérifiées en utilisant la technologie blockchain ou d'autres mécanismes cryptographiques adjacents.

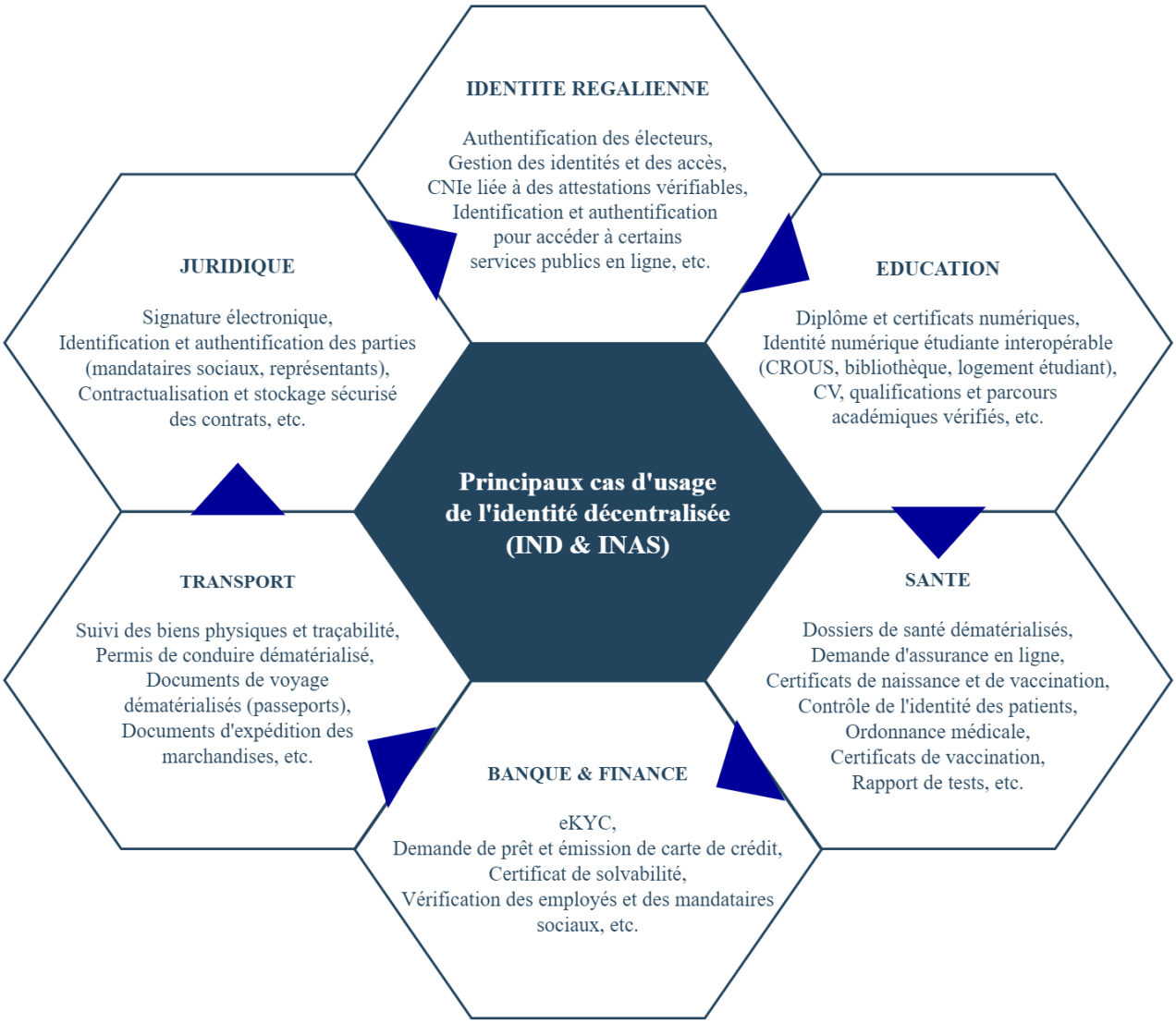
1.2.2 Dix principes fondateurs pour une identité décentralisée source de confiance

Afin que le concept et les méthodes utilisées par l'identité numérique décentralisée inspirent confiance, l'un de ses pères fondateurs et programmateurs informatiques, Christopher Allen, a proposé dix principes à respecter pour toute entité qui souhaite fournir des solutions d'IND[977], à savoir (i) l'importance de placer l'utilisateur au centre du schéma d'identité numérique, (ii) lui donner le contrôle sur son identité numérique, (iii) garantir que l'utilisateur a accès à ses propres données, (iv) assurer la traçabilité de ces données, (v) garantir la pérennité des preuves d'informations échangées, (vi) permettre la portabilité et (vii) l'interopérabilité des données, (viii) obtenir le consentement systématique de l'utilisateur, (ix) minimiser la divulgation de ses données et (x) les protéger. Énoncés en avril 2016, ces dix principes reflètent la vision personnelle de l'identité numérique distribuée au sens de Christopher Allen. Plusieurs de ces dix principes sont probablement issus des valeurs et principes du RGPD adopté le 14 avril 2016 comme étudié en amont[978]. Une fois implémentés par une solution d'identité distribuée, ces dix principes proposent donc une forme de conformité par conception avec le RGPD, comme semblent le confirmer certains spécialistes[979]. Lorsqu'on interagit avec une identité numérique, la confiance est primordiale, qu'elle soit centralisée (dépendante) ou décentralisée (indépendante). Pour instaurer la confiance, il est nécessaire d'avoir des structures sociales et institutionnelles fiables, durables et assorties d'une sécurité juridique. Les fournisseurs de services doivent pouvoir avoir confiance dans la source d'une identité distribuée, nécessairement liée à l'identité régalienne et civile des individus. L'État garantit ainsi l'identité des personnes et l'identité numérique doit continuer à s'appuyer sur cette identité légale, fondamentale, tout en laissant le libre arbitre aux individus d'utiliser des pseudonymes avec une identité numérique auto-souveraine (INAS). Dans le cas d'une identité numérique distribuée, les sous-jacents cryptographiques transparents et contrôlés directement par les personnes concernées peuvent fournir un recours juridique efficace en cas d'usurpation d'identité[980] ou de révocation d'attestations numériques[981]. Il est également important d'avoir confiance dans la traçabilité des interactions et de chaque action en ligne, ce qui est devenu essentiel pour les forces de l'ordre dans la lutte contre la criminalité ou le terrorisme. La minimisation ou le cloisonnement des données d'identité numérique pourrait devenir une nouvelle sécurité et norme informatique fondamentale, habilitée au demeurant par l'IND. Cette minimisation décourage et limite en effet la portée de toute utilisation malveillante et frauduleuse des données personnelles. Bien que ce principe de minimisation d'attributs d'identité soit en contradiction avec certains usages sociaux propres à la crypto-économie et aux blockchains ouvertes, cette recherche soutient cette idée pour l'avènement d'une identité numérique de

[977] ALLEN Christopher, « The path to self-sovereign identity - Ten principle of self-sovereign identity », 25 avril 2016, disponible sur son blog personnel à l'adresse suivante
[978] V. *supra*, I, Titre 2, chap. 2, 2.4
[979] Société Archipels, « Pourquoi le SSI est compatible avec le RGPD ? », 16 février 2022. Disponible à l'adresse suivante
[980] V. *supra*, Partie I, Titre 2, chap. 1, 1.4.1.1
[981] La révocation d'une attestation signifie son annulation cryptographique, il s'agit d'une fonctionnalité inédite et possible par conception dans chaque attestation vérifiable

dernière génération. Ces principes fondamentaux pour l'avenir de l'identité numérique décentralisée peuvent sembler difficiles à concilier pour chacune des trois entités du triangle de confiance, il revient donc à chaque acteur impliqué dans cette chaîne de valeur de les garantir et de ne pas laisser cet objectif à atteindre uniquement aux pouvoirs législatifs et exécutifs.

1.2.3 Les usages et applications sectoriels de l'identité décentralisée



La nécessité d'utiliser une IND est directement liée aux exigences des industries qui ont besoin d'une identification systématique et en ligne de leurs utilisateurs. Ces industries sont potentiellement infinies, comme cela est illustré dans le diagramme ci-dessus, incluant le secteur public (numérisation des permis de conduire et des passeports), le secteur privé (numérisation des cartes professionnelles), le secteur financier (transfert d'actifs), le secteur bancaire (processus d'embarquement et d'identification des

clients), le secteur des assurances (attestations de sinistres), de l'éducation (diplômes, attestations de stage), celui de la santé (attestation de vaccination) et le secteur juridique comme étudié précédemment (stockage de documents et signature électronique). De manière générale, l'utilisation d'attestations d'identité vérifiables (VC) et de portefeuilles d'identité numériques décentralisés (PIND) étudiés plus loin, peut avoir un impact considérable sur les processus d'enregistrement et d'embarquement du commerce en ligne. Par exemple, un utilisateur qui n'est pas enregistré sur un site internet commercial pourrait passer une commande en utilisant simplement un portefeuille numérique contenant ses attributs d'identité. En scannant un QR code, il pourrait confirmer la divulgation de certaines informations d'identité tels que son adresse ou son âge directement contenues dans des attestations d'identité vérifiables (VC). Cette méthode permet de réduire significativement l'utilisation d'identifiants et de mots de passe numériques, voire de les éliminer complètement dans certains cas, ce qui constitue un avantage pratique par rapport à l'identité numérique 2.0 actuellement utilisée. Un exemple couramment utilisé depuis l'avènement d'Internet concerne la messagerie en ligne, aujourd'hui massive, qui pourrait également bénéficier de l'IND pour offrir une meilleure interopérabilité, sécurité et intelligence entre de multiples services en ligne. En permettant aux utilisateurs de prendre le contrôle de leur identité numérique, l'identité numérique décentralisée contribue à leur permet de reprendre le contrôle de leur destin numérique. Ce nouveau modèle d'identité 'augmentée', fondé sur une transparente donc confiance numérique, représente une nouvelle opportunité - d'intérêt - sociétale. Cette nouvelle identité numérique 3.0 peut également être appliquée à l'authentification d'objets numériques comme suggéré plus loin, en rendant plus transparents et fiables tous les processus en ligne ou hors ligne nécessitant la preuve d'une ou de plusieurs qualités par l'intermédiaire d'attributs d'identité. À moyen terme, il est probable que l'identité décentralisée sera hybride, comprenant des infrastructures numériques et des briques technologiques conjoitement centralisées et décentralisées, c'est-à-dire distribuée. Pour être largement adoptée, elle devra être soutenue par un consensus technique, économique, politique et juridique. Un amendement du Règlement européen eIDAS[982], dont il est question plus loin, décrit partiellement certains cas d'utilisation possibles de l'IND, telle que la capacité des citoyens et résidents à prouver qu'ils détiennent un permis de conduire valide et les autorités compétentes à vérifier et faire confiance à cette information phygitale. A plus long terme, il semble que les identités numériques auto-souveraines (INAS) également détaillées plus loin trouveront leurs applications dans certains univers les plus décentralisés du Web 3.0. En fin de compte, les besoins fondamentaux du marché de l'identité numérique se concentrent sur la sécurité des méthodes d'enregistrement, de gestion, et d'identification, ainsi que sur la confiance informatique et juridique des solutions mises à disposition. Il semble essentiel de proposer des systèmes et des schémas d'identification auxquels tous les utilisateurs peuvent faire confiance, tout en respectant le droit des données personnelles, le droit à un pseudo-anonymat déjà évoqué, ainsi qu'à un consentement par conception et systématique.

[982] V. *infra*, II, Titre 1, 2.1.1.1.a

1.2.4 Enjeux et bénéfices théoriques

Les apports de l'identité numérique distribuée en comparaison aux méthodes conventionnelles de management de l'identité 2.0 déjà étudiées sont nombreux et peuvent être résumés à travers le prisme de l'utilisateur (i) puis celui des organisations (ii). Pour l'utilisateur (i), l'identité numérique (distribuée) deviendra davantage facile d'utilisation. Une fois déployée, une attestation vérifiable (VC) peut être facilement partagée entre différents services internet aux fins d'authentification. L'utilisateur n'a plus besoin de mot de passe pour chaque service et l'identité numérique devient consentie, portable et interopérable d'un service en ligne à un autre. Les applications mobiles et web traditionnelles pourront se connecter à ce(s) système(s) distribué(s) pour solliciter la permission d'accéder à l'identité de l'utilisateur. Ainsi, il est à la discrétion de ce dernier d'accepter et de partager certaines informations souhaitées et de choisir quand attribuer ou révoquer l'accès à ses données d'identité jusqu'alors accessibles par des tiers. Cette nouvelle fonctionnalité de sélectivité cryptographique bénéficiera aux internautes et contribuera à endiguer la commercialisation indue de leurs données personnelles sur Internet. Étant donné sa conception par essence respectueuse de la vie privée et des données personnelles[983] l'identité distribuée rend moins probable l'agrégation des données et les abus de confidentialité des utilisateurs par des services numériques tiers. L'IND est aussi plus sécurisée que l'identité numérique centralisée puisque l'utilisateur contrôle en principe seul l'accès et le partage de ses attributs d'identité via son portefeuille d'identité numérique décentralisé (PIND) précisé plus loin. L'identité devient plus complexe à usurper, une aubaine pour 8% des Français qui déclarent avoir été victimes d'usurpation d'identité au cours des dix dernières années[984]. Pour ses utilisateurs, l'identité décentralisée implique toutefois une expérience de navigation en ligne moins intuitive pour ses utilisateurs, mais elle contribuera à diminuer le nombre de victimes d'hameçonnage numérique tant pour les personnes physiques que morales[985]. Dans le PIND de l'utilisateur, il est possible de stocker différents types de documents tels que des cartes nationales d'identité, des factures, des certificats, des permis et des autorisations. Grâce à cette fonctionnalité, l'utilisateur pourra à l'avenir détecter chaque attestation vérifiée (VC) et remplir automatiquement des formulaires en ligne pour le compte d'autres utilisateurs, ce qui réduira considérablement leur charge de travail et améliorera leur confort d'utilisation. Pour les organisations (ii), un système d'identité décentralisée confère une sécurité ainsi qu'une fiabilité cryptographique aux informations stockées et aux interactions effectuées avec d'autres entités. L'identité numérique distribuée permet aux organisations de fournir à leurs utilisateurs un nouveau moyen d'authentification simple, sécurisé et universel et d'automatiser en toute efficience certains

[983] Les standards techniques du W3C se fondent sur les « 10 principes de l'identité auto souveraine » énoncée précédemment « Existence, contrôle, accès, transparence, pérennité, portabilité, interopérabilité, consentement, minimisation, protection »
[984] CSA, « Les Français et la criminalité identitaire », sondage, in *Fellowes*, oct. 2012, p.4 et *v. supra*, Partie I, Titre 2, Chap. 1, 1.4.1.1
[985] Il peut en résulter une diminution du nombre de victimes de « *phishing* » puisque l'utilisateur n'a qu'un seul canal de communication fiable avec une entreprise en lieu et place de recevoir des courriels électroniques provenant d'une source de confiance, mais en réalité provenant d'un tiers frauduleux.

processus internes ou externes nécessitant une confiance numérique accrue. A titre d'illustration[986], en cas d'injustice ou de censures numériques d'un utilisateur sans motif légitime par un service en ligne, les actes par exemple non motivés pour censure, fermeture injustifiée de comptes professionnels seraient aisément et techniquement retraçables. Avec l'IND, certains coûts d'infrastructures sont également partagés entre les entreprises, les institutions publiques et toutes autres organisations parties prenantes à l'infrastructure, souvent une blockchain fermée sous-jacente et commune. Par conséquent, une nouvelle ère de collaboration se dessine pour les organisations qui peuvent bénéficier d'une même infrastructure informatique distribuée, tout en développant des applications privées et souveraines fonctionnant en toute confiance et conformité. Les collaborations en silo disparaissent ainsi au profit d'acteurs et d'utilisateurs professionnels qui contrôlent leurs données, leurs identifiants décentralisés et leurs attestations vérifiables. Avec une IND, une organisation peut désormais prouver en toute confiance l'authenticité de ses produits, l'intégrité de ses données et l'identité de ses collaborateurs.

1.3 Aspects technologiques : l'union de l'identité décentralisée et de la blockchain

L'identité numérique décentralisée est un concept fortement axé sur la technologie en raison de ses méthodes et interactions qui nécessitent plusieurs couches cryptographiques pour produire les fonctionnalités escomptées. L'intérêt de la combinaison des standards de l'identité décentralisée avec les différents types de blockchains existantes est traité par la littérature scientifique et informatique depuis 2015[987]. Sur le plan informatique, l'IND ne requiert pas toujours l'utilisation d'une technologie blockchain pour maintenir en ligne un registre contenant des preuves de transactions d'identités. Des serveurs centralisés[988] peuvent le réaliser avec plus de pertinence, par exemple lorsque le triangle d'incompatibilité étudié en première partie[989] empêche une technologie blockchain de répondre aux besoins d'une entreprise pour ses cas d'usage. Néanmoins, les avantages conférés par une technologie blockchain semblent notoires et particulièrement adaptés aux standards DID et VC que mobilise l'IND. En effet, pour être inviolable et immuable, une attestation vérifiée doit être liée à un type de registre de données et de preuves vérifiables pérenne, c'est-à-dire à une blockchain ouverte en l'état actuel du Web 3.0. En 2023, il n'existe pas encore d'unanimité informatique, juridique et économique suffisante au regard des nombreux standards existants pour le concept d'IND. Cela génère des problématiques en matière d'interopérabilité entre les portefeuilles d'identité numérique décentralisée (PIND) - étudiés plus loin - qui ne peuvent alors communiquer qu'avec un nombre limité de registres de preuves vérifiables disponibles (serveurs centralisés versus blockchains ouvertes et décentralisées). A cet égard,

[986] Le réseau social MINDS implémente un identifiant décentralisé à chacun de ses utilisateurs de manière facultative ce qui signifie que ce réseau social pourra émettre des attestations vérifiables à l'avenir, « Minds raises $10M for decentralized and encrypted social network and messaging app », plus d'informations disponibles à l'adresse suivante
[987] Rapport Ministère de l'Intérieur, « Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité' (BCID) », *op. cit.*, 2020, version 1.0, disponible à l'adresse suivante
[988] Tels les « *Hardware Security Module (HSM)* » pour un maximum de protection informatique.
[989] V. *supra*, I, Titre 1, 2.3.2

ces portefeuilles numériques 3.0 peuvent offrir des fonctionnalités contradictoires et le passage d'un portefeuille à un autre peut entraîner une perte de fonctionnalité pour l'utilisateur, des situations à éviter pour que l'identité numérique décentralisée puisse être massivement adoptée par les internautes. Cependant, ces difficultés ne sont que partielles, car les fonctions essentielles tels que le stockage des attestations vérifiées et la réception des demandes de preuve sont en principe pris en charge de façon native et indifférenciée par tous les portefeuilles d'identité numérique décentralisée, grâce à ses standards 3.0 conçus à cet effet. Une carte interactive recensant une partie de ces projets liés à l'IND est accessible en ligne et apporte un éclairage en temps réel sur les projets en cours de développement concernant ce nouveau standard technologique[990].

1.3.1 La chaîne de valeur de l'identité décentralisée

La notion de souveraineté numérique est une composante fondamentale de l'identité numérique distribuée. Pour la comprendre, il est nécessaire d'examiner dans les parties qui suivent les aspects techniques et juridiques de son interopérabilité et de ses modes de gouvernance. Ces deux piliers sont essentiels pour garantir une identité numérique sûre et durable au bénéfice des utilisateurs d'Internet. Il convient également de comprendre le fonctionnement de la nouvelle chaîne de valeur informatique que propose l'IND décentralisée. Certaines de ses composantes techniques ne sont volontairement pas détaillées dans cette étude en raison d'une moindre pertinence au regard d'autres enjeux plus importants rappelés ci-après, les identifiants décentralisés (DID), les attestations vérifiables (VC), puis les portefeuilles d'identité numérique décentralisée (PIND), représentant au sens de cette étude les trois principaux piliers numériques fondamentaux de cette nouvelle chaîne de valeur 3.0.

1.3.1.1 Les identifiants numériques décentralisés (DID)

En ligne, les identifiants sont généralement uniques et temporaires, utilisés pour des contextes spécifiques tels que les plateformes de réseaux sociaux et les services publics en ligne. Ces identifiants numériques sont aujoud'hui toujours sous l'administration d'une ou quelques autorités centrales, ce qui signifie qu'ils n'appartientent pas véritablement à leurs utilisateurs. Dans le Web 2.0 actuel, ils sont plutôt octroyés et délégués gratuitement par les fournisseurs de services d'identité ou en ligne, qui se rémunèrent ultérieurement en collectant les données personnelles de leurs utilisateurs, le plus souvent en relative conformité avec le RGPD. En proposant une alternative aux identifiants numériques centralisés (couple d'identifiants et mots de passe), l'IND vise à permettre aux utilisateurs de conserver le contrôle de leurs identifiants décentralisés (DID) sans passer par une autorité supposée de confiance que représente un fournisseur d'identité. En effet, pour représenter leur(s) identité(s) en ligne, les

[990] Pour participer à la mise à jour ou consulter cette carte interactive, *v.* l'adresse suivante

utilisateurs ont besoin d'un identifiant numérique unique au sein de l'univers numérique. Bien qu'il existe de nombreux identifiants numériques différents pour chaque personne, tels que des adresses électroniques, des pseudonymes de réseaux sociaux ou encore des numéros de téléphone, l'IND introduit un nouveau type d'identifiant numérique décentralisé (« Decentralized Identifier - DID »). Ce nouveau type d'identifiant est inédit, car il utilise la cryptographie pour revendiquer ou prouver un lien numérique sous la forme d'un certificat, d'une signature électronique, parfois rattaché à une propriété numérique. Cette norme DID a été conscrée par le W3C en 2022 pour devenir la deuxième norme d'identification - après l'URL (« Uniform Resource Locator ») aujourd'hui indispensable - à être approuvée par cette institution internationale. Les identifiants décentralisés appartiennent cryptographiquement aux utilisateurs, car ils représentent des liens numériques uniques contrôlés directement par ces derniers. De multiples degrés de contrôle et variantes technologiques existent pour cette norme et pour ces DID, ils recourent systématiquement à des mécanismes cryptographiques bien connus depuis les années 1990, c'est-à-dire à une paire de clés, l'une publique et l'autre privée, comme précédemment expliqué. De cette façon, lorsque l'utilisateur est en possession de sa clé privée, il possède et contrôle seul ses attributs d'identité[991]. Les DID sont considérés comme décentralisés par conception, car chaque utilisateur est en principe capable de les contrôler individuellement, ce qui les rend très dispersés et portables sur Internet, permettant ainsi aux personnes de manifester leur identité où elles le souhaitent dans la sphère numérique. Il est important de souligner que les identifiants numériques utilisés dans l'identité décentralisée ne sont pas strictement « décentralisés » au sens informatique du terme, mais plutôt « distribués » car le plus souvent rattaché à des tiers de confiance 3.0 comme le suggère cette étude. Néanmoins, étant donné que le terme décentralisé est communément utilisé dans le contexte de l'IND, il est courant de l'employer pour décrire ces identifiants, même si ce n'est pas tout à fait exact d'un point de vue technique. Les cas d'usage auxquels les DID peuvent être appliqués sont presques infinis et il devient possible d'imaginer un avenir où les DID sont rattachés à toutes activités numériques y compris phygitales : identité régalienne (CNIe), listes de lecture de musiques, vidéos, objets numériques (NFT), articles de blog, informations, événements, organisations, lieux numériques (Métavers étudié plus loin). Les moteurs de recherche tels que Google et Mozilla ainsi que la société Apple ont exprimé leur désaccord formel en vue de bloquer l'adoption de la norme DID au sein du groupe en charge de sa normalisation au sein du W3C, probablement car l'adoption de ce standard compromettrait leurs modèles d'affaires. Lors d'un vote en septembre 2021[992], ces trois géants du numérique ont donc voté contre l'adoption du standard des identifiants décentralisés, pourtant en cours d'élaboration par le W3C et la DIF depuis 2015. Bien que la quasi-totalité des autres membres ait voté en faveur de cette norme, ces

[991] Les identifiants décentralisés (DID) permettent à leur propriétaire cryptographique de présenter leur identité à un service en ligne tout en prouvant que les informations partagées via ce DID proviennent bien d'eux. Cette fonctionnalité est rendue possible grâce à l'association d'une clé publique au DID, qui peut être communiquée à des tiers, tandis que la clé privée est uniquement connue du propriétaire du DID. La clé privée est ensuite utilisée pour signer les événements ou interactions liés à ce même DID.

[992] DRUMMOND Reed, « Does the W3C still believe in Tim Berners-Lee's vision of decentralization », in *Eyernym*, 12 octobre 2021, consulté en ligne le 3 novembre 2021.

trois acteurs ont avancé quatre arguments techniques pour justifier leur vote, mais rapidement réfutés par l'ensemble du groupe de travail. Cette tentative de contestation, qui est en réalité une tentative de déstabilisation oligopolistique vis-à-vis de ce nouveau standard informatique à fort potentiel, montre que les géants du Web 2.0 sont préoccupés par ce possible regain de contrôle par les internautes relatifs à la tendance croissante de décentralisation de l'Internet qui devient progressivement 3.0. A ce propos, il est souligné que l'un des pionniers et fondateurs d'Internet Tim Berners-Lee - fervent défenseur de la décentralisation - est intervenu personnellement afin de trancher ce litige en faveur de l'acceptation du standard DID par le W3C et par extension pour l'Internet de demain[993]. Les identifiants décentralisés (DID) permettent de se souvenir, de reconnaître et de faire confiance aux interactions effectuées en ligne avec d'autres entités. Les DID sont créés par un contrôleur/émetteur, qui peut être une personne physique, une organisation ou même un logiciel. Ce dernier peut utiliser différents facteurs d'authentification avec un périphérique informatique, la connaissance d'une clé ou d'un mot de passe, ou l'identité corporelle basée sur de la biométrie étudiée plus loin[994]. En général, une combinaison de facteurs d'authentification est utilisée pour prouver la légitimité et l'autorité d'un identifiant décentralisé (DID). Contrairement aux attestations vérifiables (VC), qui sont stockées directement sur l'appareil de l'utilisateur ou sur un serveur de confiance, les DID peuvent être stockés dans un registre de données vérifiables, tel qu'un serveur ou une blockchain. De cette manière, tout tiers peut vérifier les informations et preuves publiées ou envoyées par l'entité à l'origine d'un DID public. En revanche, un DID privé n'est en principe jamais enregistré dans une blockchain publique et ne peut donc pas être accessible publiquement. Si un DID ne contient jamais de données personnelles, il est suggéré qu'un contrôleur de DID doit pouvoir en créer plusieurs afin d'éviter une nouvelle identification (phénomène de réidentification) par une entité tierce. Il est également recommandé de créer des DID temporaires et à usage unique pour respecter les dispositions du Règlement RGPD évoqué précédemment et du Règlement eIDAS qui est étudié plus loin. Le 19 juillet 2022[995], le W3C a finalement annoncé que les identifiants décentralisés deviennent une norme officielle d'Internet. Avec 40 témoignages de soutien lors de son communiqué de presse, cette nouvelle norme dernière génération est devenue la plus soutenu de l'histoire du W3C. A titre de comparaison, la norme « HTML5 » (que chaque internaute utilise quotidiennement) comptait seulement 19 témoignages de soutien. Cette annonce vient donc confirmer l'intérêt théorique de l'IND en tant que nouveau standard pour le Web 2.0, et permet de renforcer l'intérêt de l'identité décentralisée en tant que prochain fondement du Web 3.0[996]. Selon Christopher

[993] « Le directeur [du groupe de travail dédié au sein du W3C] conclut que la balance penche en faveur de la communauté des développeurs DID, l'encourageant à poursuivre ses travaux et à rechercher un consensus sur des méthodes DID standard. Les objections [de Google, Apple et Mozilla] sont rejetées. La spécification de base DID est approuvée pour passer à la recommandation du W3C », traduction libre de l'anglais, « Director's Decision on DID 1.0 Proposed recommendation formal objections », 30 juin 2022, disponible à l'adresse suivante www.w3.org

[994] V. *infra*, II, Titre 2, 1.3

[995] « Decentralized identifiers (DIDs) v1.0 becomes a W3C recommendation », 19 juillet 2022, disponible à l'adresse W3.Org

[996] Le Web 1.0 permet une simple lecture de données en ligne, le *Web 2.0* permet une lecture et écriture de données en ligne et le *Web 3.0* permet une lecture, écriture et propriété de données en ligne (ce dernier étant une combinaison du souhait originel de décentralisation et de gouvernance par la communauté du *Web 1.0* avec les fonctionnalités d'interaction modernes du *Web 3.0*.

Allen, l'un des promoteurs du concept d'INAS - étudié plus loin - et coauteur du standard des DID au sein du W3C s'exprime : « *Les DID sont au cœur de notre prochaine génération d'identité numérique sur internet. Je suis ravi qu'ils soient reconnus comme une norme internationale. Cependant, ils ne sont qu'une première étape. Afin de garantir une infrastructure numérique compatissante qui protège les droits numériques de l'homme, nous devons concevoir des architectures centrées sur les DID qui exploitent leurs possibilités décentralisées et réduisent au minimum les identités et les informations d'identification que nous partageons. Nous avons posé une excellente base avec la spécification DID 1.0* »[997]. Finalement, les identifiants décentralisés constituent une avancée qui permet de rendre l'utilisation de la cryptographie plus accessible au grand public, en offrant la possibilité de contrôler des identifiants fiables et interopérables en ligne. Ils contribuent également à démocratiser le phénomène de décentralisation informatique, permettant ainsi de regagner une forme de contrôle sur Internet, et peut-être un jour sur nos avatars numériques étudiés plus loin[998].

1.3.1.2 Les attestations numériques vérifiables (VC) et les attestations vérifiées (VP)

Aujourd'hui, chaque citoyen possède des certificats tels qu'un passeport pour prouver son identité à l'étranger, un permis de conduire pour attester de sa réussite à un examen national de conduite, ou encore une carte de crédit pour effectuer des achats en ligne ou en magasin. Ces certificats physiques sont ainsi utilisés pour conférer puis attester des droits spécifiques attachés à chaque personne. Pourtant, en ligne, il est complexe et parfois risqué de partager ces attestations, car il existe peu de normes informatiques établies pour garantir la fiabilité et l'interopérabilité du partage de telles qualités et informations personnelles. Pour répondre à cette problématique, le modèle de données des attestations vérifiables (« verifiable credential – VC ») offre un nouveau mécanisme permettant l'expression sécurisée et vérifiable de données d'identité en ligne, en préservant la confidentialité des informations grâce à de nouvelles méthodes cryptographiques compatible avec les infrastructures informatiques traditionnelles. Ces attestations numériques peuvent contenir d'innombrables attributs comme des images, des permissions, des consentements, des déclarations, ou encore des obligations contractuelles pour ne citer que quelques exemples de leurs applications possibles. Une attestation vérifiable permet ainsi à son émetteur d'émettre un ensemble de revendications vérifiables auprès de services en ligne. Plus précisément, cette dernière est un fichier numérique - normé par la DIF (« Decentralized Identity Foundation – DIF ») - qui contient des déclarations et des preuves d'informations comme des clés cryptographiques, des noms, des titres ou des qualifications concernant une entité (personne physique, morale ou objets connectés). Pour rappel, un VC peut être délivrée par une ou plusieurs entités (des

[997] W3C, « Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation. A new tool to empower everyone on the web with privacy-respecting online identity and consent-based data sharing », traduction libre de l'anglais, Press release, *op. cit.*, à l'adresse suivante
[998] V. *infra*, II, Titre 2, 1.4

émetteurs) et vérifiée par toute autre entité (les vérificateurs). Une attestation vérifiable est ainsi un justificatif inviolable dont l'auteur et son contenu peuvent être vérifiés par des méthodes cryptographiques. D'après une publication en 2022 de la société Gartner à propos des cycles d'innovation des technologies de l'identité numérique (*v.* Annexe 9), les attestations vérifiables sont actuellement dans une phase de « *creux de la désillusion* », dont le « *plateau de productivité* » serait atteint d'ici 2 à 5 ans. Cette recherche suggère plutôt que ces attestations 3.0 sont en phase de pré-industrialisation, avec certaines grandes plateformes de réseaux sociaux comme LinkedIn qui commencent à proposer – en partenariat avec Microsoft - ce nouveau standard numérique depuis 2023[999]. Complémentaires aux DID susvisés, ces attestations ont une forte probabilité d'être adoptées comme nouveau standard sur Internet. Il semble important d'opérer une précision sémantique et informatique entre une *attestation vérifiable* et une *attestation vérifiée* (« *Verifiable Presentation - VP* »). En effet, la première devient la deuxième après que son destinataire final - l'utilisateur - l'ait reçu puis signé cryptographiquement avec sa clé privée, au moyen de son portefeuille d'identité numérique décentralisée (PIND) qui est évoqué dans la partie suivante.

En droit communautaire, la récente proposition d'amendement du Règlement européen eIDAS (« eIDAS-2 » étudié plus loin), privilégie une qualification et une définition des attestations vérifiables (VC) et vérifiées (VP) en tant que « *attestations qualifiées d'attributs électroniques* ». Cette notion confond ainsi les attestations VC et VP, probablement en faveur d'une recherche de neutralité technologique et d'une portée générale spécifique à tout Règlement de l'UE (comme mentionné pour le Règlement MiCA et la proposition d'amendement du Règlement TFR déjà mentionnés). Outre Atlantique, le législateur de l'Etat de Californie a d'ores et déjà introduit dans un rapport datant de 2020[1000], puis dans un projet de loi adoptée en 2022, l'autorisation pour des institutions publiques de délivrer sous la forme d'attestations vérifiables légalement reconnues des documents d'identification listés à la section 1798.795(c) du Code civil californien[1001]. En septembre 2022, une loi complémentaire

[999] CHIK Joy, « LinkedIn and Microsoft Entra introduce a new way to verify your workplace », in *Microsoft Security Blog*. « Sur LinkedIn, les membres verront une option pour vérifier leur lieu de travail sur leur profil. En quelques clics sur leur téléphone, les membres peuvent obtenir leur carte d'employé numérique auprès de leur organisation et choisir de la partager sur LinkedIn. Après avoir envoyé le justificatif, une vérification du lieu de travail s'affichera sur leur profil. », traduction libre de l'anglais, disponible à l'adresse suivante

[1000] « California blockchain working group ». Juillet 2020, p.32. Disponible à l'adresse suivante, traduction libre de l'anglais : « La législature californienne devrait adopter une loi qui permette aux entités publiques à délivrer, en tant que justificatifs vérifiables autorisés, les documents d'identification visés à la section 1798.795(c) du code civil californien en tant que justificatifs vérifiables. Les personnes bénéficieraient de la possibilité de disposer de ces documents d'identification sous une forme numérique sécurisée et vérifiable sous leur contrôle. Les justificatifs vérifiables ne stockent aucune information personnelle substantielle sur la blockchain. Au lieu de cela, des identifiants décentralisés (DID) seraient stockés pour vérifier que le document a été valablement délivré et partagé avec le consentement de la personne concernée ».

[1001] Le 17 février 2022, le projet de loi N°1190 « Department of Technology: California Trust Framework » est introduit par le sénateur Hertzberg afin d'exiger, au plus tard le 1er janvier 2024, que le Department of Technology mette en place le « *California Trust Framework (CTF)* » afin de fournir des normes industrielles et des pratiques exemplaires concernant la délivrance d'attestations vérifiables permettant de vérifier les informations d'une personne ou d'une entité juridique. Le projet de loi exige que le CTF soit conçu, dans la mesure du possible, pour être interopérable avec d'autres cadres de confiance et de gouvernance gouvernementaux pour les attestations vérifiables. Traduction libre de l'anglais : « Les documents d'identification comprennent spécifiquement, mais sans s'y limiter, les éléments suivants : (1) Les permis de conduire ou les cartes d'identification délivrés conformément à la section 13000 du Code des véhicules. (2) Les cartes d'identité des employés ou des

relative à la technologie blockchain et visant à modifier la section 103526.5 du Code de la santé et de la sécurité[1002] californien a été adoptée. Celle-ci introduit la possibilité d'utiliser l'IND et tous types de technologies blockchains pour la délivrance d'informations d'état civil telles que les certificats de naissance, de décès et de mariage. Cela permet aux citoyens de prouver immédiatement leur identité via des QR codes ou avec des fichiers PDF enrichis, plutôt que de recourir à un envoi postal long de plusieurs jours, et également plus coûteux que ces nouvelles attestations numériques vérifiables. Finalement, cette qualification et reconnaissance juridique des VC en Californie implique une première qualification et reconnaissance légale inédite de cette nouvelle brique conceptuelle et technologique[1003], ce qui pourrait inspirer d'autres législations, notamment européennes (référence à eIDAS-2). Cette initiative serait bienvenue pour l'adoption régalienne d'une IND plus fiable, sécurisée et émancipatrice pour ses utilisateurs, et dont le législateur français devrait s'inspirer. Pour rappel, les VC ne stockent en principe aucune information personnelle directement sur une blockchain, mais tout au plus des identifiants décentralisés (DID), afin de vérifier que le document a été valablement délivré et partagé par une institution publique et avec le consentement de la personne concernée. D'après la CNIL, une attestation vérifiée n'est jamais stockée directement au sein d'une blockchain pour des raisons de capacité informatique limitée et de risques de non-conformité au RGPD. En cas de violation ou perte d'une attestation vérifiable, les dommages pour son titulaire sont limités, en raison d'une part de la possibilité pour son titulaire de la révoquer et d'autre part, en raison d'un système de divulgation partielle ou temporaire limitant les risques d'altération de l'identité numérique (usurpation d'identité, révocation forcée des attributs). A l'avenir, les VC devraient jouer un rôle important en contribuant à permettre aux individus de s'autodéterminer davantage et en relation de confiance avec des organisations accréditées et plus transparentes.

entrepreneurs. (3) Cartes d'identification délivrées par des établissements d'enseignement. (4) Cartes d'assurance maladie ou de prestations. (5) Cartes de prestations délivrées dans le cadre de tout programme d'aide soutenu par le gouvernement. (6) Licences, certificats, enregistrements ou autres moyens d'exercer une activité ou une profession réglementée par le Business and Professions Code. (7) Les cartes de_bibliothèque délivrées par toute bibliothèque publique ». California civil code, obligations : part 4 - obligations arising from particular transactions : title 1.80.a - Identification Documents : Section 1798.795. in *Justia Law*. Disponible à l'adresse suivante, *v.* également in *LegiScan*, disponible à l'adresse suivante

[1002] Bill Text - SB-786, « County birth, death, and marriage records: blockchain », consulté le 30 septembre 2022 à l'adresse suivante, traduction libre de l'anglais « La loi existante exige que le certificat contienne certaines informations et qu'il soit imprimé sur du papier de sécurité sensibilisé chimiquement, comme spécifié. Ce projet de loi autoriserait un enregistreur de comté à délivrer, sur demande, une copie certifiée d'un acte de naissance, de décès ou de mariage délivré conformément à ces dispositions, en plus de la méthode requise décrite ci-dessus, au moyen d'un justificatif vérifiable, tel que défini, utilisant la technologie blockchain, définie comme un système de données décentralisé, dans lequel les données stockées sont mathématiquement vérifiables, qui utilise des grands livres distribués ou des bases de données pour stocker des données spécialisées dans l'ordre permanent des transactions enregistrées ».

[1003] *Op. cit.* note 1069, California SB1190, disponible à l'adresse suivante, traduction libre de l'anglais, « un ensemble d'informations cryptographiquement sécurisées, créées conformément à des normes ouvertes [W3C], qui respectent et protègent toutes les protections existantes en matière de vie privée et constituent un moyen portable, contrôlé par l'utilisateur, de partager des informations d'une manière qui peut être authentifiée par des services accessibles au public ».

1.3.1.3 Un portefeuille numérique d'identité décentralisée (PIND)

La numérisation rapide de la société au cours de la dernière décennie a été largement alimentée par l'avènement de téléphones mobiles intelligents (smartphones)[1004]. En 2016, il y avait environ 3,67 milliards d'abonnements à ces ordiphones, un chiffre qui a maintenant doublé et il est estimé que d'ici 2026, 91% de la population mondiale aura accès à un smartphone[1005]. Fort de ce support quotidien désormais indispensable pour l'identité numérique des personnes, les normes de l'IND pourraient contribuer à résoudre le problème de sécurité soulevé par l'ANSSI en 2015, qui affirmait qu'il était « *illusoire d'espérer atteindre un haut niveau de sécurité avec un smartphone* »[1006]. En 2022, selon le Commissaire européen au marché intérieur, Thierry Breton[1007], la mise en place d'un portefeuille d'identité numérique européen (PIND) permettra aux citoyens de l'Union européenne de stocker et d'utiliser leurs données pour une variété de services, tels qu'un enregistrement dans un aéroport ou une location de voitures. Ces portefeuilles disponibles sur téléphones mobiles ou sur le Web offriront un service d'identification sécurisé et fiable pour les citoyens qui recherchent à la fois un haut niveau de sécurité et la simplicité des procédures administratives liées à leur identité civile. A ce stade, il convient de distinguer (i) les applications de téléphones mobiles actuelles déjà disponibles et fournies par certains services en ligne et les grandes entreprises technologiques (GAFAM/BAHTX), (ii) des applications mobiles de troisième génération qui implémentent les standards et mécanismes de l'IND qu'étudie cette partie. Les premiers sont ici désignés comme des portefeuilles d'identité numérique centralisés tandis que les seconds sont désignés en tant que portefeuilles d'identité numérique décentralisée (PIND)[1008]. En effet, si les fonctionnalités des premières permettent à leurs utilisateurs d'effectuer certaines actions relatives à leurs identités (Apple Digital ID, identité numérique fédérée déjà étudiée)[1009], celles des secondes utilisent des fonctionnalités cryptographiques distinctes et significativement innovantes. Il semble important de souligner que les identifiants décentralisés (DID) et les attestations vérifiables (VC) sont des données structurées et vérifiables, et non simplement des données partagées sous la forme de documents PDF comme cela est par exemple courant pour attester d'informations d'identité et de droits en ligne (CNIe, attestation de domiciliation). En recevant une multitude de ces DID et VC structurées et vérifiables directement via un PIND, il devient possible pour la première fois de compartimenter les

[1004] Selon la Commission d'enrichissement de la langue française, le terme « smartphone » doit être remplacé par celui de « mobile multifonction ». Cette thèse privilégie toutefois ce premier terme pour correspondre aux pratiques usuels du grand public. Ministère de l'Education Nationale et de la Jeunesse, disponible à l'adresse suivante

[1005] JP Morgan publication, « Payments are eating the world », [consulté en ligne le 28/10/2021], p.3.

[1006] Recommandation de l'ANSSI sur la sécurité relative aux ordiphones, 28 juillet 2015.

[1007] Commission Européenne, « La Commission propose une identité numérique fiable et sécurisée », [consulté en ligne le 10 novembre 2021].

[1008] Ce terme est introduit dans cette recherche mais il ne possède aucune traduction officielle pour l'instant. Notons qu'une autre dénomination possible consisterait à nommer ces applications d'identité décentralisée comme « *portefeuille d'identité numérique souverain - PINS* ».

[1009] Ces applications mobiles sont centralisées et leurs fonctionnements n'est pas *open source*, c'est-à-dire que leurs propriétaires [GAFAM] refusent de partager leur code informatique qui est protégé et privé, notamment sous couvert du secret commercial. Aussi ces acteurs peuvent revendre certaines données personnelles de façon plus ou moins opaque et consentie par leurs utilisateurs. Pour plus d'informations consultez « *Apple digital IDs come with conditions and costs* », sur *BBC News*, consulté en ligne le 1 décembre 2021.

informations d'identité des utilisateurs, ce qui permet un respect strict de leur vie privée et de leurs données à caractère personnel. Un PIND est au cœur de toute solution d'identité numérique décentralisée (IND) ou d'identité numérique auto-souveraine (INAS), car il permet aux mécanismes cryptographiques de fonctionner et de s'articuler ensemble. Cette application locale s'exécute directement sur l'appareil mobile de l'utilisateur et lui permet d'établir des relations avec des tiers en établissant des connexions chiffrées et P2P, c'est-à-dire sans le concours de multiples intermédiaires souvent inconnus pour l'utilisateurs. Les deux parties d'une transaction impliquant un PIND peuvent ainsi utiliser ce canal de communication chiffré pour échanger des informations vérifiées. L'émetteur d'informations d'identité peut envoyer une attestation vérifiable (VC) en quelques secondes à un utilisateur, qui peut ensuite la conserver librement sur son portefeuille décentralisé, dont les signatures électroniques permettent de créer une attestation vérifiée (VP) que l'utilisateur peut choisir de présenter ou non à des tiers soit pour accéder à des services et interactions en ligne ou en physique (contrôle douanier, de police). Chaque utilisateur peut ainsi vérifier l'identité de l'autre partie pour établir une relation de confiance basée sur ces preuves d'identité 3.0 qui sont articulés par un PIND pour l'utilisateur final. Ce dernier peut notamment conserver une trace de l'historique des informations partagées et faciliter l'exercice du droit à la protection de ses données[1010]. Étant donné que le PIND héberge plusieurs attributs et données d'identité, il est impératif de prévoir et de garantir la protection des données en cas de perte, de vol ou de destruction du dispositif de l'utilisateur. Les fonctionnalités logicielles d'un PIND peuvent varier selon les fournisseurs d'identité qui les développent, mais ils incluent souvent une variété de systèmes hybrides utilisant des protocoles de gestion d'identité numérique fédérée (2.0).

Les PIND sont similaires aux portefeuilles de crypto-actifs, car ils permettent la propriété et la gestion souveraine de clés cryptographiques. Toutefois, les cas d'usage ainsi que les acteurs de ces marchés sont très différents et requièrent une approche distincte et en adéquation avec leurs spécificités. A moyen terme, il est probable que ces deux types de portefeuilles numériques fusionnent pour assurer une réification des identités numériques financières et administratives des personnes sur une même application mobile. La Commission européenne a proposé certains standards que les fournisseurs doivent implémenter pour la standardisation d'un PIND (désigné en tant que « *EU Digital Identity Wallet – EDIW* »)[1011] conformément à l'amendement du Règlement eIDAS-2 évoqué plus loin. En 2022, le Conseil de l'UE a finalisé sa position concernant la mise en place d'un portefeuille d'identité numérique décentralisée dont le niveau de garantie sera considéré comme élevé selon eIDAS pour les États membres de l'UE. Une période de transition permettra la réutilisation des solutions d'identité numérique actuelles, telles que l'identité numérique centrée et fédérée. Depuis 2021, le consortium POTENTIAL

[1010] KOENIG Gaspard, « La propriété de soi », « En choisissant en amont, dans un smart wallet, quelles données j'accepte de partager et à quelles conditions, je pourrais réinstaller une forme de libre arbitre dans l'univers du nudge », consulté en ligne le 18 novembre 2021, p.10.
[1011] V. *infra*, II, Titre 1, 2.1.1.1.a, v. *op. cit.* « Blockchain et Digital ID Wallet : vers une identité européenne décentralisée ? », Ateliers Les Temps Numériques, EHESS, 2022, disponible à l'adresse suivante

sélectionné par la Commission européenne et composé de 19 États membres assure la coordination de six cas d'usage pilotes pour le nouveau prototype de portefeuille d'identité numérique européen[1012]. Ce prototype et ces cas d'usage seront testés entre 2024 et 2025, puis de nouvelles expérimentations seront implémentés à partir d'avril 2025[1013]. En parallèle, le consortium NOBID[1014], qui comprend l'Allemagne, l'Italie et quelques pays d'Europe du Nord, travaille sur le développement d'un portefeuille d'identité numérique européen visant à permettre une interopérabilité bancaire et financière. En matière de responsabilité, il semble dans un premier temps que celle des fournisseurs de PIND ne soit pas systématiquement engagée au regard des données qui transitent par ces derniers. En cas de perte, de vols ou d'usurpation d'identité, si en principe, la responsabilité de la vérification des données devrait être imputée au fournisseur du système, au fabricant du PIND ou au fournisseur de données ayant provisionné des VC sur le PIND, l'utilisateur peut aussi - dans certains cas - endosser une part de cette responsabilité si une négligence ou faute de son fait est rapportée (cas d'exposition de ses données sans précaution). Si les technologies blockchains permettent nativement un horodatage et des signatures cryptographiques utiles pour ses utilisateurs, notamment pour prouver la détention de fonds ou encore pour voter, il existe de nouveaux mécanismes cryptographiques plus sophistiqués pour prouver une information avec certitude sans révéler la moindre information au préalable. Finalement, toujours selon la société Gartner et la publication en juillet 2022 de son graphique des cycles d'innovation concernant les technologies de l'identité numérique, le concept de PIND aurait atteint le « *sommet de son attractivité* »[1015], une perception en partie surprenante en l'état de ce segment de marché qui est plutôt en phase de pré-industrialisation face à l'adoption du cadre de confiance eIDAS-2. De façon pragmatique, la société Gartner estime qu'un « *plateau de productivité* » sera atteint d'ici cinq à dix ans pour cette brique technologique.

1.3.1.4 Sauvegarde, récupération et responsabilité des attributs d'une identité décentralisée

Lorsqu'une personne possède le pouvoir de contrôler et de gérer ses données, il lui appartient de les protéger et de les contrôler pour éviter toute perte accidentelle comme la perte de son appareil informatique ou de ses clés cryptographiques lorsqu'elle les conserve. Comme pour tout autre support d'identité, il est nécessaire d'avoir un mécanisme de sauvegarde fiable pour restaurer les données accumulées ou perdues en cas de besoin. Si un tel moyen de sauvegarde n'est pas disponible, l'utilisateur risque de ne pas être en mesure de restaurer tout ou partie de ses attributs accessibles via son PIND. En

[1012] Voici les cas d'usage compris dans ce consortium : (i) ouverture de compte bancaire, (ii) attestation de permis de conduire électronique, (iii) service(s) public(s) en ligne, (iv) signature électronique, (v) prescription électronique ou (vi) enregistrement électronique de carte SIM. « Consortium POTENTIAL : vers un portefeuille européen d'identité numérique », consulté le 20 décembre 2022. Pour plus d'informations consultez le site internet à l'adresse suivante
[1013] *Ibid*. Consortium POTENTIAL.
[1014] NOBID Consortium, 14 décembre 2022, pour plus d'informations consultez l'adresse suivante
[1015] V. Annexe 9.

pratique, étant donné que les identités numériques décentralisées seront probablement rattachées à la source à des tiers de confiance 2.0 (CNI, passeports), il est probable que les mécanismes de sauvegarde et de récupération des attributs 3.0 générés impliquent à nouveau ces mêmes acteurs, c'est-à-dire une forme de recentralisation par les mêmes institutions et services publics que nous avons par exemple déjà évoquées (FranceConnect, etc.). Il existe donc plusieurs options de sauvegarde concernant des attributs d'identités décentralisées (DID, VC) qui varient en fonction des exigences, des procédures et de la gouvernance spécifique à chaque cas d'usage. De façon basique, la sauvegarde peut prendre la forme d'un fichier chiffré[1016] contenant les clés cryptographiques[1017] et d'autres informations associées directement sauvegardé et conservé par l'utilisateur. Cela implique que l'utilisateur stocke le fichier dans un conteneur sécurisé plus ou moins intuitif d'accès et spécifiquement développé par des fournisseurs d'identité, puis qu'il sauvegarde par exemple sa phrase de récupération unique et personnelle (clé privée). Toutefois, cela suggère une importante responsabilité pour l'utilisateur qui doit posséder une connaissance suffisante pour maîtriser et conserver ses clés cryptographiques. En d'autres termes, ce fichier chiffré peut être stocké localement sur l'appareil de l'utilisateur dans le cas d'une identité auto-souveraine (INAS), étudiée dans le paragraphe suivant, ou bien téléchargé depuis un serveur externe, certes informatiquement centralisé, mais légalement garanti car hébergé par un tiers de confiance certifié comme un « *cloud souverain* »[1018]. Cette seconde option mixte consiste à utiliser un mécanisme de fractionnement de la clé privée en plusieurs parties que l'utilisateur peut ainsi envoyer à différents contacts de confiance (membres de la famille, notaires, avocats). Cette procédure serait facile à exécuter via un PIND, mais elle peut ne pas être viable pour les personnes qui n'ont pas accès à plusieurs appareils ou qui sont isolées. Une troisième et dernière option consiste à sauvegarder les données auprès d'un tiers de confiance qui garanti seule la sauvegarde et permettra la récupération des données pour l'utilisateur final en cas de perte de ses accès. En 2022, il n'existe pas encore d'unanimité concernant ces méthodes d'authentification et la façon d'éviter les abus de la part dedits tiers de confiance 3.0, supposés plus fiables qu'avec l'utilisation d'outils 2.0. À court terme, il est probable que cette troisième option soit la plus utilisée par les fournisseurs d'identité pour leurs premières implémentations de portefeuilles d'identité décentralisée, notamment pour assurer une expérience utilisateur plus simple et intuitive que la première option certes plus libératrice pour les internautes, mais plus complexe et donc utopique. En principe, chaque fournisseur d'une solution d'identité décentralisée devrait proposer plusieurs options

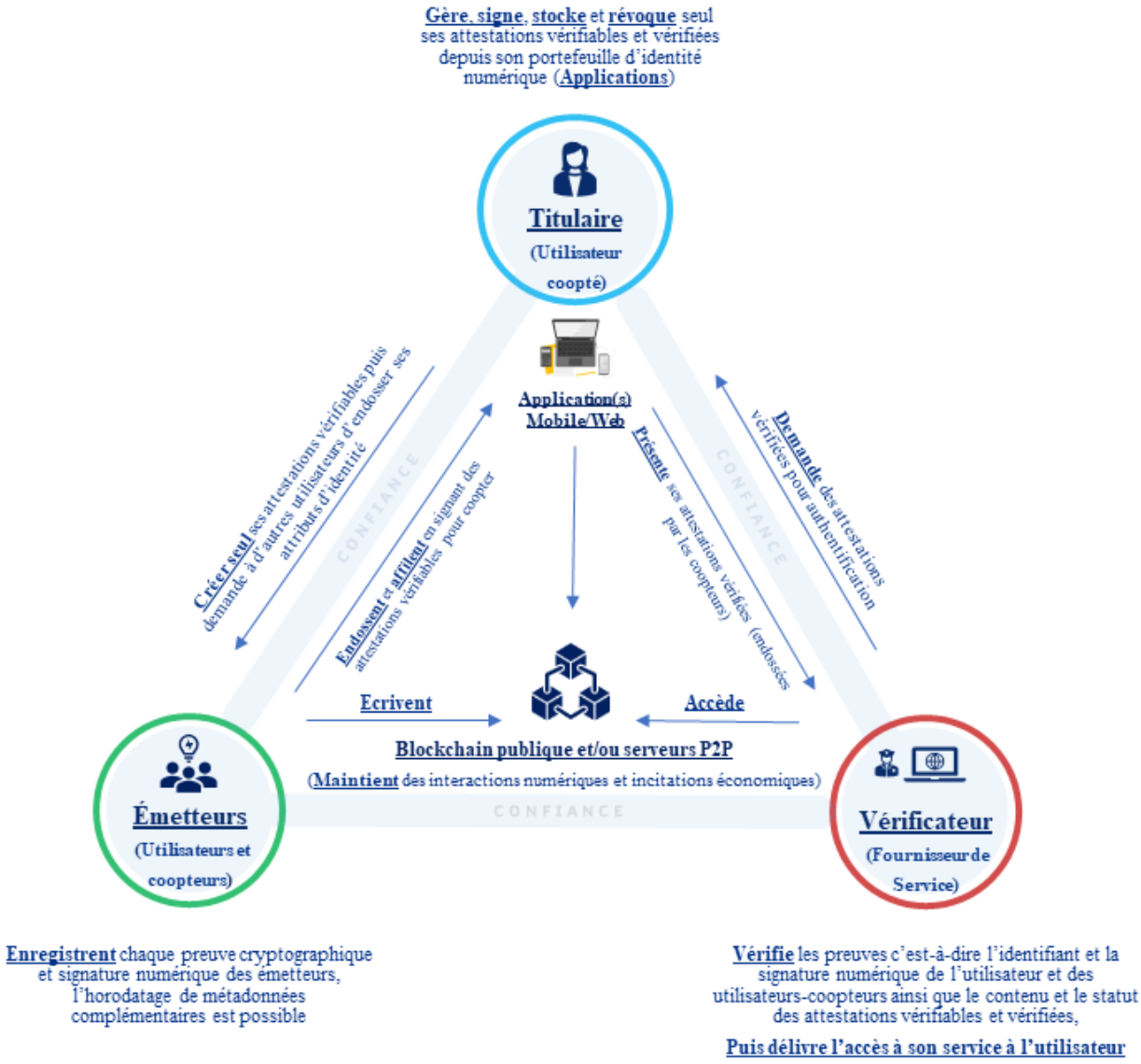
[1016] Le terme « déchiffrer » est à privilégier face à celui de « décrypter » qui est souvent utilisé à tort. Pour plus d'informations, consultez le lien suivant

[1017] Pour qu'une clé soit restaurable et lisible par un être humain, elle est donnée sous la forme d'une phrase (également appelée « *phrase de récupération* » ou « *graine mnémonique* ») généralement composée de 12 ou 24 mots. Ce mécanisme est utilisé depuis plus d'une décennie par les portefeuilles de crypto-actifs. Pour plus d'informations sur ces portefeuilles, consultez l'adresse suivante. Pour comprendre le caractère aléatoire et 'privé' d'une *clé privée*, consultez le lien suivant

[1018] Il est fait référence à l'initiative européenne nommé « Gaia-x » ainsi qu'à la norme et liste des *prestataires d'informatique en nuage qualifiés* délivrée et mise à jour par l'ANSSI. En théorie, ces *clés* sont indispensables pour restaurer seul et avec succès les données rattachées à un portefeuille d'identité numérique décentralisé. En pratique, les risques de pertes ou de vols de ces identifiants sont nombreux et complexes à éviter pour un utilisateur grand public. Ainsi, les fournisseurs d'identité se réserveront très probablement le droit de conserver ces clés d'une façon ou d'une autre afin de proposer une sauvegarde de secours en cas de besoin.

de sauvegarde de façon cumulative et de façon le plus intuitif possible pour ses utilisateurs. Il convient de rappeler que les fournisseurs d'identité devront se conformer aux nouvelles règles de l'amendement eIDAS-2, étudié plus loin, notamment en intégrant un élément sécurisé, c'est-à-dire un composant de sécurité physique intégré à l'appareil mobile de l'utilisateur, nécessairement relié à son PIND et à son périphérique informatique (téléphone mobile). Cette exigence matérielle imposée aux fournisseurs d'identité, au bénéfice d'un stockage plus sécurisé des clés cryptographiques des utilisateurs, pourrait significativement retarder l'adoption des solutions européennes d'IND. Finalement, la responsabilité de la gestion et de l'exactitude de ces attributs 3.0 (VC, DID) repose sur les différentes parties impliquées dans la chaîne d'attribution et de vérification d'une identité décentralisée. Dans les versions semi-centralisées que cette étude suggère les plus courantes à court et moyen termes pour l'identité numérique de troisième génération, informatiquement distribuée, les fournisseurs d'identité ont la responsabilité de vérifier l'exactitude des informations fournies par chaque utilisateur en s'assurant que les attributs sont pertinents pour des contextes d'utilisation préalablement ciblés. Finalement, dans une version fortement décentralisée (cas de l'INAS), les titulaires d'attributs d'identité ont la responsabilité de mettre à jour leurs attributs en temps opportun, de veiller à ce qu'ils soient exacts et que leur stockage soit pérenne. Les destinataires d'attributs ont également la responsabilité de vérifier l'exactitude des attributs avant de les utiliser pour toute action ou décision liée à une identité numérique. La transparence et la collaboration entre les parties d'une IND, exposées ci-dessous, semblent aujourd'hui essentielles pour garantir que des attributs d'identité décentralisée soient fiables, précis et pertinents selon chaque contexte d'utilisation.

1.4 L’identité numérique auto-souveraine (INAS) au paroxysme de l’identité décentralisée



L'identité numérique auto-souveraine (INAS) repose sur le principe fondamental que chaque individu devrait être le seul responsable de la délivrance et de la gestion de sa propre identité numérique, sans dépendre d'une tierce partie. Dans ce modèle troisième génération du concept d’identité numérique que nous avons étudié, la décentralisation est poussée à l'extrême pour tendre vers une autonomie informatique et sociale en matière d'identification et d'authentification numérique, comme l’illustre ci-dessus le triangle de confiance spécifique à l’INAS. Les utilisateurs sont ici capables d'émettre et de gérer de manière totalement autonome et indépendante leurs attestations vérifiables et leurs identifiants

décentralisés[1019]. L'INAS permet aux individus de privatiser leur identité numérique à leur seule discrétion sur le plan informatique, social, voire économique, sans solliciter aucune autorité pour la délivrance d'un attribut d'identité numérique, contrairement au modèle d'identité numérique distribuée (IND)[1020] illustré par le schéma - relativement similaire - étudié auparavant. En 2020, le spécialiste et Professeur en droit Ignacio Alamillo Domingo propose une définition assez précise de l'INAS : « *l'adoption des principes de la SSI implique* (...) *une complexité accrue en matière de gestion de la confiance ainsi qu'un basculement depuis des cadres de garantie de la confiance hiérarchisés ou fédérés* (...) *vers des modèles de confiance socio-réputationnels basés sur des cadres de garantie consensuels notamment grâce à l'utilisation de méthodes quantifiables pour agréger la confiance en matière de revendications et d'identités numériques* »[1021]. Cette importante personnalisation cryptographique semble ainsi au service des utilisateurs et internautes en favorisant l'exercice en ligne de certains de leurs droits fondamentaux (comme l'art. 10 et 11 de la DDHC)[1022]. En partant du postulat qu'une majorité d'internautes et de citoyens apprennent à utiliser une paire de clés cryptographiques publique et privée, l'identité numérique auto-souveraine présenterait par conception certains avantages informatiques et juridiques pour ses utilisateurs, comme le consentement, le pseudo-anonymat, l'interopérabilité, la propriété et la portabilité cryptographique sur leurs données à caractère personnel. Si l'identité auto-souveraine (INAS) est pour l'identité distribuée (IND) ce que Bitcoin est à la blockchain, c'est-à-dire une première application hautement décentralisée et socialement disruptive, alors l'INAS sera probablement confrontée à des réactions ainsi qu'à des défis sociaux, techniques, juridiques et politiques probablement similaires. Parce ce qu'elle ouvre la porte à un nouvel écosystème identitaire indépendant de la supervision et de l'approbation directe des gouvernements, il est probable que le concept d'identité numérique distribuée, semi-centralisée et hybride, devienne plus largement adopté à moyen terme que cette notion d'INAS entièrement sous le contrôle cryptographique des personnes. Cependant, bien que l'INAS conforte l'idée d'une identité numérique universellement

[1019] Sémantiquement, il existe plusieurs traductions possibles depuis l'anglais « *Self Sovereign Identity* » vers le français. Début 2023, la traduction en français du texte de la proposition d'amendement du Règlement eIDAS (« eIDAS-2 ») propose une première traduction juridique dans son considérant (34) avec le terme de « *solutions d'identité autonomes* ». Cette thèse privilégie le terme « *d'identité numérique auto-souveraine* » et son acronyme français « INAS » à son équivalent anglais « Self-Sovereign Identity - SSI ». En effet, l'acronyme « SSI » est couramment utilisé dans le secteur informatique pour désigner la « Sécurité des Systèmes d'Informations – SSI », il peut donc difficilement être réutilisé comme acronyme. Un constat similaire est possible concernant l'acronyme français « IAS » déjà utilisé par l'Agence Nationale des Titres Sécurisés (ANTS) pour désigner l'« Identification, Authentification et Signature – IAS ». L'utilisation de ces derniers acronymes pourrait ainsi être source de confusion à l'égard de ce concept d'identité numérique auto-souveraine. v. également « Proposition d'une taxonomie francophone pour l'identité décentralisée », 2021, ⟨hal-03398096⟩.

[1020] Le terme d'*identité numérique distribuée (IND)* fait référence dans cette partie et celles qui suivent à celui d'*identité numérique décentralisée (IND)*. Il s'agit du même concept, l'acronyme « *IND* » pouvant faire référence à ce concept sans distinction. Ce changement de terme vise néanmoins à éviter un contre-sens dans cette partie concernant le fait qu'une identité numérique décentralisée n'est en réalité pas complètement « *décentralisée* » sur le plan informatique, mais plutôt « *distribuée* » par rapport à une INAS qui est supposée complètement décentralisée comme mentionné dans cette partie.

[1021] Dr. ALAMILLO DOMINGO Ignacio, « SSI eIDAS Legal Report », for European Commission, traduction libre de l'anglais, consulté en ligne le 06/08/2021, p. 26.

[1022] Art. 10 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 : « Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi », et *v.* Art. 11 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre à l'abus de cette liberté dans les cas déterminés par la loi ».

accessible sans tiers de confiance, il semble important de ne pas exacerber ni effacer la diversité culturelle qui existe déjà en ouvrant la voie à la revendication d'inombrables singularités et appartenances en ligne. Comme le souligne le sociologue Allemand Andreas Reckwitz « *la singularisation peut mener à de nouvelles formes d'inégalité entre ceux qui s'imposent dans un monde de singularités et ceux qui n'y parviennent pas faute de moyens* »[1023]. Cette volonté sociale de singularisation de nos êtres en ligne pourrait-elle faire émerger une culture libertarienne de l'INAS similaire à celle existante dans l'univers des crypto-actifs ? Cela semble plausible en raison de la proximité informatique et sociale de ces deux sphères, dont la convergence apparait comme inévitable. Toutefois, si l'INAS peut contribuer à une forme de libération de l'identité des personnes en ligne, il s'agit de veiller à ce qu'elle n'exacerbe pas les inégalités sociales, culturelles et économiques, c'est-à-dire qu'elle respecte le droit positif pour ne pas empiéter sur les droits d'autres personnes, notamment sous couvert d'anonymat. Ce paradoxe doit ainsi être souligné et pris en compte lors de la conception et des interactions entre des solutions d'IND et d'INAS, tant par les fournisseurs d'identité privés que par les services de l'Etat. A plus long terme, il est supposé que l'identité numérique auto-souveraine s'imposerait au sein d'environnements numériques initialement supposés peu régulés comme les Métavers[1024], le marché des crypto-actifs ou encore dans certains systèmes d'échange pair à pair (*v.* Finance Décentralisée, DAO, tbDEX[1025]). Ces concepts et briques technologiques peuvent se confondre voire fusionner avec des identités auto-souveraine afin de former de nouveaux cas d'usage en ligne. L'INAS offre également une solution pour créer des preuves d'existence universelle décentralisées. Cependant, cela représente à la fois un défi informatique et sociétal pour les tiers de confiance traditionnels du secteur de l'identité numérique, et une opportunité sociale et juridique pour la liberté numérique des internautes. Bien que la conception d'une telle humanité numérique décentralisée soit désormais possible grâce à des solutions 3.0 comme le projet Proof of Humanity (PoH) déjà mentionné, un équilibre entre les libertés numériques et la stabilité sociale doit être trouvé et discuté. Il est crucial de ne pas tomber dans l'illusion d'un contrôle total par les individus, finalement soumis au contrôle numérique d'entités oligopolistiques similaires à celles d'ores et déjà en activité dans le Web 2.0 et infiltrant progressivement le Web 3.0. Il est important de se rappeler qu'Internet était censé libérer les personnes sur le plan philosophique, et non pas les enfermer.

En matière de responsabilité, une solution d'identité numérique distribuée (IND)[1026] n'implique pas les mêmes effets juridiques qu'une solution d'identité numérique auto-souveraine (INAS). Le schéma

[1023] RECKWITZ Andreas, « La singularisation est devenu un phénomène de masse », 2022, in *Libération*, chercheur rattaché au Centre Georg Simmel (EHESS/CNRS), disponible à l'adresse suivante
[1024] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, « Mission exploratoire des Métavers », 2022, disponible sur vie-publique.fr
[1025] V. *infra,* II, Titre 2, 2.3
[1026] *Op. Cit.* Le terme *d'identité numérique distribuée* (IND) fait ici référence et écho à celui *d'identité numérique décentralisée* précité. Il s'agit du même concept, l'acronyme « *IND* » pouvant faire référence à ce concept sans distinction. Ce changement de terme vise néanmoins à éviter un contre-sens dans cette partie concernant le fait qu'une identité numérique décentralisée n'est en réalité pas complètement « *décentralisée* » sur le plan informatique, mais plutôt « *distribuée* » par rapport à une INAS qui est complètement décentralisée comme mentionné.

présenté précédemment diffère du schéma ci-dessus en ce sens que les DID et les VC ne sont pas validés par des serveurs centralisés ou distribués gérés par des entités étatiques ou privées. Au lieu de cela, ils sont directement vérifiés entre les utilisateurs et une blockchain ouverte comme Bitcoin[1027] ou Ethereum[1028]. Dans un système d'INAS, aucune entité publique ou privée n'est légalement responsable du bon fonctionnement de l'identification, de l'authentification et de l'autorisation d'accès à des services numériques par les utilisateurs. En théorie, les utilisateurs ont donc la responsabilité exclusive de gérer raisonnablement leurs identifiants numériques (DID, VC) ainsi que leur PIND (y compris les clés cryptographiques), comme s'ils géraient des crypto-actifs soit sans recourir à de multiples tiers de confiance. Cependant, il est illusoire de penser qu'une identité numérique, en particulier sociale, peut exister sans l'implication d'un mandataire reconnu, qu'il s'agisse d'une autorité publique ou privée. En effet, en cas de litige impliquant des identités exclusivement auto-souveraines, un titulaire pourrait rencontrer des difficultés à prouver la défaillance de son système d'INAS qui est décentralisé de bout en bout et qui ne repose sur aucun tiers de confiance. Dans ces cas, un juge pourrait considérer qu'une solution d'IND avec un tiers de confiance aurait été plus fiable et donc faire peser la responsabilité sur le titulaire de l'identité numérique en conflit, car il en avait le contrôle exclusif. Les développeurs ou les acteurs des blockchains publiques ou des solutions d'INAS pourraient difficilement être tenus responsables dans ce cas précis. En réalité marginal, cette situation ne pourrait toutefois pas s'appliquer à tous les citoyens en raison de compétences informatiques bien souvent inégales, en référence à « *la fracture numérique* »[1029] qui s'accroît. Pour réussir, l'identité numérique auto-souveraine nécessiterait à court et moyen termes une nécessaire acceptation de la part des gouvernements et des institutions, qui ont pourtant tendance à rejeter les technologies les plus décentralisées sur le plan informatique et social. A cet égard, il est possible qu'une forme de défiance entre des attributs d'INAS et d'IND se manifeste sur les marchés de l'identité numérique. Cela signifie que des fournisseurs d'identité numérique hybrides 2.0 et 3.0 pourraient créer des 'prédicats' ou des 'restrictions' concernant d'autres attributs issus d'INAS qui doit démontrer son bienfondé technique, juridique et politique, pour les personnes et leurs futurs comportements numériques. Aujourd'hui, il est encore tôt pour une implémentation informatique et internationale d'INAS, mais de nombreux développements sont prometteurs et rapides au sein des communautés les plus décentralisées du Web 3.0. Néanmoins, il semble bien qu'une prolifération de solutions d'identité auto-souveraine soit tributaire d'une compréhension et d'une reconnaissance légale de certaines de ses composantes informatiques, comme semble le démontrer l'histoire de l'évolution d'Internet étudiée en amont de cette thèse.

[1027] V. Annexe 3, Focus 1 à 6.
[1028] V. Annexe 6, Focus 2. V. également *infra*, II, Titre 2, 2.1
[1029] BEN YOUSSED Adel, « Les quatre dimensions de la fracture numérique », in *Réseaux*, 2004, disponible en ligne

1.5 Facteurs et limites d’adoption de l’identité numérique décentralisée

Au cours des dernières années, des progrès significatifs ont été accomplis dans le domaine de l'identité décentralisée par les gouvernements, les entreprises et les institutions tels que le W3C et la DIF, grâce à des projets pilotes qui ont utilisé les normes de l'identité numérique distribuée/décentralisée et les technologies blockchains (principalement fermées). Les avantages technologiques et sociaux de l'utilisation d'une IND sont progressivement mis en évidence. La récente proposition de modification du Règlement eIDAS suggère que l'identité décentralisée permet de considérablement réduire les coûts associés à la vérification d’une identité, indépendamment du niveau de garantie et de confiance requis par ce Règlement (niveau faible, substantiel ou élevé). Par exemple, une personne peut effectuer une vérification en ligne de ses documents d'identité officiels une seule fois, puis recevoir des attestations vérifiables et vérifiées associées (VC et VP), qu'elle peut ainsi utiliser pour plusieurs services en ligne sans avoir besoin de se re-identifier à chaque fois. Les mécanismes de l'identité décentralisée permettent également de se conformer aux exigences du RGPD, ce qui réduit davantage les coûts associés à la conformité à la protection des données personnelles. Cependant, l’adoption des standards mentionnés de l’identité numérique décentralisée (VC, VP, DID, PIND) est encore loin d’atteindre son potentiel sur le plan informatique. Cela s’explique par des difficultés à trouver un modèle commercial fiable et pérenne pour les fournisseurs d’identité et de services. Lorsqu’une nouvelle technologie émerge, la recherche d’une disruption informatique et sociale prime à court terme sur la recherche d’une rentabilité économique ou sur la recherche d’une conformité juridique. Les solutions actuelles d’IND ne sont pas encore satisfaisantes pour les consommateurs comme pour les entreprises et leurs avantages varient de façon importante selon leurs segments de marché. La recherche de modèles commerciaux non intrusifs et transparents, par les fournisseurs d’identité décentralisée, semble aussi être un élément fondamental à court et à long terme pour assurer le succès de cet écosystème prometteur.

Le concept d’identité numérique décentralisée doit faire face à plusieurs obstacles structurels. Tout d'abord, il existe des défis informatiques liés à la complexité des mécanismes cryptographiques 3.0. Ensuite, certains enjeux juridiques tels que la qualification, la reconnaissance et l'harmonisation juridique des IND, y compris des blockchains, sont à prendre en compte pour l’avenir de ce Web 3.0 dans lequel elle s’inscrit. Les enjeux politiques sont également présents, ne serait-ce parce que l'expression « décentralisé » demeure souvent associée à tort aux crypto-actifs en France, ce qui démontre le besoin et l’importance d’une éducation des corps législatifs et exécutifs. Enfin, il y a les enjeux expérientiels, c’est-à-dire la simplicité de la gestion d’une identité numérique offerte par les attestations vérifiables et vérifiées (VC/VP) qui ne doivent pas entraîner une surcharge ou expérience peu intuitive pour accéder à des services en ligne. Les utilisateurs doivent également faire un usage raisonnable de leur VC/VP en ligne pour éviter toute utilisation excessive de leurs attributs d’identité. Pour garantir une identité décentralisée fiable et respectueuse de la vie privée, il est nécessaire de concevoir des solutions qui respectent les normes de confidentialité et de sécurité tout au long de leur

cycle de vie et en vertu du concept de « *confidentialité programmée* » initialement introduit par la CNIL[1030]. Il est également crucial d'identifier et de limiter les acteurs malveillants qui pourraient proposer des portefeuilles d'identité décentralisée à des fins trompeuses ou illégales. La décentralisation de l'information des utilisateurs est une autre mesure de sécurité importante pour minimiser les risques de piratage. En outre, il est important d'associer des normes strictes à ces solutions pour garantir le respect des droits en ligne. D'après la théorie de diffusion de l'innovation d'Everett Rogers[1031], la diffusion d'une nouvelle technologie dépend de cinq caractéristiques. Il est soutenu que l'identité numérique décentralisée remplit d'ores et déjà partiellement ces cinq critères : (i) l'avantage relatif, (ii) la compatibilité, (iii) la complexité, (iv) la démontrabilité et (v) l'observabilité. De plus, la loi de Lindy[1032] semble pertinente à appliquer à l'identité numérique décentralisée, ce qui signifie que plus l'IND sera utilisée dans le temps, plus sa durée de vie sera longue et son taux d'échec diminuera. En fin de compte, il semble que l'identité décentralisée finira par s'imposer, mais la question est de savoir où, quand et à quel rythme.

1.5.1 Les sciences informatiques et les connaissances ouvertes au centre de l'IDN

1.5.1.1 L'importance des logiciels libres et codes sources ouverts

En avant-propos, il convient de faire une distinction entre la notion de transparence mentionnée tout au long de cette étude, et celle d'explicabilité[1033] pour ce qui concerne des programmes informatiques 2.0 et surtout 3.0. En effet, la transparence suppose que le code informatique soit ouvert et public et donc susceptible d'être examiné par de nombreux pairs à travers le monde (développeurs, chercheurs). L'explicabilité, quant à elle, se réfère à la compréhension et à l'intelligibilité du fonctionnement, des interactions et des finalités d'un programme informatique. Dans l'idéal, ces deux notions doivent être combinées pour assurer une confiance numérique maximale pour tous les acteurs impliqués dans des technologies 3.0 (fournisseurs, utilisateurs, législateurs). A l'origine, les logiciels[1034] étaient plus ou moins libres selon les souhaits de leurs créateurs, la nature même d'un logiciel permettant sa distribution

[1030] Le décret publié le 31 août 2019 au Journal Officiel offre de nouveaux équivalents français pour le terme anglophone de la « privacy by design » qui se traduit désormais par « confidentialité programmée », « Vocabulaire du droit (liste de termes, expressions et définitions adoptés) », JORF n°0202 Texte n° 91, ressource disponible à l'adresse suivante
[1031] BENOIT-GUILBOT Odile, « Rogers Everett M., Diffusion of innovations », 1964, *Rev. Fr. Sociol.*, 5, in Persée, 1964, consulté le 5 août 2021, p.15, disponible en ligne
[1032] ELIAZAR Iddo, « Physica A: Statistical Mechanics and Its Applications », 2017, vol. 486, issue C, 797-805. La *loi de Lindy* stipule que plus un concept non périssable, tel qu'une technologie pérenne ou une idée, a survécu longtemps et est encore utilisé, plus il a de chances d'avoir une longue durée de vie. *L'effet Lindy* montre que, lorsque cette loi s'applique, le taux d'échec d'une technologie diminue avec le temps. Selon cette théorie, l'identité décentralisée n'a pas encore atteint son seuil critique, contrairement à certaines blockchains publiques comme Bitcoin et peut-être Ethereum. Cependant, notre étude suggère que l'identité décentralisée bénéficiera de cette loi une fois qu'elle aura été massivement adoptée (ce qui nécessite du temps).
[1033] *Op. cit.*, JEAN Aurélie, « Les algorithmes font-ils la loi ? », position de lecture dans le livre : 61%.
[1034] BRAUDO Serge, « Logiciel – Définition », in *Dictionnaire Juridique*, « Un 'logiciel' est, selon le vocabulaire officiel de l'informatique, 'l'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données' (JORF 17/01/1982). », disponible à l'adresse suivante

et sa modification[1035]. Cependant, lorsque les fournisseurs de logiciels ont commencé à se différencier des fournisseurs de matériel informatique, des licences contractuelles[1036] ont été introduites pour encadrer les conditions d'utilisation des logiciels, tels que des droits d'accès au code source soit des droits de modification. Le concept de « *logiciel libre* », également connu sous le nom de « *free software* » en anglais, a pris de l'importance depuis les années 2000 et est aujourd'hui considéré par les spécialistes comme un « (…) *mélange de produit (objet fini) et de service (de gestion de l'adaptation et de l'évolution de cet objet). C'est précisément cette dualité qui est à l'origine et l'intérêt du logiciel libre.* »[1037]. Richard Stallman, un chercheur et programmeur américain du MIT, est considéré comme le fondateur du concept de logiciel libre. En 1985, il a défini quatre libertés essentielles associées au logiciel libre et a créé la « *Free Software Fondation* »[1038] pour défendre ces libertés en attribuant des licences logicielles spécifiques. Premièrement, il s'agit de la liberté d'exécuter le logiciel sans limitation d'utilisation, de finalité ou de territorialité. Deuxièmement, la liberté d'étudier le fonctionnement du logiciel, d'en obtenir les codes sources, de les modifier ou de les adapter à des besoins spécifiques. Troisièmement, la liberté de redistribuer le logiciel à tout tiers, gratuitement ou moyennant une rétribution, sans aucune restriction. Enfin, quatrièmement, la liberté de publier et de diffuser les modifications apportées à un programme original. Pour garantir ces libertés, l'accès au code source du logiciel libre est une condition essentielle, et le logiciel doit être disponible sous la forme de sources éditables. Le principe du logiciel libre offre aux utilisateurs la liberté d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel. Cette liberté permet aux utilisateurs de contrôler le programme et de l'adapter à leurs besoins, individuellement et collectivement. Un parallèle peut être fait en droit français avec les licences de « *logiciel libre* », l'auteur du programme informatique, dans cette hypothèse, ne pouvant interdire l'écriture d'un nouveau programme aux fonctionnalités proches, compatibles et interopérables avec les standards informatiques du programme initial. Les logiciels libres sont protégés par le droit d'auteur et les dispositions du Code de la propriété intellectuelle. Ces licences permettent aux utilisateurs de copier, modifier et distribuer le logiciel librement, mais exige que toutes les versions modifiées soient également libres. Ces licences sont très répandues[1039] et les plus protectrices à ce jour. De cette manière, un plus grand nombre de personnes peuvent contribuer au(x) code(s) source(s) ouvert(s), ce qui favorise l'innovation et la sécurité des infrastructures informatiques et des services en ligne. Dans le Web 3.0 et plus généralement au sein de l'univers informatique, les

[1035] VALERIAN François, COMBY Gérard, KAPPELMANN Alexia, GIMON Magali, et al. « Annales des mines n°18 sur les enjeux numériques : Propriété et gouvernance du numérique », série trimestrielle - N°18 - Juin 2022, Institut Mines-Télécom, « […] l'approche du logiciel libre ne représente pas un déni de la propriété intellectuelle, mais une nouvelle façon de la gérer. », disponible à l'adresse suivante, p. 71.

[1036] Une licence de logiciel est un contrat portant sur les droits et les devoirs des utilisateurs par lequel le titulaire des droits d'auteur sur un programme informatique définit avec son cocontractant (exploitant et/ou utilisateur) les conditions dans lesquelles ce programme peut être utilisé, diffusé ou modifié.

[1037] *Op. cit.* « Annales des mines n°18 sur les enjeux numériques : Propriété et gouvernance du numérique », p.72.

[1038] Free Software Foundation, « Depuis plus de 20 ans, l'équipe Licences et conformité de la FSF est la principale ressource en matière de licences libres pour les développeurs de logiciels libres. », consultez le site internet à l'adresse suivante

[1039] Pour plus d'informations, consultez les sites internet suivants Choose a License – *choosealicence.com* et v. également Browse Licenses – *tldrlegal.com*

termes de « *logiciel libre* » et de « *code source ouvert* » sont régulièrement utilisés de façon interchangeable, bien qu'ils véhiculent des réalités qu'il semble important de distinguer en informatique. D'après Richard Stallman, il existe une distinction notable : « *les termes 'logiciel libre' et 'open source' recouvrent à peu près la même gamme de logiciels. Cependant, ils disent des choses profondément différentes sur ces logiciels, car ils se basent sur des valeurs différentes. Le mouvement du logiciel libre fait campagne pour la liberté des utilisateurs de l'informatique ; c'est un mouvement qui lutte pour la liberté et la justice. L'idéologie open source, par contre, met surtout l'accent sur les avantages pratiques et ne fait pas campagne pour des principes* »[1040]. Dans les faits, la majorité des logiciels open source sont des logiciels libres. Un logiciel open source est donc souvent un logiciel libre, c'est-à-dire ouvert, mais il n'est pas nécessairement accessible à titre gratuit contrairement aux logiciels libres qui le sont par conception. Un aspect crucial du logiciel libre est que les utilisateurs sont libres de coopérer. Il est absolument essentiel de permettre aux utilisateurs qui désirent s'entraider de partager leurs correctifs et améliorations avec d'autres. En attirant un nombre croissant de personnes autour d'un projet collectif et ouvert, le logiciel libre représente dès lors un formidable moyen de mutualisation de compétences et connaissances décentralisées sur le plan social. Par ailleurs, en 2009, le pseudo à l'origine de la création de Bitcoin[1041], Satoshi Nakamoto, explique sa vision du caractère open source de son innovation en ces termes : « *être open source signifie que n'importe qui peut examiner le code de manière indépendante. Si c'était un code fermé, personne ne pourrait vérifier la sécurité. Je pense qu'il est essentiel qu'un programme de cette nature soit open source* »[1042]. A ce titre, si les fondements d'Internet prônaient une transparence maximale, c'est-à-dire l'open source pour les programmes informatiques qui le composent, il s'avère aujourd'hui qu'il se compose plus de logiciels propriétaires (fermés) que libres (ouverts). Ainsi, Internet a progressivement perdu la bataille des logiciels libres face aux logiciels propriétaires, mais il est suggéré que les technologies blockchains permettent pour la première fois de venir nuancer cette tendance grâce aux logiciels libres et open source qui les composent. A cet égard, il est souligné que lutter contre la décentralisation informatique comme étudié en amont, revient indirectement à lutter contre un Internet reposant sur plus de logiciels libres (3.0). En effet, les blockchains publiques reposent et favorisent le caractère ouvert et accessible de ces logiciels et protocoles[1043]. A l'inverse, les blockchains hybrides et privées se fondent sur des logiciels initialement libres, mais progressivement propriétaires. Comme mentionné précédemment, il peut être trompeur de penser que la notion de logiciel libre est synonyme de gratuité, bien que certains des logiciels libres que nous utilisons demeurent gratuits comme VLC media player[1044] et Firefox[1045]. En réalité, la gratuité n'est qu'un effet secondaire

[1040] STALLMAN Richard, « En quoi l'open source perd de vue l'éthique du logiciel libre », in gnu.org, consulté en ligne le 27 octobre 2021.
[1041] V. Annexe 3 et Annexe 6, Focus 1.
[1042] NAKAMOTO Satoshi, « Re : Questions about Bitcoin », 2009, in *satoshi.nakamotoinstitute.org*, traduction libre de l'anglais, disponible à l'adresse suivante
[1043] En d'autres termes, les blockchains publiques et leur degré de décentralisation pure ne sont qu'une nouvelle forme d'outil au service d'une victoire des logiciels libres.
[1044] VLC Official site - Free multimedia solutions for all OS - VideoLAN. Disponible à l'adresse suivante
[1045] Pour plus d'informations consultez la liste des logiciels libres et gratuits à l'adresse suivante

de la licence sous laquelle les auteurs ont choisi de les distribuer lors de leur création. Finalement, l'importance du caractère ouvert des logiciels semble se conjuguer parfaitement au concept de la décentralisation informatique des technologies 3.0. Ensemble, ces deux concepts forment en quelque sorte un contre-pouvoir au service de l'ouverture et de la transparence du Web, une orientation qui mériterait d'être à minima conservée ou renforcée.

1.5.1.2 L'importance d'une éducation informatique et juridique conjointe

Si le standard informatique « *HyperText Transfer Protocol – http* » n'avait pas été ouvert et gratuit lors de sa création puis de son développement aux débuts du Web, Internet n'aurait probablement jamais vu le jour sous sa forme actuelle (son adoption n'aurait pas pu être exponentielle). Il est suggéré que ce constat se transpose et s'applique également aux standards de l'identité numérique décentralisée (VC, VP, DID). Cela amène cette recherche à l'importance de l'ouverture mentionnée de ces standards informatiques, mais également à l'éducation et aux connaissances nécessaires à leur diffusion et adoption. Par exemple, si la majorité du grand public ne connaît pas en détail le fonctionnement du protocole « *http* », la majorité semble connaître le principe plus intuitif du « *cadenas vert* » en haut à gauche du navigateur qui atteste d'une navigation en ligne relativement sécurisée. Pour l'identité numérique décentralisée, il serait envisageable de mettre en place un mécanisme standardisé et intuitif similaire pour faciliter la compréhension des utilisateurs des avantages et des conditions d'utilisation d'une IND, comme le principe du « *cyber score* » déjà évoqué[1046] ou encore des « *label de confiance de l'UE pour le portefeuille d'identité numérique* » étudiés précédemment[1047]. En théorie, pour prendre des décisions éclairées, les individus doivent être informés, et une abondance de connaissances est essentielle pour comprendre les avantages de l'utilisation d'une IND. Toutefois, comme l'a souligné dans les faits Jean-Jacques Quisquater lors d'une conférence en 2021[1048], il manque de main-d'œuvre dans ce secteur, car il y a un manque d'informaticiens connaissant suffisamment les technologies blockchains et la sécurité informatique spécifique au Web sémantique (3.0). Pour répondre à cet écueil, des ressources éducatives doivent être disponibles dans différentes langues et formats (vidéos, infographies, textes, supports, audio), et sur différentes plateformes (livres, articles, médias sociaux, télévision) adaptées au public cible (enfants, entreprises, juristes, représentants du gouvernement, personnes âgées)[1049]. Les fournisseurs d'identité décentralisée, les établissements d'enseignement, ou encore les pouvoirs publics

[1046] V. *supra*, I, Titre 1, 2.3.1.1
[1047] V. *supra*, II, Titre 1, 1.3.1.3
[1048] Propos suivants recueillis auprès de Jean-Jacques Quisquater lors du Forum International sur la Cybersécurité (FIC), le 09/09/2021, Table ronde : « Quels modèles alternatifs pour l'identité », « Il n'y a pas assez d'informaticiens qui connaissent suffisamment la technologie blockchain et la sécurité informatique ».
[1049] DOUTAUT Vincent (Dir.). « Informatique et culture scientifique du numérique », pp.1-433, 2021, « Il est […] crucial que les nouvelles générations, lycéens comme collégiens, s'emparent de ces questions et y soient initiés au travers de l'enseignement qui leur est dispensé. Au-delà des services apportés par le numérique, il est capital que la population en comprenne au mieux les contreparties juridiques, politiques et éthiques », disponible à l'adresse suivante

doivent s'assurer que ces ressources éducatives sont disponibles et surtout à jour. La future blockchain européenne (EBSI) fournit déjà des ressources éducatives en ligne à destination du public, tant à l'échelle nationale que communautaire comme cela a été mentionné en première partie[1050]. Pour atteindre le seuil critique de connaissances, il est nécessaire de convaincre la société civile des avantages de cette technologie : la confiance, la confidentialité, le stockage partiellement décentralisé et la vérifiabilité asynchrone des preuves et des attributs d'identité. Il est également important que les systèmes d'identité distribuée soient conçus pour que le maximum d'acteurs puisse participer à leur compréhension, ce qui représente déjà un défi pour les systèmes d'identité numérique traditionnels (2.0), mais d'autant plus pour ceux décentralisés. Pour garantir l'inclusivité, il faut également développer un accès sans obstacle aux personnes concernées par la fracture numérique, déjà désavantagées par l'utilisation de ces nouveaux outils numériques. Par exemple, les personnes qui ne possèdent pas la capacité juridique d'agir peuvent tout de même utiliser une IND en se reposant sur un tiers de confiance, nommé un gardien[1051], grâce à un système de délégation des clés cryptographiques en cours de développement et de standardisation par le W3C. Enfin, les difficultés du droit de l'informatique résident dans le manque d'information du grand public, tandis que les professionnels de l'informatique sont conscients des nombreuses possibilités ou impossibilités (mythes) informatiques. Face à ce constat, l'éducation concernant l'IND doit être accessible pour tout internaute et non pas seulement à des spécialistes de l'informatique qui pourraient en détourner certains mécanismes et usages à des fins idéologiques, politiques ou commerciales.

Chapitre 2 : Vers un droit cryptographique parfait et augmenté

2.1 La conformité règlementaire en Europe : fournisseurs d'identité et services de confiance

2.1.1 L'encadrement de l'identité numérique centralisée et décentralisée (eIDAS-1 & 2)

2.1.1.1 Le Règlement eIDAS

De nombreux spécialistes du droit estiment que l'identité numérique actuelle est déjà règlementée par les principes relatifs aux données personnelles, à la protection de la vie privée, ainsi qu'à l'identification et l'authentification électronique[1052]. Depuis le 23 juillet 2014, le Règlement eIDAS n° 910/2014/UE, ici désigné « eIDAS-1 », fournit une définition précise de l'identification électronique comme étant un « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique*

[1050] European Blockchain Service Infrastructure (EBSI). [Vidéo]. YouTube, ressources disponibles à l'adresse suivante
[1051] L'Art. 1242 du Code civil, dans sa version en vigueur depuis le 1er octobre 2016, dispose « On est responsable (…) des choses que l'on a sous sa garde ». Dans le cadre d'une identité numérique décentralisée, une personne qui ne possèderait pas les compétences techniques pour gérer elle-même ses clés cryptographiques, pourrait déléguer cette tâche à un tiers gestionnaire de confiance, qui agira en tant que « *gardien* » de ses clés. Ainsi, la délégation des clés cryptographiques à un tiers gestionnaire permet de faciliter l'accès à une identité numérique décentralisée pour les personnes qui ne possèdent pas les compétences informatiques nécessaires, tout en garantissant la sécurité et la confidentialité de leurs données.
[1052] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, *op. cit.* « L'identité numérique ; quelle définition pour quelle protection ? », 2020.

représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale »[1053]. L'authentification y est également définie comme « *un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* »[1054]. Les définitions précédentes ne cherchent pas à définir l'identité en tant que telle, mais plutôt à fournir une définition qui aborde les éléments immatériels de l'identité sans la décrire de manière précise. Ces définitions se concentrent sur l'identité des personnes physiques et morales, sans englober celles des machines (serveurs, ordinateurs)[1055]. La première version de ce Règlement a été négociée entre 2013 et 2014, publiée le 28 août 2014, et est entrée en vigueur le 17 septembre 2014. Une mise en œuvre partielle du Règlement a commencé en juillet 2016 pour les premiers services de confiance[1056], suivie d'une mise en œuvre complète en septembre 2018 pour les schémas et moyens d'identification électronique nationaux[1057]. L'objectif d'eIDAS-1 était de créer un environnement interopérable pour les différents systèmes numériques mis en place au sein des États membres aux fins de favoriser le développement d'un marché européen de confiance numérique. Il est fondé sur divers amendements de textes législatifs existants, telle que la directive du 20 mai 2015 sur la prévention de l'utilisation du système financier à des fins de blanchiment[1058] ainsi que sur la directive du 25 novembre 2015 sur les services de paiement dans le marché intérieur[1059]. Ce Règlement pose également plusieurs fondements. Il établit d'une part des standards de communication informatique communs et mutuels (des « *nœuds eIDAS* »)[1060] permettant d'évaluer la fiabilité des services numériques certifiés comme étant de confiance[1061], et institue d'autre part un pilier commun pour les services d'identification numérique à destination des citoyens européens. Au sens de ce Règlement, l'identification numérique est une identification vérifiée et authentifiée numériquement, dont le niveau de garantie est considéré élevé pour ses utilisateurs. En

[1053] Art. 3.1 du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, OJ L, 2014, consulté en le 15 septembre 2021.
[1054] *Ibid.*
[1055] V. *infra*, II, Titre 2, 1.6
[1056] En 2016, eIDAS distingue cinq services de confiance (disposant chacun de deux ou trois *niveaux de confiance* sous-jacents) : (i) la *signature électronique* pour les personnes physiques, (ii) les *cachets électroniques* pour les personnes morales, (iii) *l'horodatage électronique* et (iv) *l'authentification en ligne* des sites internet et enfin (v) les services d'envoi de *recommandés électroniques*.
[1057] Il s'agit d'une reconnaissance mutuelle des schémas d'identité numérique nationaux notifiés à la Commission européenne, via les *nœuds eIDAS* communs (serveurs centralisés) basés sur la technologie « SAML ». V. *infra*, I, Titre 1, 2.2.2.1.a
[1058] Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le Règlement (UE) n°648/2012 du Parlement européen et du Conseil et abrogeant la Directive 2005/60/CE du Parlement européen et du Conseil et la Directive 2006/70/CE de la Commission, 141, nº OJ L, 5 juin 2015, consulté en ligne le 24 novembre 2021.
[1059] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les Directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le Règlement (UE) n°1093/2010, et abrogeant la Directive 2007/64/CE, 337, nº OJ L, 23 décembre 2015, consulté en ligne le 24 novembre 2021.
[1060] En pratique, ces *nœuds* représentent des serveurs standardisés qui fonctionnent avec un protocole commun maintenu par le bras droit technique de la Commission européenne : « *Connecting Europe Facility* ». Le Règlement eIDAS-1 se matérialise ainsi par ce logiciel (« *eIDAS nodes* ») à destination de chaque État membre, leur permettant d'échanger et de synchroniser des données de confiance sur des serveurs privés (hébergés par des institutions publiques) et compatibles les uns avec les autres. V. « EIDAS-Node PRE-RELEASE version 2.6 », in *CEF Digital*, pour plus d'informations en ligne
[1061] *Ibid.*

principe, cette identification est unique, établie avec le consentement de l'individu[1062], tout en protégeant sa vie privée. Cette reconnaissance mutuelle entre les systèmes informatiques de confiance des Etats membres permet aux citoyens de l'UE d'accéder à des services publics transfrontaliers, y compris par l'intermédiaire de prestataires de services de confiance[1063]. Toutefois, la mise en œuvre de ces systèmes d'identification électroniques varie d'un État membre à un autre. Afin de pouvoir bénéficier de cette reconnaissance mutuelle, un moyen d'identification électronique doit avoir été délivré conformément à un schéma d'identification électronique notifié par l'État membre[1064] et figurant sur la liste publiée par la Commission européenne[1065]. Depuis le 29 septembre 2018, une reconnaissance réciproque des moyens d'identification numérique susvisés est devenue obligatoire[1066]. Le Règlement eIDAS introduit trois « *niveaux de garantie* » ou niveaux d'assurance[1067]. Ces degrés de confiance comprennent des critères précis permettant aux États membres de comparer leurs moyens d'identification électronique à un point de référence communautaire (faible, substantiel et élevé). Ces derniers sont accordés selon le respect de procédures, de spécifications et de normes techniques minimales à respecter[1068] :

- Un niveau de garantie faible[1069] : il s'agit de réduire marginalement le risque d'utilisation abusive ou d'altération de l'identité (usurpation d'identité).
- Un niveau de garantie substantiel[1070] : il s'agit de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité des utilisateurs.

[1062] V. *infra*, II, Titre 1, 2.2.3

[1063] L'utilisation des services de certification électronique, tels que la signature électronique, l'horodatage et les cachets électroniques (*v.* ci-avant), permet à un prestataire de services de confiance de garantir l'intégrité d'un document électronique à long terme. Ces prestataires peuvent être des fournisseurs technologiques publics ou privés, qui sont soumis à des normes et des contrôles établis par la norme européenne eIDAS. Pour exercer leur activité, ils doivent être certifiés et disposer de moyens techniques spécifiques, permettant ainsi de renforcer la confiance dans les transactions électroniques au sein de l'UE.

[1064] ANSSI, « Le règlement eIDAS », in *ssi.gouv*, disponible en ligne

[1065] Consultez la liste en temps réel des 27 prestataires de services de confiance français sur le site de la Commission européenne à l'adresse suivante

[1066] Acteurspublics.fr, « Modèles économiques de l'identité numérique », « La reconnaissance mutuelle des MIE est effective depuis le 29 septembre 2015 sur une base volontaire et deviendra obligatoire le 29 septembre 2018. », p.17, consulté en ligne le 24 novembre 2021.

[1067] Les niveaux d'assurance doivent caractériser le degré de confiance dans les moyens d'identification électronique, donnant ainsi l'assurance que la personne qui revendique une identité particulière est bien celle à laquelle cette identité est attribuée. V. Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du Règlement (UE) no 910/ 2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, consulté en ligne le 24/11/2021.

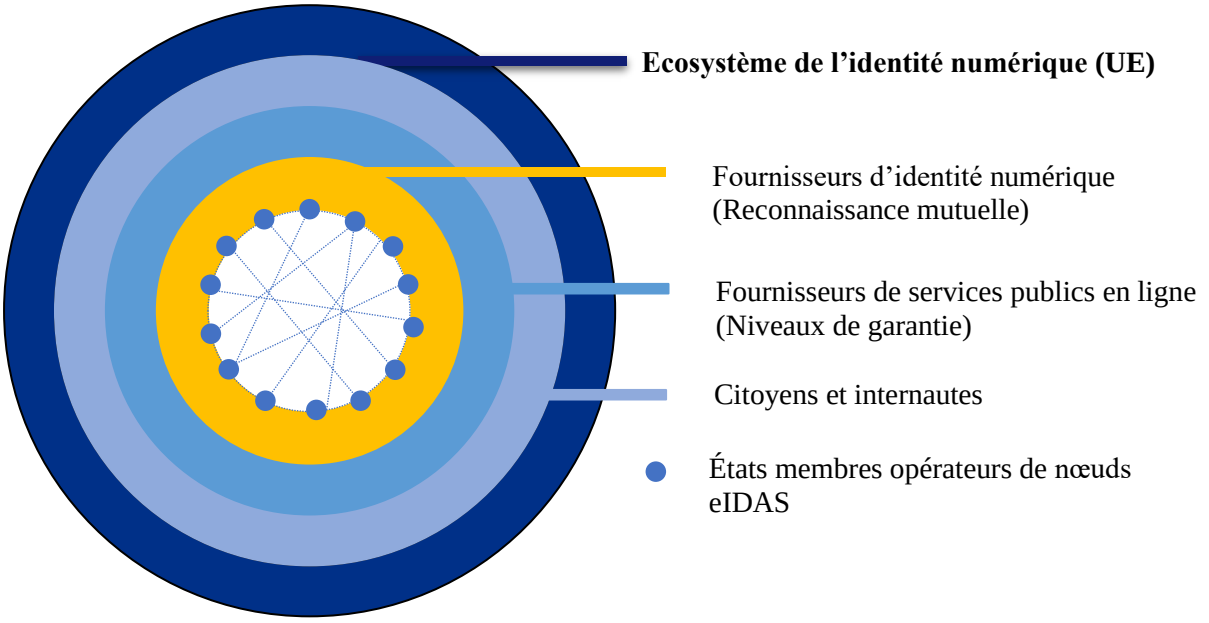
[1068] *Ibid*. Règlement d'exécution (UE) 2015/1502 de la Commission. V. Annexe pp.4-14 qui distingue chaque catégorie, caractéristiques et conception des moyens d'identification électronique à destination des personnes physiques ainsi que morales.

[1069] *Ibid*. Un moyen d'identification électronique de niveau de garantie faible nécessite : « 1. […] au moins un facteur d'authentification. 2. Le moyen d'identification électronique est conçu pour que l'émetteur prenne des mesures raisonnables afin de vérifier qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession. », p.9.

[1070] *Ibid*. Un moyen d'identification électronique de niveau de garantie substantiel nécessite : « 1. […] au moins deux facteurs d'authentification de différentes catégories. 2. Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession. ».

- Un niveau de garantie élevé[1071] : il s'agit d'empêcher toute utilisation abusive ou la moindre altération de l'identité d'une personne.

En amont de la proposition d'amendement eIDAS-2 étudiée plus loin, eIDAS-1 ne s'appliquait pas à l'identification entre personnes de droit privé, mais seulement entre États membres qui proposaient des moyens d'identification électronique à destination des citoyens (services publics)[1072]. Cependant, des exceptions ont été introduites au cas par cas en raison de la demande croissante des entreprises et du secteur privé pour étendre ces méthodes d'identification à la société civile. Par conséquent, de nombreux internautes utilisent désormais des méthodes d'identification et d'authentification numérique 2.0 fournies par des acteurs privés, comme évoqué dans cette étude.



Les trois niveaux de protection mentionnés impliquent que les solutions d'identité numérique étatiques relèvent par conception d'un niveau élevé, car elles sont dérivées de titres d'identité physiques et régaliens. En Allemagne, par exemple, la loi exige une vérification d'identité de niveau élevé incluant une vérification physique imposée par le BaFIn[1073] pour l'ouverture d'un compte bancaire en ligne. Fin

[1071] *Ibid*. Un moyen d'identification électronique de niveau de garantie élevé doit satisfaire au niveau substantiel en plus de devoir : « 1. […] protéger contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé. 2. Le moyen d'identification électronique est conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée ».

[1072] Pour plus de précisions, le Règlement eIDAS établit des exigences précises en matière de reconnaissance mutuelle des moyens d'identification électronique et de signatures électroniques pour les échanges entre les organismes du secteur public et leurs utilisateurs. Toutefois, il exclut les échanges internes des administrations qui n'ont pas d'impact direct sur les tiers, ainsi que les actes sous seing privé. Le Règlement s'applique spécifiquement aux échanges entre l'administration et le public, tels que les citoyens et les entreprises, mais ne s'applique pas aux systèmes informatiques jugés « *fermés* » comme les blockchains publiques (v. pages suivantes).

[1073] « La BaFin réagit face aux méthodes d'authentification adoptées par N26 », « En Allemagne, la loi exige que le contrôle des cartes d'identité soit un préalable à toute ouverture de compte. Cette vérification peut être effectuée dans un bureau de poste ou en agence. Il est même possible d'entamer la procédure à travers un appel vidéo », 2018, in *meilleurtauxbanques.com*, consulté en ligne le 24 novembre 2021.

2022, seuls trois pays sur 28 n'ont pas encore de schéma d'identification électronique d'un niveau de garantie élevé, dont la France (un niveau substantiel voire élevé étant accordé au schéma *FranceConnect* associé à l'identité numérique du Groupe la Poste)[1074]. En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) joue un rôle central et indispensable dans l'application opérationnelle de l'article 24-1 du Règlement eIDAS, qui concerne la délivrance de « *certificats qualifiés* »[1075] et la phase d'identification préalable à leur délivrance. Seules quatre méthodes sont actuellement reconnues pour réaliser cette phase de vérification en présentiel ou à distance[1076]. La reconnaissance de l'ANSSI est donc essentielle pour tout acteur de ce marché, car elle confère une présomption de fiabilité[1077] à l'identité numérique et aux moyens d'identification en ligne qui respectent son cahier des charges[1078]. En d'autres termes, l'ANSSI est en mesure de définir la conformité informatique des différentes méthodes d'identification et de leur attribuer un niveau de garantie substantiel ou élevé au visa de ce Règlement. Dans les années à venir, la proposition d'amendement du Règlement eIDAS permettra une reconnaissance légale complète des schémas d'identité numérique forts et dérivés de titres d'identité physiques au sein de l'UE. Il semble ainsi important de tenir compte de ce facteur dans le déploiement de futures solutions d'identité numérique décentralisée. L'article 11-1 du Règlement eIDAS édicte que différentes parties sont responsables des dommages causés par un manquement à leurs obligations[1079], notamment l'État membre, le fournisseur d'identification électronique ou la partie chargée de la procédure d'authentification. Cette coexistence des responsabilités à différents niveaux peut entraîner une certaine difficulté de compréhension et de lisibilité pour les fournisseurs d'identité et de services en ligne, ainsi que pour les citoyens et utilisateurs de services publics ou privés conformes à eIDAS-1. Une exception permet de déroger à cette responsabilité générale et communautaire lorsque les transactions d'identité numérique sont réalisées à l'échelle nationale ou lorsqu'un régime de partage de responsabilité est mis en place par les États membres[1080]. Les sanctions pour non-respect des règles applicables aux prestataires de services de confiance sont fixées par le droit interne de chaque État membre[1081], mais à

[1074] KIROVA Marina, « Overview of pre-notified and notified eID schemes under eIDAS », eID User Community, 13 septembre 2019. Disponible à l'adresse suivante

[1075] Les *certificats qualifiés de signature électronique* permettent d'attester de l'identité des personnes physiques/morales auxquelles ils ont été délivrés. Grâce à cette reconnaissance technique, l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. ANSSI, *op. cit.*, « Le Règlement eIDAS »

[1076] Art. 24-1-a-b-c-d. « Exigences applicables aux prestataires de services de confiance qualifiés eIDAS 910/2014 », consulté en ligne le 24 novembre 2021.

[1077] Art. L. 102 III du CPCE « Ce moyen d'identification électronique est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux prescriptions du cahier des charges établies par l'autorité nationale de sécurité des systèmes d'information, fixé par décret en Conseil d'État. », art. L102 du Code des postes et des communications électroniques, in *Légifrance*, consulté en ligne le 24 novembre 2021.

[1078] Agence nationale de la sécurité des systèmes d'information (ANSSI). « Référentiel d'exigences de sécurité pour les moyens d'identification électronique », version du 11 août 2022, in *ssi.gouv.fr*, disponible à l'adresse suivante

[1079] Responsabilité (Identification électronique) eIDAS 910/2014, in *marchepublic*.fr, consulté en ligne le 24 novembre 2021, « (i) L'Etat membre, (ii) la partie qui délivre le moyen d'identification électronique ou (iii) la partie qui gère la procédure d'authentification, est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent ».

[1080] *Op. cit.* EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, « L'identité numérique ; quelle définition pour quelle protection ? », *op. cit.*, « Le règlement ne s'applique pas pour les transactions nationales et les États membres peuvent prévoir un régime de partage de responsabilité différent. », p.132.

[1081] Art. 16. Sanctions (Services de confiance) eIDAS 910/2014. (2014), in *marche-public.fr*. Disponible à l'adresse suivante

ce jour, aucune disposition contraignante n'a été établie pour sanctionner la fourniture de services non qualifiés au sens d'eIDAS.

Le Règlement eIDAS, qui vise à créer une identité numérique européenne depuis plusieurs années[1082], est en cours de révision[1083], car il est confronté à certaines limites depuis sept ans[1084]. Seuls 60% de la population de l'UE, soit plus de 14 États membres sur 28, peuvent utiliser leurs systèmes d'identités numériques nationales de manière transfrontalière. Également, seuls 14 % des principaux prestataires de services publics dans l'ensemble des États membres autorisent l'authentification transfrontalière au moyen d'un système d'identité électronique. Si au moins 14 États membres disposent déjà d'une CNIe ou sont en train de la développer, une relative incertitude persiste quant à leur compatibilité et interopérabilité. De plus, la plupart des États membres ne disposent pas de nœuds eIDAS[1085] entièrement opérationnels, ce qui limite la possibilité d'authentification transfrontalière. En outre, l'infrastructure eIDAS-1 est centralisée et présente plusieurs vulnérabilités informatiques comme identifiées en 2019[1086], ce qui soulève des questions sur sa résilience à long terme. C'est pourquoi certains spécialistes proposent de recourir à la technologie blockchain pour améliorer l'interopérabilité et la sécurité de l'infrastructure eIDAS. Il nous faut donc étudier la conformité de la blockchain au Règlement eIDAS et déterminer comment elle pourrait répondre aux exigences juridiques et techniques de ce Règlement. Pour que la technologie blockchain soit au centre de cette infrastructure déjà utilisée, cela nécessiterait une refonte juridique comme l'expliquent dans un rapport en 2021 plusieurs experts mandatés par le ministère de l'Intérieur[1087]. En ce sens, les dispositions concernant les services de confiance du

[1082] *Op. cit.*, « Communication Shaping Europes Digital Future », consulté le 6 décembre 2021, p.6, traduction libre de l'anglais, « Une identité électronique publique (eID) universellement acceptée est nécessaire pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils souhaitent sans avoir à utiliser des plateformes non apparentées pour ce faire et à partager inutilement des données personnelles avec celles-ci ».

[1083] Il est fait référence au lancement d'un processus de consultation en juillet 2020 puis au projet de proposition de Règlement modificatif publié en juin 2021. La version finale du texte « *eIDAS-2* » devrait être adopté au premier trimestre 2023, v, partie suivante.

[1084] Comme l'explique Me Alain Bensoussan : « […] tous ces intervenants [du secteur de l'identité numérique] se déchargent aujourd'hui de toute responsabilité en se rangeant derrière une obligation de moyens et que le règlement eIDAS malgré les espoirs suscités n'a rien pu faire d'autre que de promouvoir l'interopérabilité des « moyens » (les Dispositifs) et sélectionner des standards existants (des « moyens » également) pour la reconnaissance mutuelle des Assertions [d'identité]. », *op. cit.* « L'identité numérique 5.0 ».

[1085] Ces *nœuds* représentent des serveurs standardisés qui fonctionnent avec un protocole commun maintenu par le bras droit technique de la Commission européenne : l'instance « *Connecting Europe Facility* ».

[1086] *Op. cit.* EYNARD Jessica, et al. « Il suffisait d'effectuer une connexion malveillante à un serveur eIDAS Node d'un État membre et fournir des faux certificats lors du processus d'authentification initial. », p.127.

[1087] *Op. cit.* COUTOR Sophie et al., « Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité'», 2020, disponible à l'adresse suivante : « […] le cadre eIDAS est trop limité pour intégrer la blockchain. Destiné à encadrer la fourniture d'un ensemble d'attributs déterminés (l'ensemble minimum d'attributs obligatoires qui identifient la personne, ou « identité pivot ») définis dans l'acte d'exécution 2015/1501, eIDAS ne permet : (i) ni la minimisation des données et la divulgation sélective d'attributs, (ii) ni l'utilisation de références anonymisées comme par exemple les assertions vérifiables certifiées (Verifiable Credentials) basées sur le modèle de données du W3C, (iii) ni la communication d'attributs connexes d'identification, autres que les « données pivot » (qui, renvoyant à l'identité juridique, servent à identifier la personne), (iv) ni des services en ligne offerts par le privé, (le Règlement traite uniquement de l'action des administrations publiques), (v) ni l'hébergement des données personnelles sur un dispositif personnel mobile de façon sécurisée [PIND]. », p.83.

Règlement eIDAS[1088] ne semblent pas permettre une interprétation favorable à la technologie blockchain. Tout d'abord, pour être accessible à un autre État membre, un service public en ligne utilisant une technologie blockchain devrait répondre aux exigences du Règlement et se voir attribuer l'un des trois niveaux de confiance mentionnés. Si l'approche de ce Règlement est technologiquement neutre, il permettrait à terme la qualification et la reconnaissance juridique des technologies 3.0, notamment au regard du niveau de garantie qu'elles peuvent légitimement inspirer en tant que service de confiance, ce que propose eIDAS-2[1089]. A titre d'illustration, eIDAS-1 ne régit pas à ce jour le cas où une entité privée (entreprise) délivre un DID/VC à destination d'une personne physique et pour une utilisation dans sa sphère privée. Il est constaté que certains cas d'usage sont concernés par eIDAS, notamment ceux impliquant le secteur public et les services à destination des citoyens comme le démontrent déjà les activités de l'EBSI en France et au sein de l'UE. A cet égard, il semble que les blockchains privées[1090] et publiques[1091] ne sont pas couvertes par celui-ci, car il ne s'applique pas aux services de confiance fournis exclusivement dans des systèmes fermés. Les blockchains privées, qui ne sont en principe accessibles qu'à un acteur, ainsi que les blockchains publiques, non conformes à ce texte dès lors qu'il ne s'agit pas de transactions liées à des identités numériques, ne semblent donc pas concernées. En revanche, les blockchains hybrides sont directement visées par le Règlement eIDAS. La blockchain européenne (EBSI) le démontre, car chacun des Etats membres opérateur et à terme ses entreprises, sera qualifié en tant que service de confiance, entraînant ainsi une reconnaissance juridique de ces technologies hybrides, qui comprendront également à terme certaines normes de l'identité numérique décentralisée étudiée précédemment (v. partie suivante).

Au sujet du degré de confiance accordé à l'identité numérique d'une personne en ligne, et au regard des trois niveaux de garantie précités, les mises en œuvre actuelles de l'identité décentralisée ont pour objectif d'être reconnues avec un niveau d'assurance spécifié comme substantiel ou élevé, lorsque couplé à d'autres mécanismes traditionnels de vérification en ligne d'une identité (devant être équivalents à une vérification d'identité en physique comme mentionné avec l'exemple Allemand). Une infrastructure sécurisée fonctionnant sur la technologie blockchain pourrait gagner en crédibilité en étant qualifiée de

[1088] Art. 16.a)b)c) et 17 « Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE », OJ L, 2014, consulté en ligne le 24 novembre 2021.
[1089] V. partie suivante.
[1090] En principe, les blockchains privées ne semblent pas soumises aux règles du Règlement eIDAS, car seuls les utilisateurs authentifiés et autorisés peuvent effectuer des transactions et accéder à ce registre électronique. Seuls les mineurs, qui sont des nœuds validateurs identifiés et enrôlés, ont la possibilité de mettre à jour le registre et de faire évoluer sa charte de gouvernance afférente ainsi que d'autres composantes juridiques comme les conditions générales d'utilisation, la charte de non-concurrence, les statuts ou encore le pacte d'associé dudit consortium. Il est souligné que la reconnaissance par les pairs de tels systèmes fermés ou tout mieux semi-ouverts semble difficilement conciliable avec le principe de reconnaissance mutuelle imposé par eIDAS-1 (contrairement aux blockchains ouvertes où il est plus simple de savoir si une conformité existe ou non car leurs systèmes sont accessibles). Pourtant, eIDAS-2 privilégie indirectement les systèmes fermées et hybrides comme cela est étudié ci-après.
[1091] En principe, les blockchains publiques sont également hors du champ d'application d'eIDAS-1, car tout internaute peut soumettre des transactions et accéder au registre. Parce que tout le monde peut déployer un nœud validateur et soumettre un nouveau bloc pouvant compléter le registre et s'impliquer dans la gouvernance de cette blockchain publique, alors les règles d'eIDAS initialement conçues pour des tiers et services de confiance, ne peuvent que difficilement trouver une application.

service de confiance au sens dudit Règlement. En 2022, les solutions d'identité décentralisée sont progressivement considérées comme des offres de services de qualité pour les entreprises et les citoyens, en raison de leurs nombreux avantages technologiques et juridiques. Depuis 2020, deux principales solutions ont été envisagées pour proposer une reconnaissance légale à l'identité décentralisée. Tout d'abord, plusieurs recommandations et scénarios décrits dans le rapport sur l'identité décentralisée et eIDAS, publié en avril 2020 par le Docteur en droit Ignacio Alamillo Domingo[1092], pouvaient être implémentés par le législateur européen. En 2023, ces recommandations sont présentes dans la proposition d'amendement eIDAS-2 exposée dans la partie suivante. Aussi, il était proposé de se référer à l'initiative du « *pont SSI eIDAS (eIDAS Bridge)* »[1093] pour ajouter des fondamentaux juridiques aux services de confiance fournissant des attestations vérifiables, en complément de l'utilisation de certificats électroniques et de sceaux électroniques conventionnels au sens d'eIDAS-1.

Si depuis 2016, le Règlement eIDAS a permis de transformer de manière holistique les secteurs publics et leurs services de confiance, l'encadrement de l'identité numérique au sein de l'espace économique européen demeure fragmenté et peu harmonisé. Deux constats sont possibles. Premièrement, la version actuelle du Règlement est source d'incertitudes face à l'expansion rapide des besoins d'identités numériques, tant en termes de respect de la vie privée, que de sécurité informatique et de facilité d'utilisation. En raison des difficultés rencontrées pour l'adoption et la mise en œuvre de la version initiale d'eIDAS, la Commission européenne a reconnu la nécessité de réévaluer sa politique en matière d'identité numérique européenne, et a proposé l'amendement eIDAS-2 explicité plus loin. En effet, l'UE positionne ses entreprises et ses institutions au cœur d'une nouvelle stratégie d'ouverture et d'interopérabilité des données entre ses États membres. Deuxièmement, de nouvelles opportunités technologiques émergent à court terme, telles que l'utilisation de systèmes blockchains qui permettront d'ouvrir de nouvelles possibilités économiques et sociales. En conséquence, l'UE tente d'établir un nouveau consensus juridique au travers d'eIDAS-2, en s'inspirant de la nouvelle interopérabilité informatique permise par l'identité numérique décentralisée, et pour éviter que les consommateurs ne continuent à utiliser les alternatives d'identité numérique 2.0 du secteur privé, qui ne sont parfois pas conformes à eIDAS ou au RGPD. L'objectif final d'une identité numérique décentralisée, déjà largement adoptée par certaines communautés de spécialistes informatiques, est de permettre la création d'attestations vérifiables (VC) dérivées des titres d'identité numériques nationaux et de leurs certificats nationaux (tels que la CNIe ou le permis de conduire compatible en ligne). Pourtant, il subsiste certains obstacles à l'avènement d'identités numériques libérées, de confiance et partiellement décentralisées.

[1092] Dr. ALAMILLO DOMINGO Ignacio, « SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market (B-1049 Brussels) », *op. cit.*, disponible à l'adresse suivante
[1093] *Ibid*. p.105.

2.1.1.1.a Le Règlement eIDAS révisé (eIDAS-2)

Le 03 juin 2021, Margrethe Vestager, vice-présidente exécutive de la Commission européenne pour « *Une Europe adaptée à l'ère numérique* »[1094] a annoncé la création d'une identité numérique européenne qui permettrait aux citoyens de se déplacer et de réaliser des transactions d'identité en ligne dans n'importe quel État membre sans frais supplémentaires et en toute confiance[1095]. Cette volonté politique a été suivie d'une proposition d'amendement pour modifier le Règlement eIDAS et établir un cadre européen pour l'identité numérique eIDAS-2[1096], fondé sur l'évolution des attentes des utilisateurs en matière de contrôle des données d'identité et sur la croissance du marché numérique[1097]. L'objectif de cet amendement est de fournir une identité numérique européenne interopérable et reconnue sur une base volontaire pour tous les citoyens et toutes les entreprises de la zone euro[1098]. Cette nouvelle stratégie politique et juridique européenne repose sur trois piliers principaux. Le premier pilier vise à améliorer l'efficacité des systèmes de reconnaissance mutuelle des schémas d'identification numérique nationaux (eIDAS-1). Le second pilier a pour but de permettre au secteur privé d'offrir des services basés sur une identification numérique améliorée (partiellement 3.0) et conforme à un niveau de garantie élevé. Enfin, le troisième pilier a pour objectif de fournir un « *portefeuille européen d'identité numérique* »[1099] de confiance et permettant le stockage et l'utilisation d'attributs uniques, interopérables et sous le seul contrôle de l'utilisateur. Ces fonctionnalités étant par conception rendue possible par l'identité numérique décentralisée (IND), précédemment étudiée, ce portefeuille d'identité numérique européen peut ainsi être considéré comme un portefeuille d'identité numérique décentralisée (PIND) au sens de la présente étude. Bien que le Règlement eIDAS-1 ait été efficace pour offrir un haut niveau de confiance et encourager l'adoption des services de confiance, il n'a pas réussi à répondre aux nouvelles demandes du marché en termes de nouvelles technologies et de digitalisation croissante de la vie quotidienne des citoyens européens[1100]. Le manque de solutions d'identité électronique notifiées dans tous les États

[1094] *Op. cit.* European Commission (EC), « A Europe fit for the digital age », 2019, disponible en ligne
[1095] European Commission (EC), « La Commission propose une identité numérique fiable et sécurisée », in *Press Corner*, consulté en ligne le 25 novembre 2021, traduction libre de l'anglais, « L'identité numérique européenne nous permettra d'agir dans n'importe quel État membre comme nous le ferions chez nous, sans frais supplémentaires et plus facilement, que ce soit pour louer un appartement ou pour ouvrir un compte bancaire en dehors de notre pays d'origine. Et ce, en toute sécurité et transparence. Ce sera donc à nous de décider quelles informations personnelles nous souhaitons partager, avec qui et à quelle fin [référence à l'IND]. Nous aurons ainsi une occasion unique d'approfondir ce que cela signifie de vivre en Europe et d'être européen. ».
[1096] *Op. cit.*, Proposition de Règlement du Parlement européen et du Conseil modifiant le Règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, disponible à l'adresse suivante
[1097] Il est fait référence au lancement d'un processus de consultation (en juillet 2020 puis au projet de proposition de Règlement modificatif publié en juin 2021, disponible à l'adresse suivante. La version finale du texte « *eIDAS-2* » devrait être publiée et adoptée au cours du premier semestre 2023.
[1098] *Ibid.* « Exposé des motifs, Contexte de la proposition, Résultats des évaluations ex post », 3. « La grande majorité des besoins en matière d'identité électronique et d'authentification à distance s'observent dans le secteur privé, en particulier chez les acteurs de domaines comme la banque, les télécommunications et l'exploitation de plateformes, qui sont tenus par la loi de vérifier l'identité de leurs clients. La valeur ajoutée du règlement eIDAS en ce qui concerne l'identité électronique est limitée en raison de sa faible couverture et de son faible degré d'adoption et d'utilisation. ».
[1099] *Ibid.* « 2. Base juridique, subsidiarité et proportionnalité. Droits fondamentaux ».
[1100] CE, « Shaping europe's digital future », 2020, consulté en ligne le 15 septembre 2021, p.6, traduction libre de l'anglais, « Une identité électronique publique (eID) universellement acceptée est nécessaire pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils souhaitent sans avoir à utiliser des plateformes non apparentées pour ce faire et à partager inutilement des données personnelles avec celles-ci ».

membres et leur manque de flexibilité pour prendre en charge de nouveaux cas d'usages numériques sont des raisons qui ont motivé la Commission européenne à proposer l'amendement eIDAS-2. De plus, les solutions d'identité numérique 2.0 qui ne sont pas couvertes par le champ d'application d'eIDAS-1[1101] sont source d'inquiétudes quant à la protection de la vie privée et des données des utilisateurs. Ainsi, l'eIDAS-2 est conforme aux priorités de la transformation numérique définies dans la stratégie « *Façonner l'avenir numérique de l'Europe* »[1102] et contribue à la réalisation des objectifs énoncés dans la « *Décennie numérique de l'Europe : objectifs numériques pour 2030* »[1103]. Cette proposition vise à soutenir la transformation de l'UE vers un marché numérique unique en proposant des mesures pour les autorités publiques, les citoyens et les fournisseurs de services en ligne. De plus, le Règlement est obligatoire et directement applicable dans tous les États membres de l'UE. Si eIDAS-1 a tout de même permis de répondre à certaines problématiques liées à la qualification juridique et à l'encadrement technique de l'identité numérique au sein des pays de l'UE, eIDAS-2 confère incontestablement une nouvelle reconnaissance juridique à l'identité numérique décentralisée[1104] ainsi qu'à la technologie blockchain[1105]. L'ambition concrète de cet amendement est de passer des 60% d'utilisation actuelle des identités numériques nationales encadrées par eIDAS-1, à 80%[1106] d'ici 2030 grâce au présent amendement. Cet objectif est d'autant plus ambitieux qu'il fait face à un temps d'application très court, d'environ trois ans (2023-2026), comme le résume prospectivement la frise chronologique suivante :

[1101] Il est fait référence aux solutions proposées par les GAFAM/BHATX ou encore par certaines institutions financières. Leurs solutions de « *Single sign-on - SSO* » ou « *Authentification toute en un* » permettent à des utilisateurs de naviguer entre plusieurs services en ligne sans s'inscrire à nouveau sur chacun d'entre-deux, mais simplement en s'authentifiant rapidement grâce à une solution d'identité numérique fédérée (cette solution très plébiscitée des utilisateurs repose toutefois sur une collecte massive et opaque de leurs données personnelles). En effet, ces solutions *SSO* sont sujettes à de nouvelles attaques informatiques qui peuvent facilement tromper leurs utilisateurs, *v. supra*, I, Titre 1, 2.2.1.1

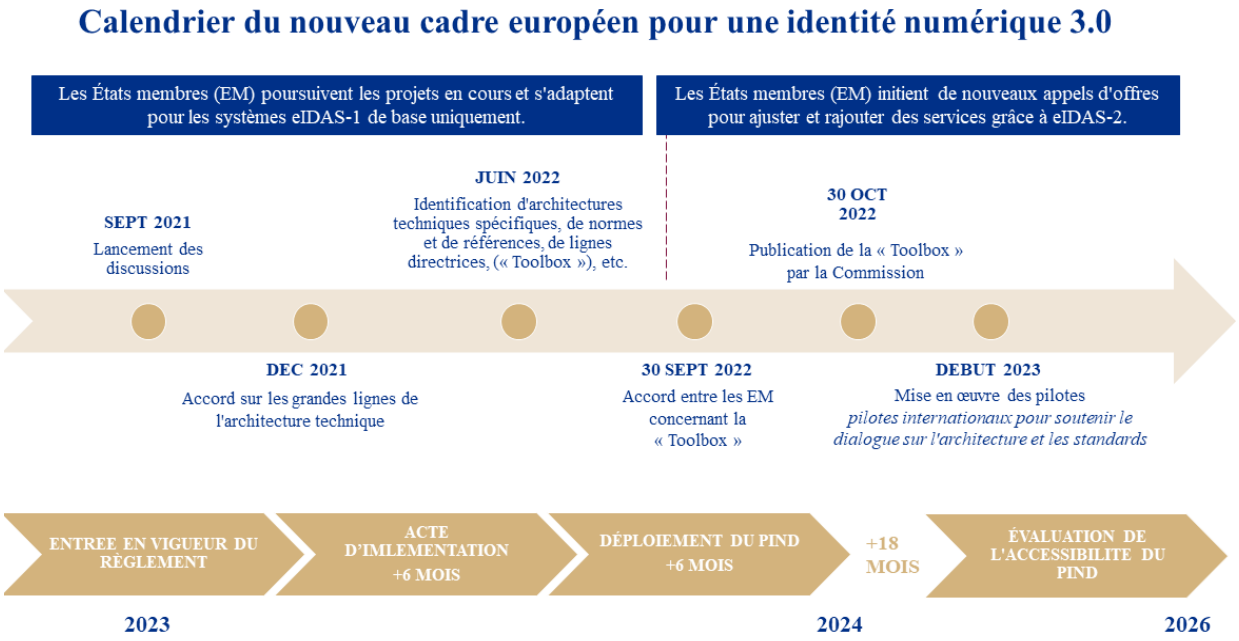
[1102] Commission européenne (CE), « Façonner l'avenir numérique de l'Europe. Bâtir l'avenir numérique de l'Europe », disponible à l'adresse suivante

[1103] CE, « Décennie numérique de l'Europe : objectifs numériques pour 2030 », *op. cit.*, disponible à l'adresse suivante

[1104] L'amendement désigne les attestations vérifiables (VC) comme « une attestation sous forme électronique qui permet l'authentification d'attributs » ou (« electronic attestation of attributes » en anglais). De plus, une attestation électronique qualifiée d'attributs est au sens de ce Règlement nécessaire « délivrée par un prestataire de services de confiance qualifié », *op. cit.*, (45). Pour des raisons d'intelligibilité nous conservons l'utilisation du terme d'attestation vérifiable, qui sera probablement le terme le plus utilisé par l'écosystème que nous avons décrit.

[1105] L'amendement ne nomme ni ne cite une technologie blockchain en tant que telle, mais il préfère dans un souci de neutralité technologique l'utilisation du terme « registre électronique » ou « Electronic Ledger » en anglais. En ce sens, eIDAS-2 définit dans son article premier un *registre électronique* comme « un enregistrement électronique inviolable de données, assurant l'authenticité et l'intégrité des données qu'il contient, l'exactitude de la date et de l'heure de ces données ainsi que de leur classement chronologique ». Si cette ambivalence peut fait référence à tous types de registres électroniques qu'ils soient *centralisés*, *décentralisés* ou bien *hybrides*, nous constatons que la volonté du législateur européen est de permettre une qualification puis une reconnaissance juridique aux technologies blockchains (privées et hybrides) en les incluant dans cette large définition. En mars 2023, cette section 11 dédiée aux registres électroniques a été enlevée du texte, en réaction, une lettre ouverte de l'écosystème a été signée par plus de 200 spécialistes des technologies blockchains. INATBA, "Open Letter for the preservation of the Electronic Ledger's provisions in eIDAS 2", in *inatba.org*, disponible à l'adresse suivante

[1106] CE, « Commission proposes a trusted and secure Digital Identity for all Europeans », « […] d'ici à 2030, tous les services publics clés devraient être disponibles en ligne […] et 80 % des citoyens devraient utiliser une solution d'identification électronique », in *Press Corner*, consulté en ligne le 3 juin 2021.



Face à l'adoption de cette proposition d'amendement du Règlement eIDAS, prévue d'ici septembre 2023, il est possible de résumer ses points cardinaux, notamment en relation avec le Web 3.0. Tout d'abord, trois nouvelles catégories de services de confiance qualifiés sont ajoutées aux cinq services d'ores et déjà consacrés par eIDAS-1[1107], à savoir, les services d'archivage électronique[1108], la gestion des dispositifs de création de signatures et de cachets électroniques à distance[1109] et les registres électroniques (blockchain y compris)[1110]. Par conséquent et à compter du premier semestre 2023, date à laquelle il faut ajouter 18 à 24 mois pour l'implémentation de certains standards technologiques par les Etats membres, eIDAS-2 encadrera environ dix services de confiance et permettra l'utilisation de multiples technologies 2.0 et 3.0. Une présomption de fiabilité et d'authenticité serait ainsi conférée aux

[1107] V. partie précédente : (i) Signature pour les personnes physiques, (ii) cachets électroniques pour les personnes morales, (iii) l'horodatage électronique et (iv) l'authentification en ligne de sites internet et enfin (v) les services d'envoi recommandé électronique. Finalement, eIDAS-1 & 2 encadrent désormais juridiquement 10 cas d'usages électroniques largement adoptés ou en cours d'adoption sur internet comme le mentionne la proposition eIDAS-2 dans son premier article : « un cadre juridique régissant les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, les services d'envoi recommandé électronique, les services de certificats pour l'authentification de site internet, l'archivage électronique et l'attestation électronique d'attributs, la gestion des dispositifs de création de signature électronique et de cachet électronique à distance, et les registres électroniques ».

[1108] Un *service d'archivage électronique* est considéré comme « un service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin de garantir leur intégrité, l'exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation », v. définitions et la Section 10, art.45g.

[1109] Art 3. 14. « 'certificat de signature électronique', une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne » et l'art. 3. 29 : « 'certificat de cachet électronique', une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne ».

[1110] Traduit librement du terme anglais « *Electronic Ledgers* », Section 11 & Considérant (34) : « Ce service de confiance est nécessaire pour éviter la fragmentation du marché intérieur, en définissant un cadre paneuropéen unique permettant la reconnaissance transfrontalière des services de confiance qui soutiennent le fonctionnement des registres électroniques qualifiés [blockchains fermées]. L'intégrité des données, quant à elle, est très importante pour la mise en commun de données provenant de sources décentralisées, pour les solutions d'identité autonomes [IND], pour l'attribution de la propriété des actifs numériques, pour l'enregistrement des processus d'entreprise à des fins de vérification du respect des critères de durabilité et pour différents cas d'utilisation sur les marchés des capitaux. ».

registres électroniques dits qualifiés : « *un registre électronique qualifié bénéficie de la présomption de l'unicité et de l'authenticité des données qu'il contient, de l'exactitude de leur date et de leur heure, et de leur ordre chronologique séquentiel au sein du grand livre* »[1111]. Les conditions pour qu'un registre électronique soit considéré comme qualifié sont les suivantes : (i) il doit émaner d'un ou plusieurs services de confiance[1112], (ii) il doit garantir l'unicité, (iii) l'authenticité des données et des transactions enregistrées ainsi que (iv) l'ordre chronologique et (v) l'exactitude de la date et de l'heure correcte des informations. Enfin il doit enregistrer les données de manière que toute modification ultérieure des données soit immédiatement détectable. Concernant les moyens d'identification et d'authentification en ligne, de nouveaux « *portefeuilles européens d'identité numérique* » (« *European Digital Identity Wallets - EDIW* »)[1113] seront développés et proposés par les États membres d'ici début 2024 comme le suggère la frise précédente. Ces portefeuilles d'identité numérique décentralisée (PIND, déjà évoqué), cette fois européens, seront mis à la disposition des citoyens, des résidents et des entreprises (personnes physiques et morales) de l'UE souhaitant s'identifier ou fournir la confirmation de certaines informations personnelles[1114]. Ils pourront être utilisés en ligne et hors connexion[1115] pour accéder à des services numériques publics et privés[1116], y compris de façon transfrontalière (interopérable) dans tous les États membres de l'UE. Ces mallettes d'identité devront supporter de larges ensembles d'attributs électroniques (VC qualifiés ou non qualifiés), ce qui n'était pas le cas de la version initiale du Règlement eIDAS[1117], tout en permettant une « *divulgation sélective* » des attributs d'identité[1118] ainsi qu'une fonctionnalité de « *signatures électroniques qualifiées* »[1119], par exemple pour faciliter la participation politique des citoyens européens (vote en ligne, référendum par exemple)[1120]. Chaque mallette d'identité

[1111] Section 11, art. 45 nonies, disponible en ligne
[1112] Art. 3. 16. Et Annexe V et VI du Règlement eIDAS-2 (Exigences applicables aux attestations électroniques qualifiées d'attributs & liste minimale d'attributs).
[1113] Art. 6 bis. La traduction par « mallette d'identité numérique » est également possible, v. également « Proposition d'une taxonomie francophone pour l'identité décentralisée ». 2021. ⟨hal-03398096⟩.
[1114] Ces mallettes d'identité ou PIND devront « permettre aux utilisateurs de stocker des données d'identité, des justificatifs et des attributs pour les fournir sur demande aux parties qui se fient à eux et les utiliser pour l'authentification en ligne et hors ligne et pour créer des signatures et des sceaux électroniques », (i) (42).
[1115] Chaque PIND doit permettre une communication directe et pair à pair (c'est-à-dire sans tiers) entre le porteur du PIND (utilisateur) et un vérificateur (service en ligne). Cette communication peut être effectuée en ligne (via une connexion à internet) mais aussi et surtout hors ligne (via QR code, Bluetooth, SMS, etc.).
[1116] Contrairement à sa première version plutôt restrictive pour les services privés, cet amendement du Règlement permet ainsi aux services privés de fournir des identités numériques (avec une authentification forte) aux personnes, au sens d'une liste telle que définie : « Les parties prenantes privées fournissant des services dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, de l'infrastructure numérique, de l'éducation ou des télécommunications devraient accepter l'utilisation des portefeuilles d'identité numérique européens pour la fourniture de services où une authentification forte de l'utilisateur pour l'identification en ligne est requise par le droit national ou de l'Union ou par obligation contractuelle. », (28) disponible en ligne
[1117] *Op. cit.* v. Explanatory memorandum 1. : « […] le cadre eIDAS actuel ne couvre pas la fourniture d'attributs électroniques » ; « le règlement eIDAS ne permet pas aux utilisateurs de limiter le partage des données d'identité à ce qui est strictement nécessaire à la fourniture d'un service ».
[1118] Results of ex-post evaluations and impact assessments, traduction libre de l'anglais, « […] permettant aux utilisateurs de choisir quand et avec quel fournisseur de services privé partager divers attributs, en fonction du cas d'utilisation et de la sécurité requise pour la transaction concernée. » ; (29) « L'EDIW devrait permettre techniquement la divulgation sélective d'attributs aux parties concernées. ».
[1119] Art. 6 bis. 3.(b), Proposition de Règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, disponible à l'adresse suivante
[1120] Exposé des motifs, 1. « Le portefeuille permettra en outre de disposer de signatures électroniques qualifiées susceptibles de faciliter la participation à la vie politique ». *v. infra*, I, Titre 2, 2.2.7

numérique nationale sera également gratuite[1121] et d'utilisation facultative pour les citoyens européens. Par ailleurs, il est constaté que tous les fournisseurs « *d'attributs électroniques qualifiés* » (DID, VC) doivent fournir ces services via une entité juridique distincte de celle qu'ils utilisent pour leur PIND afin d'écarter les risques d'agrégation ou de vol desdits attributs d'identité.

Les États membres doivent fournir[1122] puis notifier[1123] au moins un PIND dont le niveau de sécurité et de garantie est élevé[1124], et cela au plus tard douze mois après l'entrée en vigueur d'eIDAS-2, c'est-à-dire d'ici septembre 2024[1125]. De cette façon, les fournisseurs d'identités fourniront des attestations vérifiables compatibles entre chaque PIND. Grâce aux VC, une nouvelle possibilité s'ouvre ainsi pour les pays européens afin d'accepter de nouveaux types de justificatifs informatiquement et légalement transfrontaliers, interopérables et sécurisés (y compris avec des pays non-membres de l'UE, ce qui permet de tendre vers une première forme d'identité numérique universelle[1126]). En effet, eIDAS-2 évoque cette possible reconnaissance internationale d'attestations vérifiables européennes[1127], une avancée significative pour l'identité numérique qui est ainsi moins dépendante de la conclusion d'innombrables accords juridiques afin de reconnaître multilatéralement des solutions d'identité numérique. Toutefois, cette proposition explique qu'un « *processus de coopération étroite et structurée entre la Commission, les États membres et le secteur privé est nécessaire.* »[1128]. Pour cela, une « *boîte à outils* » (« Toolbox ») propose la mise en œuvre d'une architecture informatique qui repose sur des standards et des pratiques communes que les États membres devront respecter pour leurs PIND. A cet égard, ils devront (i) permettre la fourniture et l'échange d'attributs d'identité (VC, DID), (ii) assurer la fonctionnalité et la sécurité des PIND ou (iii) ériger une gouvernance ou étudier leurs dépendances à l'égard des fournisseurs d'attributs d'identité. La Commission européenne instaure également des « *Codes de conduite* »[1129] pour faciliter la mise à disposition et l'utilisation des PIND. Ces codes de conduite seront élaborés dans un délai de douze mois à compter de l'adoption d'eIDAS-2 puis mis en

[1121] Art. 6a.
[1122] Introduction d'une obligation pour les États membres de délivrer un portefeuille d'identité numérique 12 mois au plus tard après l'entrée en vigueur de l'amendement (article 6 bis 1.), v. ci-après.
[1123] Les États membres devront notifier leur EDIW/PIND selon l'art. 6a2, *op. cit.* Proposition de Règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique. Disponible à l'adresse suivante
[1124] Art. 6 bis. 4.(c).
[1125] « Afin de garantir à toutes les personnes physiques et morales dans l'Union un accès sécurisé, fiable et continu à des services publics et privés transfrontaliers, chaque État membre délivre un portefeuille européen d'identité numérique dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement. ».
[1126] V. *supra*, I, Titre, 1.1.3.2
[1127] *Ibid.* Fiche financière législative, 1.4.4. Indicateurs de performance. « Accroître la reconnaissance et l'acceptation transfrontalières des schémas d'identification électronique, l'ambition étant de parvenir à une acceptation universelle ».
[1128] Art. 36.
[1129] (28) « Des codes de conduite d'autorégulation au niveau de l'Union ("codes de conduite") devraient être élaborés afin de contribuer à une large disponibilité et à une grande facilité d'utilisation des moyens d'identification électronique, y compris les portefeuilles d'identité numérique européens, dans le cadre du présent Règlement. Les codes de conduite devraient faciliter une large acceptation des moyens d'identification électronique, y compris les EDIWs. Ils devraient être élaborés dans les douze mois suivants l'adoption du présent Règlement. ».

œuvre dans un délai de dix-huit mois[1130]. Ces codes de conduite devront également intégrer des composantes éthiques, que cette recherche dédie dans une partie[1131]. De plus, la responsabilité de ces mallettes d'identités européennes (PIND) incombe aux États membres[1132] et leur labélisation ne sera pas soumise à des processus « *d'examen par les pairs* »[1133] comme l'exigeait pourtant eIDAS-1. Un État membre doit fournir une interface commune aux utilisateurs et citoyens afin de permettre une interaction facilitée entre des services en ligne et cette interface. À cette fin, un « *label de confiance* »[1134] européen pour le portefeuille européen d'identité numérique (« *Trust Mark* ») est instauré. Une liste des PIND certifiés est également réalisée et maintenue à jour par la Commission européenne[1135]. Il convient de souligner qu'un PIND a pour effet de s'imposer aux grandes plateformes en ligne ou « *Gatekeppers* »[1136] en vertu d'eIDAS-2. Certains fournisseurs de services privés, dont les activités sont essentielles pour la société civile, seront ainsi dans l'obligation de proposer et d'accepter ces PIND étatiques ou à défaut de mettre en place une authentification élevée de leurs utilisateurs[1137]. A cet égard, il est probable que certaines grandes entreprises technologiques décident de développer leurs propres PIND dont le niveau de garantie serait élevé, non seulement parce que ces applications décentralisées peuvent supporter de multiples cas d'usage ce qui ouvre un nouveau champ des possibles sur le plan commercial, mais éventuellement aussi pour échapper à cette tentative de l'UE d'imposer un PIND européen souverain.

[1130] Section III, (16), 4. « Ces codes de conduite veillent à ce que les moyens d'identification électronique, y compris les portefeuilles européens d'identité numérique […] soient acceptés en particulier par les prestataires de services qui recourent à des services d'identification électronique tiers pour l'authentification de l'utilisateur. La Commission facilite l'élaboration de ces codes de conduite en étroite coopération avec toutes les parties intéressées et encourage les prestataires de services à achever l'élaboration des codes de conduite dans un délai de douze mois à compter de l'adoption du présent règlement et à les mettre effectivement en œuvre dans un délai de dix-huit mois à compter de l'adoption du présent règlement. ».

[1131] V. *infra* II, Titre 2, 1.1

[1132] Les PIND doivent être « *délivrés* » ou « *approuvés* » par les autres États membres, ce qui a des implications en termes de responsabilité : un État peut ainsi être tenu responsable en cas de violation de données à caractère personnel issue de son *portefeuille numérique national*, art.10a, disponible à l'adresse suivante

[1133] Possibilité de s'appuyer sur la certification pour garantir la conformité au Règlement en remplacement du processus d'examen par les pairs : les PIND seront évalués par référence à des « normes et références techniques communes » et seront donc reconnus de façon égale au sein de l'Union européenne, conformément à l'art. 42 du RGPD

[1134] « 'label de confiance de l'UE pour le portefeuille d'identité numérique', une indication formulée d'une manière simple, claire et reconnaissable selon laquelle un portefeuille d'identité numérique a été délivré conformément au présent règlement », art.1. 3.(i) 49.

[1135] Art. 6 quinquies, « la Commission établit, publie et met à jour une liste des portefeuilles européens d'identité numérique certifiés. », disponible à l'adresse suivante

[1136] « Lorsque de très grandes plateformes en ligne exigent des utilisateurs qu'ils s'authentifient pour accéder à des services en ligne, ces plateformes devraient être tenues d'accepter l'utilisation de portefeuilles européens d'identité numérique à la demande volontaire de l'utilisateur. Les utilisateurs ne devraient pas être tenus d'utiliser le portefeuille pour accéder à des services privés, mais, lorsque l'utilisateur le souhaite, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données. », considérant (28).

[1137] Les grandes plateformes comme Amazon, Google ou Facebook seront concrètement tenues d'accepter l'utilisation des portefeuilles d'identité numérique de l'UE à la demande de l'utilisateur (par exemple pour prouver son âge). *Ibid.* « Les parties utilisatrices privées qui fournissent des services dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications devraient accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit national ou de l'Union ou une obligation contractuelle exigent une authentification forte des utilisateurs à des fins d'identification en ligne ».

En matière de protection des données personnelles, l'utilisation des données (la consultation, le partage ou la révocation) doit être possible directement par l'utilisateur[1138]. Cette sécurité et sélectivité des données que l'utilisateur choisit de partager renforcerait d'après cette étude certains droits fondamentaux[1139]. L'émetteur d'un PIND doit pouvoir assurer une « *identification unique* » des utilisateurs. Par conception, l'émetteur d'un PIND ne doit pas pouvoir combiner les données d'identification avec des données personnelles provenant d'autres services (excepté si l'utilisateur en fait la demande)[1140]. Également, une séparation physique des briques technologiques et logicielles (2.0 & 3.0) doit être appliquée face à des données d'autres natures[1141]. A ce titre, les fournisseurs de périphériques matériels comme les opérateurs mobiles sont dans l'obligation de proposer cette séparation via un « *composant informatique sécurisé* » (« *secure element* »). Pour qu'une telle fonctionnalité soit possible sur l'appareil de chaque citoyen et compatible avec son PIND souverain, cela implique que tous les fabricants de périphériques électroniques (fabricants de téléphones et d'ordinateurs, etc.)[1142] implémentent ces composants dans leurs produits dès leur conception. Un tel processus semble indispensable, bien que complexe et coûteux ce qui pourrait complexifier la mise en œuvre de cette règle qui ne serait ainsi que partiellement respectée à court terme. A ce jour, les PIND ne proposent que des clés cryptographiques connectées à des serveurs, et ne tirent pas encore parti des avantages de sécurité issus d'un élément matériel directement intégré dans l'appareil des citoyens européens (comme la CNI française qui intègre plusieurs puces sécurisées comme déjà mentionné). A

[1138] Considérant (29) : « Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel. ».

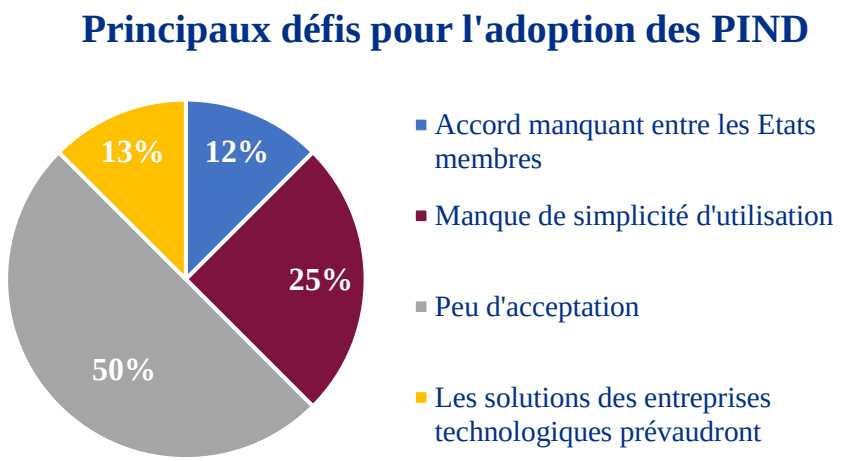
[1139] V. Résultats des évaluations ex post, Droits fondamentaux, « En utilisant le portefeuille européen d'identité numérique, l'utilisateur pourra exercer un contrôle sur la quantité de données fournies aux parties utilisatrices et être informé des attributs qui seront exigés pour la fourniture d'un service particulier. », *v. infra*, II, Titre 1, 2.2

[1140] L'émetteur de portefeuilles ne peut pas collecter les données d'utilisation des portefeuilles sauf si elles sont nécessaires au fonctionnement du portefeuille selon l'art. 6bis, 7 : « L'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés ».

[1141] En d'autres termes, une combinaison restreinte des données à caractère personnel des utilisateurs doit être assurée par son fournisseur : le fournisseur d'un PIND ne pourra pas combiner des données d'identification avec des données personnelles provenant d'autres services (excepté si l'utilisateur en fait la demande).

[1142] L'amendement eIDAS-2 nécessite un élément périphérique sécurisé (« *Hardware element* ») afin de stocker les clés cryptographiques de chaque utilisateur. Cet élément sécurisé et intégré peut l'être sur une carte SIM ou encore via d'autres méthodes telles que l'utilisation du NFC, Bluetooth, etc.

cet égard, un constat similaire s'applique à l'authentification biométrique qui est également privilégiée par eIDAS-2[1143].



Avec l'adoption d'eIDAS-2, un service en ligne (public ou privé[1144]) qui recourt à la technologie blockchain pourrait être accessible et légalement reconnu comme tiers de confiance au sein de l'UE. Une solution d'identité décentralisée déployée par un État membre se verra également attribuer l'un des trois niveaux de confiance initialement institués par eIDAS[1145]. Concernant la reconnaissance légale accordée aux « *attestations électroniques qualifiées* », eIDAS-2 les définit comme une caractéristique c'est-à-dire comme la qualité d'une personne physique ou morale sous une forme électronique. La similarité entre cette définition et celle des « *vérifiables credentials - VC* », étudiés précédemment et spécifique au modèle de l'identité décentralisée selon le W3C, est frappante et sans aucun doute liée. Une attestation vérifiable signée et qualifiée au sens de ce Règlement modifié garantit une opposabilité juridique à son titulaire grâce à la traçabilité et à l'intégrité de sa source, c'est-à-dire au service et tiers de confiance auquel il est lié. Toutefois, tous les attributs gérés par un PIND ne seront pas qualifiés au sens d'eIDAS-2, comme pour les VC issus d'identités numériques auto-souveraines (INAS). Ainsi, certains environnements numériques seront plus propices à l'utilisation d'attributs non qualifiés, notamment les métavers[1146] étudiés au titre deuxième de la deuxième partie, et plus précisément tout segment particulièrement décentralisé du Web 3.0. Cette vérification de l'authenticité d'attributs auprès de leurs sources et tiers de confiance semble primordiale pour les cas d'usage liés à l'identité civile et primaire des citoyens. En effet, cette identité numérique européenne sera donc plutôt hybride, c'est-à-dire qu'elle comportera à la fois des composantes informatiquement centralisées et d'autres distribuées (soit informatiquement semi-décentralisées). Le recours à ces services de confiance qualifiés pour

[1143] Considérant (11), « Le recours à l'authentification biométrique est l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec d'autres éléments d'authentification. ».
[1144] Et non plus simplement public comme dans la version actuellement en vigueur du Règlement eIDAS-1, qui limite fortement les services d'identification électronique aux services publics.
[1145] Les mises en œuvre actuelles de l'identité décentralisée ont pour objectif d'être reconnues avec un niveau d'assurance spécifié comme à minima *substantiel* (à court terme) et si possible *élevé* (à moyen et long terme).
[1146] V. *infra*, II, Titre 2, 1.4

délivrer des VC par extension également qualifiés au sens d'un État membre permettra en définitive de les reconnaître mutuellement dans tout autre État membre[1147]. Par exemple dans une procédure judiciaire ces attributs qualifiés 3.0 ne pourront pas se voir refuser l'effet et la recevabilité juridique en tant que moyen de preuve numérique au seul motif qu'ils sont sous un format électronique. En effet, eIDAS-2 reconnaît et présume la fiabilité cryptographique des sources et des interactions de chacun de ces attributs notamment grâce à l'utilisation de blockchains hybrides ou privées reconnues en tant que services de confiance. Il est donc prévu qu'une attestation vérifiable qualifiée produise les mêmes effets juridiques que des attestations physiques légalement délivrées sur papier[1148]. Pour autant, les règles relatives à l'émission, au format, au fonctionnement et à l'interopérabilité de ces attestations ne sont pas encore précisées[1149]. Elles devront faire l'objet d'une définition par les États membres dans le cadre du programme de la boîte à outils qui a débuté en septembre 2021.

La nouvelle section 11 dédiée au « *registre électronique qualifié* » (blockchains) consacre la présomption d'unicité, d'authenticité et d'immuabilité des données qui y sont contenues. Courant 2023, débuteront les définitions des actes d'exécution et des actes délégués d'eIDAS-2. Ces actes préciseront les cadres règlementaires et techniques au regard des spécificités sectorielles de certains marchés et services (santé, transports, permis de conduire, contrôle des frontières, moyens de paiement et transactions financières, diplômes, certifications ou attestations liées à l'éducation ou à la formation des personnes). Cette « *présomption de fiabilité* » a trait à la traçabilité des opérations concernant par exemple une donnée d'identité, leur horodatage et leur intégrité. Les entreprises opérant une blockchain privée ou hybride pourront donc demander que celle-ci soit certifiée, c'est-à-dire qualifiée en tant que service de confiance[1150]. Cette couverture est positive pour l'ensemble de la communauté du Web 3.0 et tout particulièrement de l'IND qui pourra se fonder sur de multiples blockchains privées ou hybrides dont les données et transactions seront officiellement reconnues comme de confiance tant au niveau national qu'européen, peut-être international à long terme. Néanmoins, il convient dans un premier temps de s'assurer que la version antérieure des nœuds eIDAS-1 soit compatible avec la version qui sera mise à jour par eIDAS-2 et qui permettra l'implémentation de la technologie blockchain - comme l'EBSI, évoqué au titre premier de cette étude - et du concept d'une identité numérique européenne partiellement décentralisée. Dans un second temps, l'obligation de fournir un PIND est intimement liée aux schémas d'identification électronique dont le niveau de garantie notifié doit être élevé[1151], ce qui

[1147] Art. 45 bis. Proposition de Règlement du Parlement européen et du Conseil modifiant le Règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, disponible à l'adresse suivante
[1148] Considérant (27) : « il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a un effet juridique équivalent à celui des attestations délivrées légalement sur papier. Toutefois, ces exigences devraient s'appliquer sans préjudice du droit de l'Union ou du droit national définissant des exigences sectorielles particulières supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontalière des attestations électroniques qualifiées d'attributs, le cas échéant. ».
[1149] Art. 45(c) et 45(d), *op. cit.*, Proposition de Règlement.
[1150] Conformément à l'art. 24 d'eIDAS-1
[1151] Section 1, (7), 6. « Les portefeuilles européens d'identité numérique sont délivrés dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie 'élevé' ». Dans les faits, cela risque de poser des difficultés à certains Etats membres dont le schéma d'identification électronique notifié n'est pas encore reconnu comme étant d'un niveau élevé.

n'est pas encore le cas pour la France dont le schéma d'identification électronique est d'un niveau de garantie substantiel à la date d'avril 2023[1152]. En d'autres termes, la France doit délivrer un schéma d'identification électronique dont le niveau de garantie est élevé afin de pouvoir délivrer son PIND.

Par ailleurs, l'amendement eIDAS-2 semble renforcer la complémentarité avec certaines règlementations financières étudiées précédemment (MiCA, TFR, Data Act). Pour les crypto-actifs, ces règlementations imbriquées (eIDAS-2 y compris) auront pour effet de recentraliser socialement et informatiquement[1153] leurs protocoles et écosystèmes décentralisés, tout particulièrement concernant les blockchains publiques. Ces règles de droit émanent ainsi et s'articulent au travers d'une pression politique et parfois sociale sur ces écosystèmes du Web 3.0. Concrètement, le droit et certaines technologies semblent réutilisés pour mieux identifier chaque acteur et chaque interaction au sein de diverses chaînes de valeur économiques, sociales et financières[1154]. Autrement dit, eIDAS-2 confortera une forme de centralisation indirecte par l'identification des acteurs du Web 3.0, au même titre que d'autres Règlements (MiCA, TFR), néanmoins sous couvert d'autres règles de droit et motivations politiques, pourtant toutes convergentes (contre les blockchains publiques). Si la neutralité technologique semble partiellement respectée par ces textes en droit, les échanges d'attributs électroniques qualifiés ne se feront avec eIDAS-2 que dans un circuit informatique en réalité plutôt fermé, c'est-à-dire majoritairement circonscrits entre des prestataires de services de confiance. Il s'agit plutôt d'une semi-ouverture de ces attributs électroniques qualifiés plutôt que d'une ouverture totale comme la Commission européenne peut le laisser paraître au sein de cet amendement et de ses références technologiques et littérales, par exemple en utilisant le terme « *universel* » à cinq reprises. Au sens des règles juridiques précitées et imposées par eIDAS-2, il apparaît que les blockchains publiques (Bitcoin, Ethereum) ne pourront jamais devenir des prestataires de services de confiance, c'est-à-dire remplir les conditions de certifications des prestataires de services de confiance qui sont centralisées. Cela implique qu'elles ne bénéficieront donc pas de la reconnaissance juridique précitée (présomption de fiabilité) dont bénéficient pourtant les blockchains privées et hybrides. Par conséquent, il semble se profiler une nouvelle tentative de désinstitutionalisation - par le droit - de l'adoption sociale actuelle des blockchains ouvertes, au profit des blockchains fermées, supposément plus protectrices des droits et efficientes[1155] dans tous les domaines d'après certaines communications et certains communicants politiques, institutionnels ou même gouvernementaux. Dès lors, eIDAS-2 semble indirectement favoriser cette lutte contre la décentralisation pure de certaines blockchains publiques, ce qui est d'après cette étude néfaste

[1152] Consultez les mises à jour concernant la France, d'après la liste officielle de la CE, disponible à l'adresse suivante
[1153] V. Annexe 7.
[1154] Considérant (31), « L'identification électronique sécurisée et la fourniture d'attestations d'attributs devraient offrir davantage de souplesse et de solutions au secteur des services financiers en ce qui concerne l'identification des clients et l'échange des attributs spécifiques nécessaires pour respecter […] la réglementation relative à la lutte contre le blanchiment de capitaux [TFR] et les exigences en matière d'adéquation découlant de la législation sur la protection des investisseurs [MiCA], ou pour permettre le respect d'exigences en matière d'authentification forte du client à des fins d'ouverture de session et d'exécution de transactions dans le domaine des services de paiement ».
[1155] V. Annexe 6, Focus 3.

pour tous les acteurs du Web 3.0, y compris paradoxalement pour les blockchains fermées, à la condition que cette hypothèse se confirme à l'avenir. Effectivement, les blockchains hybrides et privées tirent leur innovation technologique en grande partie de celles issues des blockchains publiques qui possèdent des communautés de développeurs bien plus importantes et sources d'innovation comme le constatent plusieurs parties précédentes et Annexes de cette recherche[1156]. De plus, ce manque de reconnaissance juridique semble paradoxalement déboucher sur une confusion au regard de l'utilisation textuelle du terme « *immuable* »[1157] en référence aux PIND qui reposeront donc sur des blockchains privées ou hybrides, centralisées et donc muables, car seules quelques blockchains sont informatiquement hautement décentralisées et donc immuables. Cela met en exergue une probable concurrence exacerbée - probablement assumée par le législateur européen[1158] - entre les blockchains ouvertes et fermées, comme semble le confirmer le faisceau de constats politiques et juridiques des autres Règlements européens mentionnés.

2.2 Les enjeux juridiques d'une identité 3.0 : vers des droits en ligne augmentés

L'identité numérique décentralisée implique des défis juridiques. Les droits en ligne augmentés qu'elle permet sont nombreux, notamment une plus grande autonomie pour les utilisateurs, une meilleure protection de la vie privée et une réduction de la dépendance aux tiers de confiance centralisés. Ses enjeux juridiques sont donc importants, mais ils nécessitent une coopération et un alignement règlementaire national ou international. Concrètement, en offrant une identité numérique forte et sécurisée, l'identité décentralisée peut contribuer à renforcer les droits des personnes, en leur donnant un moyen de prouver leur identité et de protéger leurs données personnelles. Grâce à son accessibilité en ligne ou hors ligne, les attributs d'une IND pourraient également aider à lutter contre les discriminations et les inégalités en fournissant un accès à des services aux populations qui en sont souvent exclues. En d'autres termes, chaque utilisateur devient plus autonome, libre et confiant en matière de preuve d'identification et d'authentification en ligne. Aucun tiers non autorisé ne peut en principe déjouer ou empêcher l'utilisateur de s'identifier à un service numérique (public ou privé). Les droits des utilisateurs deviennent ainsi « augmentés » ou plutôt « renforcés ». L'utilisation du terme augmenté dans cette étude a pour vocation de susciter un intérêt immédiat pour le grand public eu égard aux nombreux avantages de l'identité décentralisée. Il n'est ainsi pas fait référence à une signification transhumaniste. Le mouvement et les technologies de décentralisation permettront aux personnes de

[1156] V. Annexes 3 & 6 & 7
[1157] Considérant (9), « En s'appuyant sur le niveau de garantie 'élevé', les portefeuilles européens d'identité numérique devraient bénéficier du potentiel offert par des solutions infalsifiables », disponible à l'adresse suivante
[1158] Considérant (35), « La certification en tant que prestataires de services de confiance qualifiés devrait apporter une sécurité juridique aux cas d'utilisation fondés sur des registres électroniques. […] Les cas d'utilisation concernant des crypto-actifs devraient être compatibles avec toutes les règles financières applicables, par exemple avec la directive concernant les marchés d'instruments financiers, la directive concernant les services de paiement et le futur règlement sur les marchés de crypto-actifs [MiCA] ».

renouer avec l'exercice de leurs droits en ligne, à condition que des cadres juridiques et informatiques soient définis pour encadrer certaines de ses modalités d'expression. Si l'utilisation massive d'attributs d'identités décentralisées prendra probablement un certain temps à se diffuser dans la société civile en raison de son stade préindustriel en 2023, l'utilisation de la technologie blockchain possède déjà une avance notable pour certains services, notamment (crypto)financiers. Ainsi, l'adoption progressive de l'IND impliquera mécaniquement un renforcement de l'exercice des droits des personnes physiques et morales en ligne, grâce à une nouvelle identité numérique plus fluide, sécurisée, interopérable. Lorsqu'une blockchain privée ou hybride est utilisée avec les standards de l'IND, le niveau de confidentialité se trouve renforcé, car les données des utilisateurs sont échangées de façon pair à pair, bilatérale, sélective et cryptographiquement vérifiable. Ces caractéristiques sont particulièrement intéressantes pour les interactions numériques entre les services d'administrations publiques en ligne et les citoyens souhaitant réaliser des démarches en ligne, dont la collecte et le traitement des données par les autorités publiques peuvent être plus transparent et mieux contrôlés, tout en reposant sur un consentement numérique clair et non équivoque. Cette nouvelle 'identité cryptographique' qui sera en réalité informatiquement centralisée semble parfaire le concept de « *citoyen en réseau* » imaginé en 2014 par Pierre Bellanger[1159]. Cependant, l'identité décentralisée peut également avoir des implications plus nuancées en termes de propriété intellectuelle, de responsabilité, de confidentialité et de protection des données personnelles. Les utilisateurs peuvent en effet être tentés de falsifier leur identité numérique ou d'utiliser les attributs d'autres internautes à des fins illégales, ce qui pose des problèmes de responsabilité juridique. Le niveau élevé de confidentialité ne doit pas favoriser de comportements frauduleux et illicites, comme cela peut être le cas aujourd'hui sur certaines applications de messageries supposées chiffrées de bout en bout comme Telegram ou Signal[1160]. Dès lors, il revient aussi bien aux fournisseurs de solution d'IND, qu'au(x) législateur(s), de trouver un équilibre entre l'innovation technique 3.0 relative à la protection des données et l'altération de la sécurité juridique qu'elle peut engendrer en cas d'anonymat en relatif à des activités illicites. Les juridictions nationales peuvent également avoir des approches différentes quant à la règlementation des identités décentralisées, ce qui peut rendre difficile la mise en place de normes communes. Malgré ces défis qui semblent plutôt circonscrits à l'INAS, les avantages d'une identité numérique distribuée l'emportent donc sur ses inconvénients potentiels. Finalement, il s'agit de prendre conscience qu'au sein du Web 3.0, les régulateurs sont presque aussi importants que la régulation elle-même. En effet, si les régulateurs qui interprètent la règlementation ont des connaissances suffisantes pour comprendre les enjeux de ce dont ils discutent, les prises de position législatives en réponse auront toutes les chances d'être informatiquement et socialement pragmatiques et proportionnées.

[1159] BELLANGER Pierre, *La souveraineté numérique*, *op. cit.*, in *Revue Le Débat* 2012/3 (n°170), pp149-159.
[1160] ROOSE Kevin, CHEN Brian, « Are Telegram and Signal the Next Misinformation Hot Spots? », 30 février 2021, in *The New York Time*, consulté en ligne le 1 mars 2022.

2.2.1 Un renforcement du secret des correspondances et des affaires

Le secret des correspondances et des affaires est une préoccupation majeure respectivement pour les individus et pour les entreprises. Avec le développement des technologies de l'information et de la communication, la protection de la confidentialité et de la sécurité des données et des communications est devenue plus complexe. Le respect du secret des correspondances et des affaires est une condition essentielle à la protection des libertés individuelles et des intérêts économiques des personnes physiques et morales. A l'échelle nationale, la loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, prise en application de la Directive européenne (EU) 2016/943 du Parlement européen et du Conseil du 8 juin 2016, fixe le cadre légal de la protection des secrets d'affaires[1161]. Les conditions d'application sont depuis 2018 strictes sans pour autant entraver le droit à la liberté d'expression et de communication, le droit à l'information d'un salarié, le droit à la protection d'un intérêt légitime reconnu notamment par le droit de l'Union européenne[1162]. En pratique, chaque situation s'apprécie au cas par cas au visa de l'article L.151-1 du Code de commerce[1163]. La question de la preuve à rapporter est toujours complexe, mais les attestations vérifiables (VC), évoquées au chapitre précédent, peuvent offrir une nouvelle solution en permettant à chaque personne de prouver l'envoi, la réception, le partage ou l'accès à des informations auprès de ou par un tiers. Étant donné que le consentement est essentiel pour une IND, celle-ci permet une nouvelle forme de traçabilité cryptographique difficilement contestable, contribuant à renforcer les droits des personnes. L'identité numérique distribuée offre donc une source de confiance en ligne ainsi qu'une forme de présomption de fiabilité des correspondances à laquelle des preuves cryptographiques conformes au droit de la protection des données sont associées. Aujourd'hui majoritairement liée à des blockchains fermées, une IND semble ainsi de nature à garantir les conditions de sauvegarde du secret des correspondances et du secret des affaires, par une identification certaine des informations et de leurs auteurs, de façon probante, sécurisée et résiliente. Les progrès technologiques ont donc ici ouvert la voie à de nouvelles solutions informatiques qui renforcent l'effectivité du droit, en assurant la confidentialité des échanges et des communications.

[1161] Loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, complétée par le décret n°2018-1126 du 11 décembre 2018 relatif à la protection du secret des affaires, pris en application de la Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulguées (secret d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

[1162] MORALES Valérie, « Mais le secret des affaires n'est pas un talisman absolu », in *Marvellavocats.com*, Les actualités de Marvell Avocats, v. également De MAISON ROUGE Olivier, avocat, « Petit guide juridique de protection du secret des affaires », 1ère parution, 13 octobre 2020, in *Village de la Justice*.

[1163] Art. L.151-1 du Code de commerce « Est protégée au titre des affaires toute information répondant aux critères suivants : 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur activité ; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret ».

2.2.2 Simplification et renforcement de la conclusion des contrats

Sans reprendre les conditions de la conclusion d'un contrat, au visa des articles 1112 à 1127-6 du Code civil pour être régulièrement formé, ni les dispositions de la loi n°2000-230 du 13 mars 2000[1164] sur la signature électronique qui a plus de vingt ans, les échanges dématérialisés se sont depuis considérablement développés. C'est la confiance entre contractants qui assure la bonne exécution d'un contrat dans le temps. Il est donc essentiel que les parties contractantes puissent dès le départ s'identifier, échanger avec certitude et vérifier la qualité des informations personnelles ou contextuelles échangées. Les normes d'identité numérique distribuée fournissent cette garantie grâce à la réception, l'assimilation et le consentement des parties via des attributs 3.0 (VC, DID). A ce titre, ces normes cryptographiques en cours de reconnaissance légale sont utiles pour les actes passés sous seing privé qui représentent plus de 90% des écrits des citoyens[1165]. La présente étude suggère ainsi que l'IND est une innovation technologique qui peut simplifier et renforcer la conclusion des contrats en ligne. Grâce à ces technologies, les parties contractantes peuvent échanger des informations confidentielles et sécurisées sans avoir besoin d'intermédiaires pour valider leur identité. Cela permet de réduire les coûts et les délais associés à la vérification des identités, ce qui peut également accélérer la conclusion ou l'amendement des contrats. De plus, l'identité distribuée permet de garantir l'authenticité et l'intégrité des informations échangées entre les parties, ce qui renforce in fine la confiance et la crédibilité des transactions en ligne. En incorporant progressivement ces nouvelles briques technologiques 3.0, les parties contractantes peuvent donc bénéficier d'un cadre juridique sur mesure et plus efficace pour la conclusion de contrats phygitaux, ce qui semblerait favoriser le développement de l'économie numérique. L'identité distribuée renforce donc tant le cadre théorique de la contractualisation (ex post et ex ante) que son exécution finale. Depuis l'identification des parties jusqu'à la qualité juridique des échanges et/ou l'archivage d'informations (documents, mandats, bénéficiaires), la relation contractuelle peut être augmentée, c'est-à-dire renforcée pour atteindre une nouvelle forme d'optimisation juridique.

2.2.3 Vers un consentement accru pour les internautes

Le consentement peut se définir comme la volonté d'engager sa personne ou ses biens de manière tacite (supposée) ou bien expresse (exprimée)[1166]. Le consentement d'une personne peut être déduit d'un faisceau d'éléments apparents et non équivoques. Toutefois, un arrêt de la CJUE dispose en 2020 qu'un accord passif ou tacite en ligne n'emporte pas nécessairement un consentement, notamment « *en cas de*

[1164] Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF du 14 mars 2000.
[1165] OUCHALLAL Mehdi, « Acte sous seing privé : de quoi s'agit-il ? », in *LegalPlace,* 2022, disponible en ligne
[1166] BRAUDO Serge, conseiller honoraire à la Cour d'appel de Versailles, « Définition du consentement », in *Dictionnaire de droit privé,* disponible en ligne

silence, de cases cochées par défaut ou d'inactivité »[1167]. En effet, la formation d'une volonté claire et non équivoque en matière de consentement en ligne semble souvent incomplète dès lors qu'elle est réduite à quelques clics de clavier ou de souris sur un service en ligne. Certains consentements numériques ne respectent ainsi qu'une partie seulement des critères de transparence énoncés au visa de l'article L.111-1 du Code de la consommation qui édicte que « (…) *le professionnel communique au consommateur, de manière lisible et compréhensible, les informations suivantes : 1° Les caractéristiques essentielles du bien ou du service, ainsi que celles du service numérique ou du contenu numérique, compte tenu de leur nature et du support de communication utilisé, et notamment les fonctionnalités, la compatibilité et l'interopérabilité du bien comportant des éléments numériques, du contenu numérique ou du service numérique* (…) »[1168]. De nombreux services en ligne peinent alors à assurer à leurs utilisateurs une lisibilité et une compréhension suffisantes des conditions contractuelles associées à leurs services numériques, sur le plan du consentement[1169]. Effectivement, chaque internaute pourrait régulièrement mettre en cause son consentement et ses actes associés, en raison de certaines informations (pré)contractuelles souvent insuffisantes, voire inintelligibles. Un consentement en ligne doit idéalement résulter d'une activité personnelle pour écarter toute interprétation aléatoire. Cela suppose une information et une compréhension totale des droits et des obligations associées à chaque service en ligne. A cette fin, les outils et les qualités intrinsèques de l'IND semblent pertinents. Parce que la notion de consentement repose sur une transparence numérique des biens ou des services dont il est question, comme démontré précédemment dans ses aspects techniques, elle offre par conception une forte traçabilité et transparence informatique. L'IND contribuerait ainsi à renforcer, c'est-à-dire à optimiser et à augmenter la capacité en ligne d'une personne à consentir. En ce sens, les règles du droit de la consommation et les normes informatiques de l'IND semblent se compléter dans leur technique informatique et juridique respective, au bénéfice des personnes et de leurs identités en ligne. Par exemple, depuis 2021, les sociétés IN Groupe, Orange et Agdatahub proposent une solution d'identité numérique distribuée nommée « *Agriconsent* ». Cette solution 3.0 qui articule des IND avec une blockchain privée fonctionne – via un PIND - au service d'un consentement inédit pour les 80 000 agriculteurs répertoriés en France. L'identité décentralisée s'avère véritablement pertinente notamment en matière d'information. L'article L.1112-1 du Code de la consommation dispose « *celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant.* (…) *Il incombe à celui qui prétend qu'une information lui était due de prouver que l'autre partie la lui devait, à charge pour cette autre partie de prouver qu'elle l'a fournie* »[1170]. Les lois sur les

[1167] Arrêt CJUE, 11 novembre 2020, affaire C-61/19 opposant Orange Roumanie SA à l'Autorité nationale de surveillance du traitement des données à caractère personnel Roumaine, dans le cadre d'une question préjudicielle posée à la Cour.
[1168] Art. L.111-1 du Code de la consommation dans sa version en vigueur depuis le 1er octobre 2021, Livre Ier : Informations des consommateurs et pratiques commerciales - Légifrance, consulté en ligne le 16 février 2022.
[1169] SOLANS Julia, « Réussir à lire les CGU de la SNCF vous prendra près de 7 heures ! », 4 février 2022, in *Capital.fr*
[1170] Art. 1112-1 du Code de la consommation dans sa version en vigueur depuis le 1er octobre 2016.

données personnelles prévoient systématiquement un traitement légal reposant sur le consentement, ainsi qu'un certain nombre d'exceptions lorsque le consentement n'est pas requis. Le consentement doit ainsi pouvoir être révoqué dans le cadre de relations numériques récurrentes. En droit de la santé, le consentement est un accord donné de manière libre et éclairée par une personne physique pour recevoir un traitement médical ou un soin. Le consentement doit être donné de manière volontaire et ne peut être obtenu par la force, la violence (harcèlement), la menace, la contrainte, la manipulation, l'intimidation, la fraude ou l'abus de confiance. Ces infractions se transposent et se constatent désormais en ligne, parfois au point d'atteindre physiquement les internautes. Le droit de la santé exige donc un consentement éclairé, ce qui signifie que la personne doit avoir suffisamment d'informations sur son état de santé, sur les traitements médicaux ou sur les soins qui lui sont proposés, avec les risques et les bénéfices potentiels, ainsi que concernant les alternatives éventuelles à sa portée. A cet égard, la personne doit avoir le temps et l'opportunité de poser des questions et de recevoir des réponses avant de donner son consentement. Au sens de cette étude, ces dispositions du Code de la santé publique[1171] pourraient inspirer le législateur pour un renforcement du consentement en ligne des personnes, aujourd'hui insuffisant au regard des échanges permanents en ligne. Si certains consentements tacites peuvent parfois suffire, la portée importante de cet outil informatique fiable que représente l'IND permet d'assurer un consentement effectif au service du quotidien en ligne et hors ligne des citoyens. Cette notion de consentement cryptographique est au cœur de cette identité 3.0 et la DIF[1172], mentionnée préalablement, propose d'ores et déjà la normalisation de récépissés de consentement 3.0 (désigné par « *Data Agreement* »)[1173] pour le stockage et la traçabilité de consentements numériques (VC).

2.2.4 Une liberté d'expression en ligne renforcée pour les citoyens

La liberté d'expression est un droit fondamental inscrit dans la Constitution française et reconnue par de nombreux traités internationaux et conventions internationales. Il s'agit du droit de s'exprimer librement, sans censure ni restriction, que ce soit par écrit, par oral ou par tout autre moyen de communication. L'identité d'une personne est ainsi intimement liée à une liberté de s'exprimer, de penser et de choisir, c'est-à-dire à sa capacité de revendication concernant tout ou partie de ses appartenances. Dès lors, la liberté d'expression peut être appréhendée sous un angle identitaire au travers des différentes façons de l'exercer en ligne, c'est-à-dire de son identité vécue. Elle représente ainsi le droit de choisir le support

[1171] Art. L1111-2 du Code de la santé publique : « Toute personne a le droit d'être informée sur son état de santé [numérique] » ; Art. L1111-4 du Code de la santé publique : « Toute personne a le droit de refuser ou de ne pas recevoir un traitement [informatique] » (ici ajouté et souligné par l'auteur).
[1172] « The Decentralized Identity Foundation (DIF) exists to advance the interests of the decentralized identity community (…) », in *Identity.foundation.com*.
[1173] Ces reçus de consentement sont alignés sur les normes ISO et certaines sociétés sont sur le point de lancer un nouveau projet dans le cadre de la *Decentralized Identity Foundation,* notamment pour définir le protocole et la mise en œuvre de référence concernant ces « Data Agreement ».

informatique souhaité pour s'exprimer. Le Conseil d'Etat rappelle que la liberté d'expression occupe dans le système des droits fondamentaux une place essentielle. En effet, constituant une condition de la liberté de la pensée, elle exprime l'identité et l'autonomie intellectuelle des individus et conditionne leurs relations aux autres individus et à la société[1174]. Un lien étroit entre liberté d'expression et liberté d'auto-détermination informationnelle[1175] se dessine ainsi au bénéfice de l'identité des personnes et de ce droit fondamental. L'identité numérique auto-souveraine (INAS) semble ainsi se rapprocher de la perception et du souhait d'une liberté d'expression totale mentionnée par la philosophe et humaniste française Simone Weil en 1949 : « (…) *la liberté d'expression totale, illimitée, pour toute opinion quelle qu'elle soit, sans aucune restriction ni réserve, est un besoin absolu pour l'intelligence* »[1176]. Il revient donc à l'Etat d'assurer à tout prix la possibilité d'une liberté d'expression en ligne en garantissant son rôle de bâtisseur de l'expression et des débats publics, tout en certifiant le sérieux de solutions d'IND à la disposition des utilisateurs (conformément à eIDAS-2 évoqué précédemment). Concernant les solutions d'identité numérique auto-souveraine, il s'agit de ne pas tenter de les interdire ou de freiner leur développement qui se trouve d'ores et déjà limité par le marché comme cela est démontré dans cette étude. Finalement, le Web 3.0 pourrait offrir des moyens technologiques innovants pour renforcer ce droit universel à l'expression ou du moins y contribuer. Les citoyens peuvent donc se prévaloir de la liberté d'expression en ligne, dans les limites du droit positif qui peut en limiter l'étendue et l'expression dans certains cas légitimes, où les outils 3.0 deviendraient autant des mécanismes de défense que de contrôle de ce droit à vocation universelle.

2.2.5 Vers une auto-détermination informationnelle de l'identité personnelle

Il convient de rappeler que la disponibilité croissante des données à caractère personnel sur les réseaux informatiques tend, avec leurs multiples applications, à diminuer l'importance de la maîtrise de ses données tout en brouillant les notions de consentement et de libre arbitre, pourtant essentielles. Tout au long de l'histoire, de nombreux individus ont privilégié une ou plusieurs facettes de leur identité au détriment de celles d'autres personnes (censures, contrôle de l'information). Ce constat qui apparait comme répété depuis l'avènement d'Internet met en exergue un nouveau courant juridique en faveur de l'introduction d'un ancien principe issu du droit allemand, le droit à « *l'auto-détermination informationnelle* »[1177] des personnes. Ce courant trouve son origine dans un arrêt du 15 décembre 1983

[1174] VERPEAUX Michel, « La liberté d'expression dans les jurisprudences constitutionnelles », 2022, in *Conseil constitutionnel*, disponible à l'adresse suivante
[1175] V. partie suivante.
[1176] WEIL Simone, « L'enracinement : prélude à une déclaration des devoirs envers l'être humain », 1949, coll. idées, disponible à l'adresse suivante
[1177] Traduit de l'allemand « Selbstbestimmungsrecht ». Ce terme peut être traduit par « droit à l'autodétermination » ou « droit à l'autodétermination personnelle ».

de la Cour Constitutionnelle allemande (« *Karlsruhe* »)[1178]. En droit allemand, ce concept est souvent utilisé pour faire référence au droit fondamental d'une personne à prendre des décisions concernant sa propre vie, à exercer une certaine liberté et autonomie dans ses choix, et à être protégée contre toute ingérence injustifiée de tiers ou de l'État. L'article 2 de cette loi garantit le droit de toute personne à la liberté personnelle, qui inclut le droit à l'autodétermination[1179]. Ce droit est souvent invoqué dans des contextes tels que le droit à la vie privée, le droit à l'intégrité physique et psychologique, le droit de choisir son lieu de résidence, le droit de décider de sa propre orientation sexuelle ou encore de son identité de genre. Finalement, ce droit est un concept important en droit allemand qui protège le droit fondamental de toute personne à prendre des décisions autonomes concernant sa propre vie, à condition que ces décisions n'entravent pas les droits et les libertés d'autres personnes ou encore l'intérêt général. Appliqué à la sphère numérique, ce droit prône ainsi une capacité de l'individu à maîtriser ses données à caractère personnel[1180]. Comme le rappelle Aurélien Bamdé, Docteur en droit, la Cour « [Constitutionnelle Allemande] *garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel […] l'autodétermination est une condition élémentaire fonctionnelle dans une société démocratique libre, basée sur la capacité des citoyens d'agir et de coopérer* »[1181]. L'autodétermination informationnelle consiste donc à permettre aux individus de contrôler la collecte, l'utilisation et le partage de leurs informations personnelles, en leur donnant la possibilité de choisir de les partager ou non, d'y accéder et de les corriger si nécessaire. Cela devient particulièrement important dans le contexte numérique actuel où les données personnelles peuvent être facilement collectées et stockées. Cette approche semble protéger la vie privée et l'autonomie de chaque individu en veillant à ce que les organisations qui collectent des informations personnelles soient transparentes quant à leur utilisation et n'utilisent pas ces informations à d'autres fins que celles pour lesquelles elles ont été collectées. Bien que l'identité soit pour rappel à la fois inclusive et exclusive[1182], l'autodétermination informationnelle vise une identité plutôt inclusive. Cette approche est liée à l'identité numérique des personnes et pourrait être reconnue explicitement au sein de l'UE pour mieux protéger les données personnelles. Cependant, cette étude affirme que l'existence physique de chaque individu doit toujours être supérieure à sa représentation numérique, contrairement à certaines promesses utopiques du Métavers qui est étudié plus loin. L'autodétermination informationnelle pourrait

[1178] La Cour constitutionnelle fédérale est l'organe juridictionnel suprême en matière constitutionnelle en Allemagne. Elle est chargée de garantir le respect de la Constitution allemande, la Loi fondamentale, ainsi que de veiller à la protection des droits fondamentaux des citoyens allemands. Le terme « *Karlsruhe* » est souvent utilisé pour faire référence à la Cour constitutionnelle fédérale elle-même ou à ses décisions, qui ont souvent un impact significatif sur la vie politique et juridique allemande.

[1179] Art. 2, [Liberté d'agir, liberté de la personne] (1) « Chacun a droit au libre épanouissement de sa personnalité pourvu qu'il ne viole pas les droits d'autrui ni n'enfreigne l'ordre constitutionnel ou la loi morale », disponible à l'adresse suivante

[1180] BAMDE Aurélien, « Autodétermination informationnelle », §2 : Le droit à l'autodétermination informationnelle, 2018, in *aurelienbamde.com*, consulté en ligne le 9 février 2022.

[1181] *Ibid.*

[1182] *Op. cit.,* MAALOUF Amin, « Les identités meurtrières », « […] grâce à chacune de mes appartenances, prise séparément, j'ai une certaine parenté avec un grand nombre de mes semblables », p.27.

contribuer à la minimisation des données et au consentement des personnes précités[1183], grâce aux solutions d'identité numérique (IND), à la condition que ces solutions soient encadrées par des Règlements européens comme eIDAS-2. Pour adopter un tel système, il serait sage que chacun réalise préalablement un « *examen d'identité* [numérique] »[1184] afin de prendre conceptuellement conscience de son identité en ligne tout en évitant certains abus pourtant connus. Enfin, l'accès aux services gouvernementaux sans identification numérique doit être maintenu au profit de la possibilité d'une identification physique ou de systèmes de délégation numérique fiable. Finalement, le droit à la protection des données est souvent considéré comme une mesure de défense, tandis que le droit à l'autodétermination informationnelle propose une approche plus proactive car alignée sur les textes européens dédiés à la protection des données et reposant sur la base des valeurs de l'individu. Cette approche ambitieuse vise à rétablir le contrôle des individus sur leurs données personnelles, qui sont progressivement perçues et traitées comme des biens à marchander[1185].

2.2.6 L'utopie renforcée d'une patrimonialisation et d'un droit de propriété sur ses données

La notion de propriété dans son acceptation générale s'exprime au travers des biens qu'une personne possède, ces derniers n'étant en réalité qu'une extension de la pleine propriété personnelle et revendiquée d'une personne par rapport à d'autres. La propriété est ainsi une extension de notre identité la plus personnelle, c'est-à-dire de nous-mêmes comme le défendait John Locke[1186]. Par exemple, le fait d'être propriétaire d'une maison procure une sensation de sécurité et de confiance, car cela permet au propriétaire d'exiger le départ de toute personne qui s'introduirait chez lui sans son consentement, sans qu'elle ait aucun lien subjectif avec ledit bien propriétaire. En conséquence, le droit de propriété crée une relation de pouvoir et de domination. Toutefois, ce raisonnement préliminaire semble surtout transposable aux données d'identité primaire (et non pas secondaires)[1187]. Le droit de propriété sur une chose ne peut perdurer dans le temps que grâce à une identité légale et racine administrée et rendu possible par un Etat de droit. Il semble néanmoins important de faire la distinction entre notre identité et les biens acquis pour aborder la question de la commercialisation des données personnelles. Si la frontière entre les deux peut être étroite et ductile, elle n'en demeure pas moins cruciale puisqu'un attribut d'identité émane de notre propre existence contrairement à un bien acquis. Il doit ainsi être gardé à l'esprit qu'une donnée n'est pas un bien tangible, bien au contraire. Face au dilemme de la reproduction

[1183] SCHWAB Pierre-Nicolas, « Statistiques RGPD Europe : évolution du nombre de plaintes par pays », « 64% des DPO anglais ont constaté [2018] une augmentation du nombre de demandes après la mise en place du RGPD », 2019, in *intotheminds.com*, consulté en ligne le 9 février 2022.
[1184] MAALOUF Amin, « Les identités meurtrières », p.23.
[1185] V. partie suivante.
[1186] BREMAEKER Nathalie, « L'identité de la personne humaine au croisement du droit et de la psychanalyse », Thèse en Droit à l'Université de Perpignan, 2021, « John Locke défendait déjà l'idée que nous sommes propriétaires de nos biens mais aussi de nous-mêmes », p.274.
[1187] V, *supra*, I, Titre 1, 2.2

infinie des données présentes sur Internet[1188], les technologies décentralisées promettent l'espoir d'un nouveau Graal de la propriété numérique. Comme le relève l'auteur Pierre Bellanger[1189], les données n'appartiennent plus aux utilisateurs, un constat auquel échappent toutefois certains crypto-actifs les plus décentralisés[1190]. En théorie, ces nouveaux modèles informatiques et commerciaux pourraient offrir aux utilisateurs de services en ligne la possibilité de recevoir une rémunération partielle ou totale en crypto-actifs en échange du partage de leurs attributs d'identité numériques soit par la vente de leurs données personnelles. L'objectif de la patrimonialisation des données n'est donc pas seulement de créer un revenu passif pour les internautes (aspect commercial et publicitaire), mais surtout et supposément de réintégrer cette valeur individuelle dans une chaîne de valeur collective où la personne physique, émettrice et source de données, redevient l'acteur central et essentiel de son identité. Pierre Bellanger estime qu'il s'agit de reconnaître que la racine des problématiques liées aux données provient d'une non-reconnaissance de leur droit de propriété. Selon lui, il faudrait simplement « (…) *étendre le statut de données personnelles à l'intégralité de la trace informatique d'une personne et lui reconnaître la nature de bien incorporel* »[1191]. Une telle réappropriation juridique permettrait théoriquement aux personnes physiques de délimiter librement l'usage qu'ils font de ces biens incorporels, en contrepartie par exemple d'une interdiction de leur usage ou d'une cession à des tiers. Soulignons que les biens incorporels sont des biens qui ne possèdent pas de forme physique ou matérielle, mais qui possèdent une valeur économique. Ils comprennent des éléments tels que les droits de propriété intellectuelle, les marques commerciales, les brevets, les licences, les savoir-faire, les bases de données, les secrets commerciaux et autres avantages économiques qu'ils représentent. Le législateur et les institutions publiques ont abordé la question des données personnelles sous un angle utilitaire, dans le but de protéger les droits en ligne des individus. Pour ce faire, une classification et une nomenclature jurisprudentielle ont été mises en place, avec plusieurs catégories de données (données de santé, données religieuses), afin de règlementer l'utilisation de chaque type de données et de prévenir tout abus. Cependant, cette nomenclature exclut certains types de données de sa protection, comme certaines données professionnelles qui ne sont pas nécessairement considérées comme des données personnelles ou sensibles au sens de cette nomenclature, une lacune identifiée et consacrée dans la partie dédiée au RGPD[1192]. En 2022, les discussions juridiques portent sur la protection de la vie privée plutôt que sur le droit de propriété, qui est toujours considéré comme un sujet complexe par les juristes.

[1188] PERRY BARLOW John, traduction de l'anglais, « Si notre propriété peut être reproduite à l'infini et distribuée instantanément sur toute la planète sans coût, à notre insu, sans même qu'elle quitte notre possession, comment pouvons-nous la protéger ? », 1994, in *The Economy of Ideas*, consultez en ligne à l'adresse wired.com

[1189] « *Res nullius* » est une expression latine utilisée en droit civil, qui désigne une chose sans maître, c'est-à-dire qui n'a pas de propriétaire mais qui est néanmoins appropriable. BELLANGER Pierre, « La Souveraineté Numérique », *op. cit.*, « À ce jour, les données n'appartiennent en droit à personne. Elles sont res nullius ».

[1190] V. *supra* partie afférente

[1191] *Op. cit.*, BELLANGER Pierre, « La Souveraineté Numérique », Ed. Kindle, emplacement 2569 sur 3565.

[1192] V. *supra*, I, Titre 2, 2.4

Cette réticence à reconnaître un droit patrimonial sur les données personnelles a été mise en évidence dès 2014 par le Conseil d'Etat[1193]. Dans cette étude de 2014, le Conseil d'Etat a en effet jugé qu'il n'était pas souhaitable de transformer le droit subjectif à la protection des données personnelles en un droit patrimonial. Il est donc nécessaire de prendre en compte la complexité de cette question pour tenter de fournir des éléments de réponse tant sur le plan juridique qu'informatique. Selon Gaspard Koenig[1194], essayiste et philosophe français, un constat doit être dressé en raison d'un abandon des données en ligne au profit d'un accès gratuit et permanent à des services en ligne. D'après cet auteur, cette cession opaque et sans contrepartie équivalente de l'émanation de notre « *moi* » - non corporel selon lui - est possible sous couvert d'une illusion de la protection des données en ligne alimentée par le RGPD. Gaspard Koenig souligne que cette gestion oligopolistique des données serait comparable à un « *système numérique féodal* »[1195]. Puisque les données ont une valeur, pourquoi ne pas simplement la reconnaître ? Combien vaut une donnée et cet objet numérique en vaut-il la peine ?[1196] Face à cette centralisation inédite des données des personnes au sein d'une sphère numérique en apparence infinie, deux principaux courants de pensée s'affrontent donc en termes de valorisation des données, le premier (i) contre une monétisation ou patrimonialisation des données personnelles et le second (ii) en faveur d'un tel principe.

(i) Certains juristes et certaines institutions (CNIL) estiment que le RGPD offre des garanties adéquates pour faire face à la collecte massive de données générées par les personnes physiques[1197]. De plus, certains considèrent que la monétisation des données ne confère pas un droit de propriété sur ces dernières, ce qui suggère qu'une frontière intermédiaire existerait entre la protection et la monétisation des données. En réalité, il semble que ces contrats de monétisation de données ne constituent pas une « *vente* »[1198] de données personnelles, mais plutôt une autorisation d'exploitation dans le respect du cadre juridique mentionné. En France, l'indisponibilité des données d'état civil ainsi que les solutions d'identité numérique fédérées et régalienne, comme FranceConnect, assurent une définition ainsi qu'une forme de protection des droits des personnes pour réaliser certaines interactions en ligne. A l'opposé, le Common law permet aux États-Unis de céder à titre onéreux

[1193] Sénat, « Projet de loi pour une République numérique », Rapport n°534 déposé le 6 avril 2016, in *www.senat.fr*, consulté en ligne le 20 novembre 2021, « le Conseil d'État, dans son étude de 2014, a considéré qu'il n'était pas souhaitable de transformer le droit personnel à la protection des données personnelles en un droit patrimonial. ».
[1194] KOENIG Gaspard, « […] le soi n'a jamais été autant sollicité. Il est temps de comprendre à qui il appartient. », « La propriété de soi », consulté en ligne le 18 novembre 2021.
[1195] Il est possible de faire un parallèle avec le Moyen-Âge, où les paysans fournissaient tout ou une partie de leur récolte aux seigneurs en échange d'une protection contre les attaques ennemies. De manière similaire, les internautes cèdent tout ou partie de leurs données en ligne (souvent via des CGU opaques, inintelligibles, voire léonines) en échange de la gratuité des services en ligne.
[1196] Selon le simulateur en ligne simulator.drdata.io, la valeur des données personnelles de l'auteur de la présente recherche valent environ 109 euros en 2022. D'après ce simulateur, il est remarqué que les *données d'identité primaires* qui semblent le plus valorisés financièrement sont le niveau d'étude, le numéro de sécurité social ainsi que le numéro de téléphone qui valent plus que d'autres *données* identifiées comme *secondaires* par notre étude (consultez les catégories « CSP » et « Internet & Consommation »).
[1197] ANCIAUX Arnaud, FARCHY Joëlle, « Données personnelles et droit de propriété », in *Rev. Int. Droit Econ.*, 2015, consulté en ligne le 20 novembre 2021.
[1198] « Annales des Mines N°18 sur les Enjeux Numériques : Propriété et gouvernance du numérique », *op. cit.*, p. 30.

certaines parties du corps humain[1199], ce qui ouvre par extension idéologique le champ à une patrimonialisation des données personnelles, qu'elles soient considérées comme corporelles ou incorporelles. Dans notre droit positif, un tel positionnement contreviendrait au principe d'indisponibilité des données, s'agissant d'une frontière déjà adoptée dans une majorité des pays du monde. Parce que les données caractérisent une personne, il semble qu'elles doivent rester indisponibles à tout tiers à l'instar du corps humain qui ne peut d'ores et déjà pas faire l'objet d'une commercialisation en vertu du droit interne.

(ii) Certains penseurs estiment qu'en reconnaissant les données en tant que patrimoine, cela permettrait une nouvelle émancipation des données et de leurs échanges. Cette position repose en partie sur le postulat de John Locke selon lequel chaque individu possède une propriété sur sa propre personne, que personne d'autre ne peut revendiquer[1200]. Pour réaliser cette reconnaissance, plusieurs mécanismes contractuels peuvent être envisagés, tels que l'extension du droit de propriété appliqué aux données personnelles ou des licences d'exploitation, plutôt que la propriété sociale et temporaire proposée par Thomas Piketty, économiste et Professeur à l'EHESS[1201]. Selon Gaspard Koenig, l'absence de patrimonialité de soi est un vestige théologique dans notre droit et dans notre organisation sociale qui nous empêche de déterminer nos propres valeurs[1202]. Le principal défi de cette reconnaissance financière de notre patrimoine numérique n'est plus seulement technologique, mais surtout moral et politique. Il est nécessaire de se demander si valoriser les données des personnes et leur identité est bénéfique, et si nous sommes prêts à abandonner notre conception démocratique de l'autonomie de jugement au profit d'entités étrangères, ou si nous allons nous réapproprier nos données au nom d'une société numérique libérée grâce au Web 3.0. Il est également pertinent de se demander pourquoi la monétisation de nos données serait indisponible voire prohibée alors que paradoxalement de nombreux services en ligne la mettent en œuvre par des arrangements légaux subtils comme avec l'application de conditions générales d'utilisation (CGU) ou encore de contrats d'adhésion numérique, auxquels les internautes ne peuvent se soustraire au sein du Web 2.0. Un droit de propriété sur nos données personnelles permettrait d'en disposer librement (partage, cession, destruction) conformément aux dispositions de l'article 544 du Code civil qui dispose que

[1199] KOENIG Gaspard, « La propriété de soi », *op. cit.*, « […] certaines parties du corps comme les cheveux, ou le sang aux États-Unis, peuvent être objets de commerce », p.2.
[1200] LOCKE John, « Second Treatise, § 25--51, 123--26. Chap. V. of Property. », consulté en ligne le 20 novembre 2021, « chaque Homme possède individuellement une propriété sur sa propre personne ; il s'agit de quelque chose dont personne d'autre n'a aucun droit sur celle-ci », in *Rapport* « Mes data sont à moi. Pour une patrimonialité des données personnelles », LANDREAU Isabelle, PELIKS Gérard, BINCTIN Nicolas, PEZ-PERARD Virginie et al., 2018, disponible à l'adresse suivante, p.18.
[1201] PIKETTY Thomas, « Je propose de dépasser la propriété privée par la propriété sociale et temporaire », consulté en ligne le 20 novembre 2021, 9 septembre 2019, in *France Inter*, disponible à l'adresse suivante
[1202] KOENIG Gaspard, « La propriété de soi », *op. cit.*, « L'absence de patrimonialité de soi nous empêche de déterminer pour nous-mêmes nos propres valeurs. C'est un reliquat théologique dans notre droit et notre organisation sociale. ».

« *la propriété est le droit de jouir et disposer des choses de la manière la plus absolue* (…) ». Cependant le droit de patrimonialité sur ces données dépend d'un libre arbitre et d'une capacité préalable, c'est-à-dire d'être libre de choisir de disposer de soi-même. Parce que le droit de propriété est un droit réel (« *Ius in re* ») qui porte sur une chose, il s'agirait en amont de qualifier une donnée personnelle en tant que bien incorporel et réel, comme susvisé. Dans cette configuration, le droit d'une personne à disposer de ses données s'arrêterait en pratique là où commence le droit à disposer des données d'une autre personne, ce qui induit de rappeler :

a. La loi de 1978 (CNIL) complétée par le Règlement RGPD qui établit des règles strictes en matière de protection de la vie privée des personnes. Les données personnelles ne peuvent être collectées, utilisées ou communiquées à des fins commerciales sans l'accord préalable et éclairé des personnes concernées. Une fois un tel consentement acté, une monétisation partielle des données est possible dans les limites contractuelles qu'imposent ce Règlement (récolte encadré, droit de rétraction, suppression des données, etc.).

b. Il s'agit de comprendre si le droit traiterait de manière égale tous les biens incorporels existants (tels que les données personnelles), et si les propriétaires de ces biens pourraient en tirer profit de manière similaire. Toutefois, dans certaines situations, la création de données dérivées ou agrégées pourrait porter atteinte à la substance de la donnée initiale (son attribut racine et pivot), ce qui altérerait le droit de propriété par effet sous-jacent. La contractualisation systématique des échanges concernant les données personnelles, grâce à l'identité décentralisée, impliquerait que l'identité des personnes serait soumise à cette contractualisation. Cependant, le droit de propriété permettrait à chacun de choisir librement ses valeurs, qu'elles soient positives ou négatives pour l'intérêt commun.

c. Le droit de disposer et d'accomplir tous les actes susceptibles de conduire à une volontaire perte totale ou partielle de son bien incorporel, le propriétaire étant investi d'un pouvoir d'affecter la substance de la chose par certains actes matériels (la consommer, la détruire, l'améliorer) ou juridiques (la transférer, la démembrer).

Dès lors, le tableau suivant permet de résumer les arguments pour et contre une patrimonialisation des données :

Arguments POUR	Arguments CONTRE
La patrimonialisation des données des internautes, soumise à des conditions contractuelles spécifiques tels que la durée et le type de données concernées, permet leur valorisation via des transactions d'achat et de vente. Cette valorisation pourrait aider à sensibiliser les individus sur la valeur de leurs données personnelles, voire les responsabiliser davantage vis-à-vis de celles-ci.	Sur le plan juridique, il existe un risque de conflits de lois, pour ce qui concerne la cession de données personnelles. Certains juristes considèrent que cette pratique est contraire aux dispositions d'ordre public de la loi informatique et liberté de 1978 ainsi qu'au Règlement RGPD qui compromettent tant la monétisation des données. Pour reconnaître un droit de propriété sur ses données, il est nécessaire de répondre à certaines questions et incertitudes, telle la manière d'identifier avec certitude le propriétaire d'une donnée, ou comment gérer les conflits de lois entre les régimes de protection stricte des données (RGPD en Europe) et ceux susceptibles d'accepter une patrimonialisation des données comme aux États-Unis. Mettre en œuvre une monétisation des données personnelles est possible, mais implique un cadre juridique contraignant[1203] et en réalité bien souvent utopique pour les utilisateurs finaux comme le suggèrent certains juristes : « *force est pour le juriste de constater que le RGPD ne facilite pas la mise en œuvre de monétisation. De plus, au-delà des questions de droit, la monétisation est souvent un marché de dupes pour la personne concernée, soit qu'elle n'ait pas vraiment conscience de cette monétisation, soit qu'elle n'ait pas de choix réel si elle veut bénéficier d'un service, soit enfin qu'elle n'en retire qu'un intérêt économique mineur quand elle décide de commercialiser, elle-même, ses données* »[1204].
Sous réserve de l'utilisation de technologies 3.0, la patrimonialisation des données permettrait d'assurer la sécurité informatique et le contrôle cryptographique des données par les individus, réduisant ainsi en théorie l'utilisation non autorisée de leurs données personnelles.	Sur le plan informatique, il existe un risque d'effet « *pot de miel* »[1205], c'est-à-dire un phénomène d'attraction des pirates informatiques. Plus les données sont valorisables et regroupées (centralisées), plus elles risquent d'être attaquées et pillées d'où l'importance de les distribuer/décentraliser.
La technologie blockchain et l'identité décentralisée pourraient dissiper la nature économiquement non-rivale des données qui empêchent actuellement leur patrimonialisation. En d'autres termes, ces technologies	D'un point de vue économique, une donnée est considérée comme un bien non rival, c'est-à-dire qu'elle peut être utilisée par plusieurs personnes simultanément ou non, contrairement à un bien rival dont la consommation par une personne empêche la consommation par une autre personne (en raison des phénomènes d'unicité et de rareté cryptographique). Cette

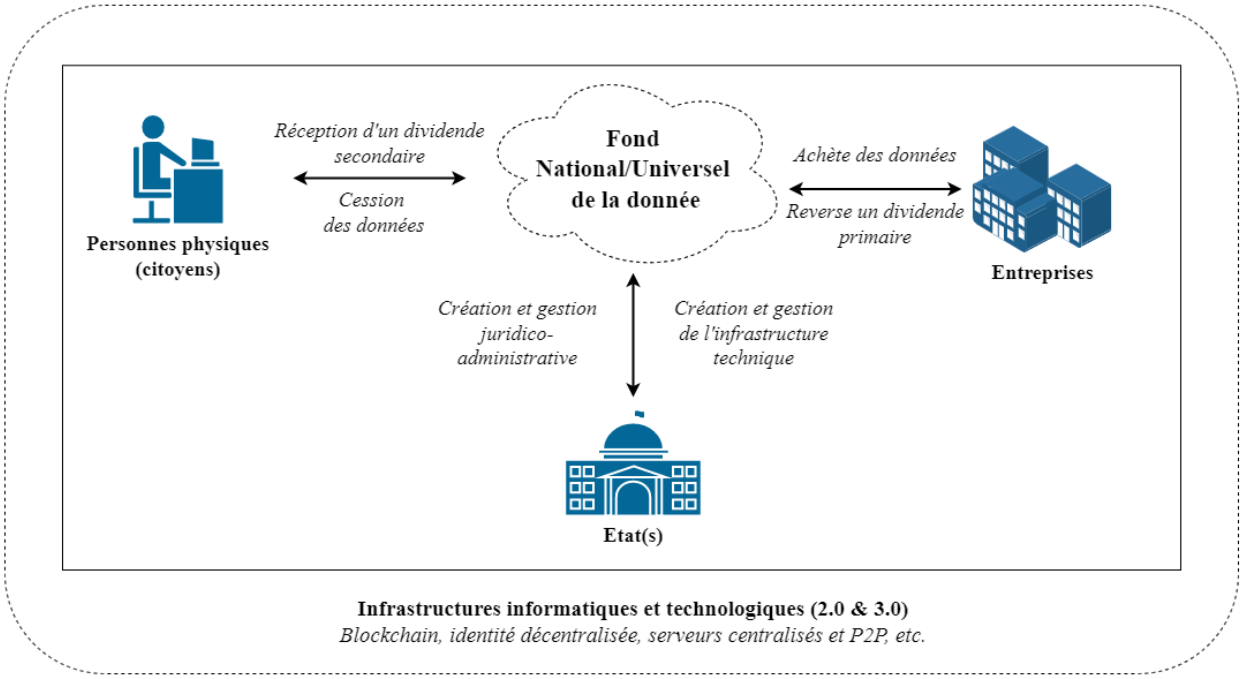
[1203] « Annales des Mines N°18 sur les Enjeux Numériques : Propriété et gouvernance du numérique », *op. cit.*, pp.30-31.
[1204] *Ibid*. p.32.
[1205] Pour rappel, la centralisation informatique de données auprès d'une ou de quelques entités identifiées peut avoir pour effet et tendance d'attirer la convoitise des pirates informatiques dont la recherche de bénéfices mal acquis peut être facilité, ce qui conforte l'utilisation de systèmes informatiques réellement décentralisés et résilients.

permettront pour la première fois que la consommation d'une donnée par un service en ligne soit exclusive, un concept qui jusqu'à présent était peu efficace avec l'identité numérique 2.0.	caractéristique s'explique par la possibilité de dupliquer les données sur Internet comme précédemment étudié[1206].
La patrimonialisation représente le prolongement du droit à l'auto-détermination informationnelle que nous avons exposé et elle contribuerait à le renforcer, voire à l'instituer. A cet égard, en Chine et en Russie, les données sont souvent considérées comme un bien commun, appartenant à la collectivité (*v*. ci-après). Cette approche vise à prévenir les scandales liés aux violations de données personnelles en adoptant une perspective plus collective pour la gestion de ces données, en termes de portée et/ou d'étendue.	Reconnaître un droit de propriété sur les données personnelles contrevient au principe d'indisponibilité de l'identité civile des personnes[1207]. En effet, accorder aux personnes un droit de propriété sur leurs données à caractère personnel reviendrait à leur conférer une disponibilité sur leurs données et par extension leur identité numérique, alors que ces données ne devraient en principe pas faire l'objet d'une disponibilité, notamment pour éviter toute tentative de patrimonialisation à leur insu (commercialisation non consentie, usurpation d'identité, manipulation).
	En France, le droit de propriété est applicable aux objets meubles ou immeubles, ce qui pose une difficulté lorsque l'objet en question est une donnée, par nature fluide et non statique. En effet, l'état en constante évolution de cette donnée peut nécessiter simultanément ou non l'application de divers régimes juridiques, en fonction du contexte d'utilisation (financier, professionnel, personnel), ce qui rend sa protection juridique complexe. Par exemple, selon l'association francophone des autorités de protection des données personnelles (AFAPDP), fondée en 2007, les données personnelles font partie intégrante de l'individu et leurs droits sont inaliénables, ce qui signifie qu'elles ne peuvent être vendues ou cédées à des tiers[1208]. Les données personnelles sont à cet égard indissociables de la personne concernée et ne peuvent pas être séparées pour être transférées à une tierce partie.

En 2019, la Professeure de droit privé Valérie-Laure Benabou de l'Université de Versailles Saint-Quentin-en-Yvelines (Paris-Saclay) a proposé une solution alternative de patrimonialisation appelée « *patrimonialisation hybride* »[1209]. Cette solution implique la création d'un fonds national public pour certaines données personnelles des citoyens. La gestion et la propriété intellectuelle de ce fond constitueraient un bien commun numérique national. Cette approche collective, plutôt qu'individuelle, de la patrimonialisation des données, reconnaît le caractère patrimonial des données tout en proposant

[1206] V, *supra*, I, Titre 1, 2.3.1
[1207] V. *supra*, I, Titre 1, 1.1.3
[1208] Vienumerique.ch, « Digital Integrity of the human person: A new fundamental right », 2020, [Diapositives], consulté en ligne le 15/01/2022, « Les données personnelles sont des éléments constitutifs de la personne. Les droits sur les données personnelles sont inaliénables, et ne peuvent être vendus. », p.9.
[1209] Propos issus de la conférence de l'AFDIT tenue en présentiel le 6 décembre 2019 à Marseille.

un cadre commun qui transcende les intérêts individuels. L'État serait le garant de ce fond commun numérique et informationnel, qui prévoirait la mise en place d'un « *dividende sur la donnée* » prélevée par l'État en contrepartie de la vente de certaines données issues du fond à des services en ligne. Remarquons que le Data Act[1210], dont l'entrée en vigueur est prévue en septembre 2023[1211], définit la notion « *d'altruisme en matière de données* »[1212], ce qui correspond au principe de ce fond universel de la donnée. Ce dernier pourrait être utilisé pour instaurer un dividende primaire au bénéfice de l'État, reversé ensuite à des causes sociales et environnementales, ainsi qu'un dividende secondaire au bénéfice exclusif et libre des personnes dont les données ont été utilisées. Cependant, aucune précision n'a été apportée quant à la nature des données incluses dans ce fond. Avec une telle proposition permettant une première forme de droit de propriété sur ces données, il serait possible de répondre aux intérêts de toutes les parties impliquées : les gouvernements pourraient prélever des taxes, les services en ligne pourraient tirer des bénéfices, et les citoyens/consommateurs pourraient obtenir une compensation pour l'utilisation de certaines de leurs données. Pour faciliter la mise en œuvre de ce droit, l'utilisation des technologies 3.0 pourrait être avantageuse, car elle favoriserait l'identification et la traçabilité des données concernées, réduisant ainsi tout manque de transparence. L'illustration suivante propose un résumé non exhaustif des éléments mentionnés, c'est-à-dire du fonctionnement global qu'un tel fond universel ou national sur les données personnelles pourrait impliquer :



[1210] V. *supra*, I, Titre 1, 2.2.1
[1211] CNIL, « European strategy for data: the CNIL and its counterparts comment on the Data Governance Act and the Data Act », 2022, disponible à l'adresse suivante
[1212] Art. 2 considérant (16) du Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le Règlement (UE) 2018/1724 (Règlement sur la gouvernance des données).

Il est important de rappeler que l'identité numérique auto-souveraine (INAS) permet de stocker les données personnelles des utilisateurs uniquement sur leur propre matériel (téléphones, ordinateurs), et de ne partager que des preuves d'informations de manière sélective. En outre, d'autres normes et applications 2.0 et 3.0 telles que les serveurs P2P, des blockchains toutes catégories confondues, des DAO ou encore des preuves à divulgation nulle de connaissance (ZKP)[1213] étudiés dans la partie suivante, constituent des outils et des bases appropriés pour mettre en œuvre l'illustration précédente. Il est possible d'établir une économie vertueuse en adoptant le modèle de la société coopérative d'intérêt collectif (mentionné dans la partie dédiée à Kleros)[1214], qui profiterait à toutes les parties prenantes en termes de gouvernance (droit de vote), qu'elles soient des personnes physiques ou morales. Cependant, pour que ce modèle soit efficace, il est nécessaire que le fonds national de données soit partiellement décentralisé, ce qui pourrait ne pas être accepté par l'Etat en raison de sa prérogative régalienne en la matière ou encore des difficultés politiques étudiées tout au long de cette recherche. Néanmoins, il semble que l'Etat doit rester le garant d'un tel système, en avoir un contrôle partiel, mais surtout totalement transparent. Cela impliquerait probablement l'utilisation de systèmes d'identités distribuées, voire d'identités numériques auto-souveraines (INAS), afin que les utilisateurs puissent volontairement alimenter le fonds avec leurs données. Finalement, en considérant une reconnaissance partielle d'un droit de propriété sur les données, il semble préférable d'adopter un régime juridique nuancé plutôt que de se contenter d'appliquer le régime juridique du droit de propriété classique aux données personnelles. Il convient de distinguer les cas d'usage et les types de données, notamment dans les cas de données de santé, biométriques ou politiques, pour lesquelles une propriété sur les données ne peut être applicable sans précaution. Finalement, la patrimonialisation des données pourrait contredire plusieurs grands principes d'Internet, telle que la libre circulation des données publiques, et faire passer les données personnelles d'un stade collectif et public à un stade strictement privé et subjectif. Il ne semble donc pas nécessaire de patrimonialiser les données en les considérant comme des biens pouvant être achetés ou vendus. Les données personnelles sont simplement des informations sur une personne et ne peuvent être considérées comme un bien au même titre qu'un objet physique. Il est donc plus important de veiller à ce que les données personnelles soient protégées par des lois et des règlementations adéquates plutôt que de chercher à les patrimonialiser à tout prix. Si une extension du droit de propriété aux données est envisagée, elle devrait à tout le moins être accompagnée de technologies sûres et fiables telles que l'IND, le ZKP et la technologie blockchain (probablement privée ou hybride). De plus, cette extension ne devrait être possible qu'à condition que les citoyens et internautes donnent leur consentement libre et éclairé et que la révocation des attributs d'identité soit possible à tout moment par l'intéressé. En somme, si une telle volonté de patrimonialisation des données était envisagée à l'avenir, elle devrait respecter ces conditions pour être justifiable et mener, tout au plus, vers le type de concept résumé schématiquement dans cette partie.

[1213] V. *infra*, II, Titre 1, 2.2.6.1
[1214] V. *supra*, I, Titre 2, 2.7.2

2.2.6.1 Le ZKP comme nouvel outil de référence au service de la protection des données

En juin 2022, le laboratoire de la CNIL a annoncé la mise à disposition d'un démonstrateur en code source ouvert qui utilise une nouvelle méthode cryptographique appelée la « *preuve à divulgation nulle de connaissance* » (« *Zero Knowledge Proof – ZKP* »), un acronyme que nous privilégions dans cette recherche[1215]. Dans ce contexte, le ZKP est un concept algorithmique qui permet à un titulaire de prouver à un tiers (vérificateur) que l'une de ses preuves – de données - est authentique sans pour autant révéler d'autres informations que celles nécessaires pour prouver l'authenticité de ladite preuve. En d'autres termes, le ZKP permet à un utilisateur de valider une transaction sans divulguer son identité ou par exemple les montants de crypto-actifs envoyés à un autre utilisateur. Pour le secteur de l'identité numérique, le ZKP peut ainsi permettre de s'assurer par la cryptographie qu'une personne est majeure, sans que le contrôleur (un officier de police judiciaire, un restaurateur, un vigile) ne connaisse l'âge exact – ou d'autres informations non essentielles - de la personne contrôlée. Le vérifieur sait simplement que la personne a plus de 18 ans, ce qui représente une information suffisante pour que le contrôle s'effectue en toute conformité. Cette technologie permet ainsi de respecter de façon inédite la vie privée de l'utilisateur en minimisant les données transmises aux fournisseurs d'identité et aux services en ligne. Selon la société Gartner, la technologie ZKP est dans une phase d'innovation et devrait atteindre un « *plateau de productivité* » dans les 2 à 5 prochaines années[1216]. La première mise en œuvre pratique de ce concept technologique prend racine avec la blockchain « *zCash* » qui a été lancée fin 2016 en utilisant une variante du ZKP appelé « zkSNARK ». Ce(s) protocole(s) et concept technologique permet de générer plusieurs preuves stockées indéfiniment sur une blockchain, sans que chacune d'entre elles ait besoin d'interagir avec le vérificateur, ce qui permet une vérification pair à pair (P2P), respectueuses des données personnelles, par plusieurs parties tierces. D'autres protocoles et blockchains, telles que Hyperledger (« ZKAT ») ou Ethereum[1217] développent des concepts similaires de confidentialité cryptographiquement programmée. A l'avenir, ces briques cryptographiques 3.0 pourraient être implémentées sur la blockchain Bitcoin, notamment grâce à certains de ses nouveaux protocoles sous-jacents comme « *Lightning Network* » et le protocole « *Taro* »[1218] étudiés dans l'Annexe 6 (Focus 4). Pour rappel, de nombreux fournisseurs d'identité collectent plus d'informations qu'ils n'en ont besoin pour vérifier l'identité d'un individu. Cette collecte massive d'informations, souvent à des fins commerciales plutôt que d'identification entrave la mise en pratique du principe de minimisation des données collectées. L'implémentation du ZKP offre une solution structurelle à cette problématique en permettant de fournir des preuves irréfutables sans divulguer leur contenu. Cette méthode cryptographique représente un outil technique innovant pour respecter le principe de minimisation des données personnelles dictée par le RGPD, mais renforce aussi la possibilité d'un pseudo-anonymat par

[1215] GORIN Jérôme, BIERI Martin, BROCAS Côme, « Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée », 2022, in *linc.cnil.fr*, consulté le 22 juin 2022, à l'adresse suivante
[1216] V. Annexe 9.
[1217] V. Annexe 6, Focus 2.
[1218] V. Annexe 3, Focus 4.

conception en ligne. En outre, le ZKP peut s'appliquer dans de nombreux domaines, tels que la preuve de diplômes[1219], d'expériences, de formations, d'actes juridiques, entre autres. Le ZKP permettrait aux organisations publiques ou privées de prouver leur conformité règlementaire sans divulguer d'informations confidentielles[1220], conformément au secret des affaires et des correspondances privées déjà étudiés. Grâce au concept et aux divers protocoles ZKP qui se développent, de nombreuses blockchains publiques, privées ou hybrides pourraient se conformer aux règlementations eIDAS, RGPD, MiCA ou TFR précédemment mentionnées, sous réserve que leurs protocoles respectifs le permettent, c'est-à-dire en développant des capacités informatiques supplémentaires (protocoles de seconde couche ou Layer 2)[1221]. Finalement, le ZKP couplé à une identité numérique décentralisée forme un alliage puissant au service d'un Web plus respectueux des données. L'implémentation du ZKP devrait ainsi être soutenue pour plus de solution d'IND afin de garantir un chiffrement ainsi qu'une protection optimale des personnes physiques et morales dans les écosystèmes numériques 2.0 et 3.0.

2.2.7 Le potentiel social et le défi informatique du vote décentralisé

Le droit de vote est essentiel à toute démocratie, car il garantit la liberté d'expression des citoyens au sein d'un État de droit. En plus d'être un moyen d'expression et de gouvernance pour les citoyens, le droit de vote symbolise un contre-pouvoir face à l'ordre politique établi. Bien que son rôle soit crucial, sa mise en place est complexe pour assurer une représentation démocratique des attentes de la société[1222]. Le vote semble ainsi être un outil au service de l'expression des personnes, et non pas le gage ni l'assurance d'une démocratie pure. Avec l'essor des réseaux de communication en ligne, les méthodes et formes de vote s'élargissent considérablement au bénéfice des institutions et des citoyens. Aujourd'hui, chaque personne peut exprimer son opinion sur d'innombrables sujets et dans de nombreux contextes au caractère plus ou moins significatifs et officiel pour la société (votes professionnels, vote pour une élection, votes sur des réseaux sociaux). Ces nombreux contextes d'expression numérique faisant appel au vote des internautes rendent aujourd'hui complexe (i) l'identification et l'authentification élevée des utilisateurs lors d'un processus de vote en ligne, et (ii) l'authenticité (intégrité, durabilité) des votes exprimés. Ainsi, tous les votes en ligne ne nécessitent pas un degré

[1219] Wikipédia, v. société BCdiploma, 2023, disponible à l'adresse suivante
[1220] Plus spécifiquement, certaines blockchains publiques (*Monero*, *Zcash*) utilisent d'ores et déjà ces procédés cryptographiques avancés de *ZKP*. Ils permettent des transactions en crypto-actifs dans lesquelles les clés publiques des participants ainsi que les détails de la transaction sont cachés de la vue du public. Si ces blockchains sont potentiellement plus en phase avec le RGPD (puisqu'il n'y a plus aucune donnée personnelle visible), elles posent toutefois un problème majeur aux autorités en charge de la lutte contre le blanchiment de capitaux et le financement du terrorisme. L'avenir semble donc aux mains des blockchains capables de concilier les impératifs suivants : respect de la vie privée de leurs utilisateurs et conformité aux règles de droit.
[1221] Ces systèmes de secondes couches peuvent être directement (« *Layer 2* ») ou indirectement (« *Sidechain* ») rattachés à la blockchain et au protocole principal, selon des modalités informatiques plus ou moins similaires et complexes. En d'autres termes, un *Layer 2* repose sur la sécurité d'un réseau blockchain déjà existant, tandis qu'une *Sidechain* repose sur son propre modèle de sécurité informatique.
[1222] MAALOUF Amin, « Les identités meurtrières », *op. cit.*, « un vote ne fait que refléter la vision qu'une société a d'elle-même, et de ses diverses composantes. Il peut aider à faire le diagnostic, mais il n'apporte jamais à lui seul le remède. », p.180.

d'expression et de fiabilité similaire. A l'heure actuelle, il est admis que deux types de vote électronique coexistent :

a. Le vote mixte en présentiel, mais avec des ordinateurs à voter ou « *machine à voter* »[1223]. Ces ordinateurs spéciaux[1224] équipent certains bureaux de vote en France. Ces bureaux de vote ne nécessitent plus d'isoloirs ni d'urne pour procéder aux votes des citoyens, qui n'ont d'autres choix que de voter sur ces machines qui enregistrent et numérisent tous les résultats des votants. Cette solution demeure à ce jour très limitée en raison d'une logistique complexe pour les collectivités et d'une accessibilité réduite et contraignante pour les votants.

b. Le vote numérique à distance, c'est-à-dire par correspondance numérique, qui est particulièrement efficace pour lutter contre l'absentéisme de l'électorat (tout particulièrement lors de la crise de la Covid-19). Si ce type de vote n'est à ce jour possible et en vigueur que pour les députés français à l'étranger[1225], ces votes possèdent souvent un caractère national et officiel et ils sont directement liés à l'identité civile des votants. Dans d'autres cadres (professionnel, universitaire, loisir), les personnes procèdent à des votes à faible impact juridique, mais parfois à forte valeur ajoutée personnelle. Ainsi, ces votes de niveau faible s'effectuent par diverses plateformes 2.0 plus ou moins fiables, crédibles ou officielles. Ces plateformes recueillent généralement des données personnelles sur leurs utilisateurs et pour des motifs plus ou moins légitimes (en principe pour permettre d'améliorer leur fonctionnement, parfois avec quelques dérives). Pour illustration, si les solutions actuelles permettent la pseudo-anonymisation des données des utilisateurs, il est bien souvent impossible pour ces plateformes d'apporter la preuve à leurs utilisateurs que leurs données sont bien pseudo-anonymisées. En effet, le vote d'un utilisateur pourrait être dévoilé à des tiers via un virus hébergé sur l'ordinateur de l'électeur ou bien directement sur la plateforme, et sans même que l'hébergeur du vote ou encore l'utilisateur en ait la connaissance. Dans un tel cas, le vote est biaisé et nul, il doit être réalisé à nouveau (en partant du postulat que l'intrusion informatique est identifiée et non pas latente).

Par conséquent, le vote en ligne 2.0 est associé à la problématique de la confiance numérique déjà évoquée précédemment. La confiance 2.0 qui est accordée à ces plateformes semble en effet juridique plus que cryptographique, car la plateforme peut prouver sa solidité informatique via un soutien étatique

[1223] Article L57-1 du Code Electoral, disponible à l'adresse suivante
[1224] Ces ordinateurs de vote sont un modèle agréé par le ministère de l'Intérieur, autorisé par l'Arrêté du 17 novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter.
[1225] Service Public, « Vote d'un Français installé à l'étranger », 2022, in *servicespublic.fr*, consulté le 01/02/2022.

et institutionnel (garantie, certifications)[1226], mais elle ne peut pas directement prouver sa solidité cryptographique auprès des utilisateurs alors que le Web 3.0 et le ZKP le permettent désormais. Toutefois, comment avoir la certitude qu'un vote est informatiquement valide et qu'il émane bien de la volonté et de l'identité civile du votant ? Si ces problématiques sont assez limitées pour les votes de faible valeur comme nous l'avons constaté (car ils ne nécessitent pas l'identité civile du votant), elles demeurent essentielles pour les votes officiels qui fondent notre démocratie et Etat de droit. Les citoyens et les internautes sont en faveur de la mise en place de nouveaux systèmes de vote en ligne via des sites internet officiels et des systèmes d'identification et d'authentification peu complexes. Cependant, il semble que ces systèmes 2.0 font face à de nombreux défis techniques qui ne peuvent être résolus qu'avec l'ajout d'autres briques technologiques 3.0 comme la technologie blockchain et l'identité décentralisée. Il est donc important d'encourager les expérimentations avec ces types de solutions pour garantir aux votants que leurs votes et droits sont sécurisés, tout comme un vote traditionnel dans une urne physique. Les citoyens souhaitent progressivement s'engager activement dans une démocratie numérique en raison de l'évolution de nos comportements en termes de débats, d'expression, d'information et d'interaction avec les gouvernements et ses institutions. En 2019, une délibération en 2019 de la CNIL estime que « *devant l'extension continue du vote par Internet à tous types d'élections, la commission souhaite rappeler que le vote* (…) *via Internet, présente des difficultés accrues* (…) *pour les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement, principalement à cause de l'opacité et de la technicité importante des solutions mise en œuvre, ainsi que de la très grande difficulté de s'assurer de l'identité et de la liberté de choix de la personne effectuant les opérations de vote à distance.* »[1227]. Les problèmes mentionnés peuvent être partiellement résolus en utilisant la technologie blockchain pour augmenter la transparence de l'outil numérique ainsi que du processus de vote, tout en utilisant l'identité décentralisée pour résoudre les problèmes d'identification et de consentement. Une solution basée sur la technologie blockchain et l'identité décentralisée réduirait au minimum l'utilisation de données personnelles des votants en utilisant le ZKP mentionné dans la partie précédente. En d'autres termes, seuls les horodatages de vote seraient enregistrés sur une blockchain (publique, hybride ou privée), tandis que le contenu du vote pourrait être stocké temporairement sur des serveurs distribués ou centralisés, certifiés par des institutions de confiance. En 2022, une entreprise française spécialisée dans les services de vote en ligne basés sur la technologie blockchain a reçu une certification de la CNIL, ce qui représente une avancée en Europe[1228]. Par ailleurs, il convient de se demander si la possibilité d'un vote décentralisé contribue à l'émergence mentionnée d'une identité universelle. A cet égard, un système de vote décentralisé semble directement et

[1226] Sénat, « Le vote à distance, à quelles conditions ? », Rapport d'information n°240 déposé le 16 décembre 2020, disponible à l'adresse suivante
[1227] Délibération n°2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (2019). Légifrance, consulté en ligne le 01/02/2022.
[1228] VASSEUR Victor, « Pour la première fois, un système de vote en ligne basé sur la blockchain est validé par la CNIL », France Inter, 2022, consulté le 3 juin 2022, à l'adresse suivante

informatiquement lié à la création d'une identité numérique universelle, bien qu'il s'agisse de deux concepts différents. Un vote décentralisé permet a priori de garantir l'intégrité du processus de vote en éliminant les risques de falsification des résultats, en permettant à chaque votant de vérifier que son vote a été comptabilisé correctement et en protégeant la confidentialité des données des votants. Cela peut être réalisé grâce à des technologies telles que la blockchain qui permettent d'enregistrer de manière immuable les votes et de garantir leur traçabilité comme mentionné. En revanche, une identité universelle est un concept plus large qui vise à fournir une identité numérique à tous les individus, indépendamment de leur nationalité ou de leur lieu de résidence. Il semble qu'une technologie de vote décentralisée, comme la blockchain, pourrait être utilisée pour soutenir la création d'une identité universelle en fournissant une plateforme sécurisée et fiable pour stocker les informations d'identité des utilisateurs. Toutefois, une telle approche nécessiterait des développements supplémentaires d'ores et déjà abordés par le projet Proof of Humanity[1229].

2.2.8 L'État fournisseur d'identités 3.0 : entre souveraineté et autonomie des individus

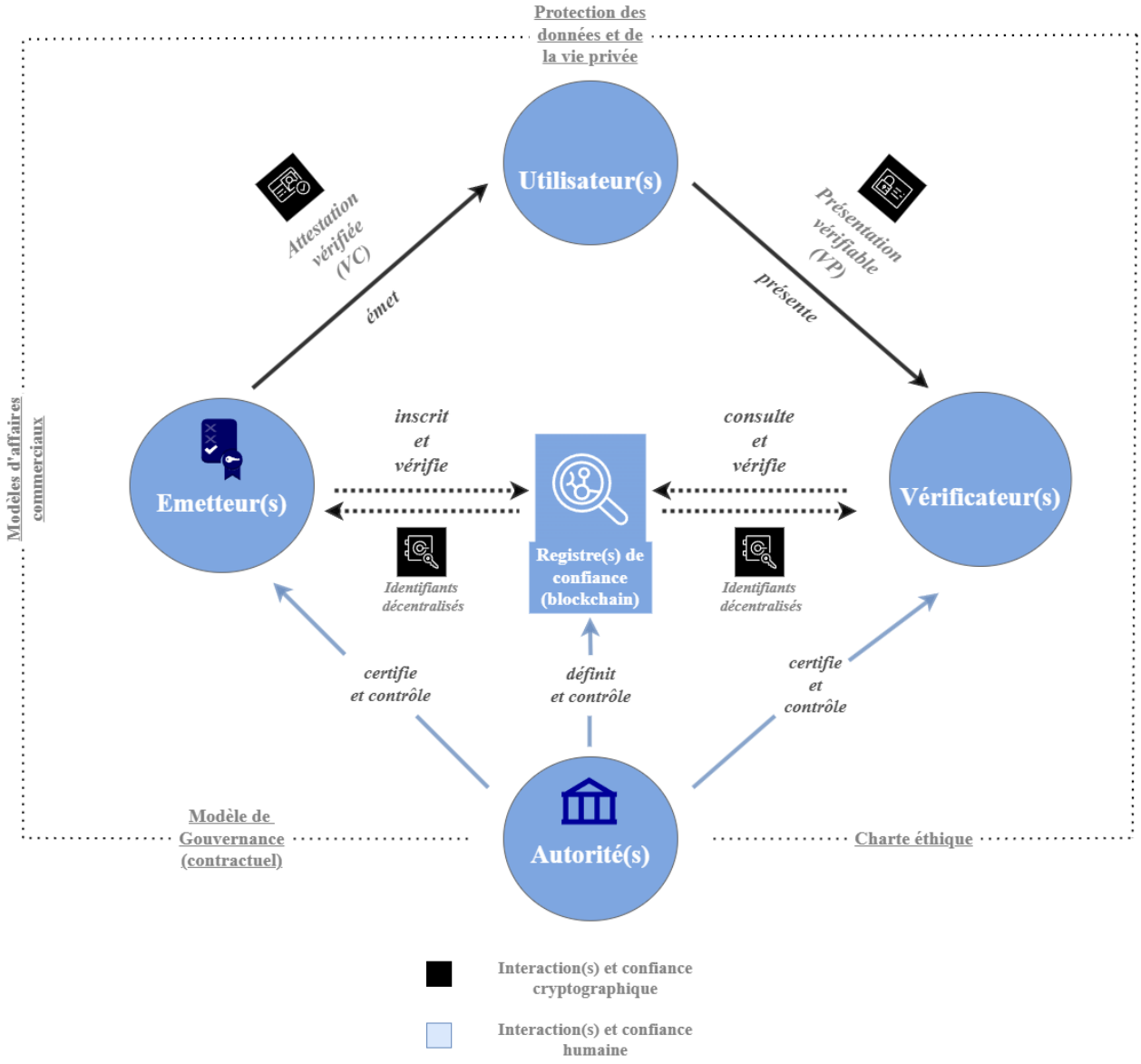
Le concept de l'État fournisseur d'attributs et de solutions 3.0 décrit dans cette partie une évolution des relations et des services numériques entre l'État et ses citoyens. Pour rappel, en tant que fournisseur historique d'attributs physiques et désormais numériques, l'État s'engage à fournir à chaque citoyen un ensemble d'identités numériques sécurisées pour accéder à de multiples services en ligne. Cette approche permet de concilier la souveraineté de l'État et l'autonomie des individus, en leur offrant un contrôle accru sur leurs informations personnelles et leurs droits, tout en garantissant la sécurité des transactions en ligne. En résumé, la puissance publique fournisseuse d'attributs 3.0 équilibre les besoins de l'État en termes de sécurité informatique et les droits des individus qui doivent être protégés en ligne. La confiance dans les solutions d'identité numérique est d'une importance primordiale, comme cela a été souligné auparavant. Un exemple classique de perte de confiance envers une institution publique et étatique est illustré par le Bureau de Poste britannique (« Royal Mail ») en 1999, lorsqu'il a introduit le système de gestion comptable « *Horizon* » dans plusieurs de ses filiales. Des écarts et des pertes comptables inexpliqués ont alors été signalés par des administrateurs et des postiers du réseau, mais le Royal Mail n'a pas pris en compte ces rapports d'incident et a maintenu que son système Horizon était fiable et qu'aucun des écarts comptables des succursales n'étaient dus à des problèmes de dysfonctionnement[1230]. Ces bogues informatiques, ont entraîné la poursuite de 918 salariés du Bureau de Poste britannique pour vol, fausse comptabilité et/ou fraude entre 1991 et 2015, sur la base de preuves informatiques uniquement et sans aucune tentative de prouver une intention frauduleuse. Ces poursuites

[1229] V. *supra*, I, Titre 2, 2.9
[1230] « Judgment (No.3) 'Common Issues' (Bates & Ors v Post Office Ltd) », The Post Office Group litigation in the High Court of Justice queens bench division, Case No: HQ16X01238, 2019, in *Judiciary.uk*., p.312.

ont causé de nombreux préjudices pour certains salariés, tels que des pertes d'emplois, des faillites personnelles, des divorces, des peines de prison injustifiées et même un cas de suicide avéré[1231]. Ce cas extrême démontre les conséquences réelles que des systèmes informatiques peuvent engendrer sur des personnes physiques, et le risque qu'il peut faire peser sur ces derniers. Afin d'éviter la répétition d'événements similaires, y compris avec l'utilisation de solutions 3.0, le recours à des modèles d'identité numérique distribuée et hybride semble essentiel comme le représente le schéma suivant. Ce dernier propose une solution partiellement décentralisée grâce à l'utilisation d'un registre de confiance au centre du système. En plus des interactions avec les attributs cryptographiques décrits précédemment (DID, VC, VP), ce schéma intègre également une dimension légale, incluant une ou plusieurs autorités

[1231] SINCLAIR Leah, « Post Office worker took his own life after being wrongly accused of stealing £60K », 2021, in *Yahoo News*, disponible à l'adresse suivante

reconnues qui ont pour rôle de superviser et de certifier, tant contractuellement qu'éthiquement[1232], la gouvernance d'un tel système gouvernemental semi-décentralisé.



En principe, un Etat de droit est au service de ses citoyens, c'est-à-dire de la société dans laquelle il s'inscrit et en fonction du système politique, juridique et social qui lui est propre. Pour qu'une puissance publique puisse fournir une identité numérique pérenne, il se doit de récolter de nombreuses données sur ses citoyens afin d'assurer une continuité dans les services publics et l'accompagnement social qu'il délivre (imposition, services aux personnes, etc.). Toutefois, force est de constater que les données récoltées par l'Etat le sont en silos, c'est-à-dire centralisées au sein de multiples institutions publiques, départements ou divisions, notamment pour des raisons historiques et/ou politiques. La croissance du

[1232] V. *infra*, II, Titre 1, 1.1

besoin d'interconnectivité que suscite notre société numérique tend ainsi à connecter ce fonctionnement en silo autrefois efficace, mais aujourd'hui relativement dépassé au regard des technologies et des besoins actuels de rapidité de la circulation des informations. La blockchain et l'identité décentralisée pourraient répondre aux enjeux de connectivité rapide et sécurisée d'une nation, comme le démontre la proposition d'amendement du Règlement eIDAS-2 étudiée en amont[1233]. Son objectif est ainsi de créer un environnement dans lequel les données peuvent facilement être partagées entre les systèmes informatiques et au sein duquel les individus et les organisations peuvent reprendre le contrôle sur leurs données, tout en assurant leurs traçabilités de bout en bout lors de leur partage (depuis les institutions jusqu'aux citoyens). Se pose ainsi la question de savoir comment l'État et la puissance publique se positionne face à la possibilité d'une libéralisation de l'identité numérique des personnes (identité numérique auto-souveraine - INAS).

Sur un plan historique et politique, l'identité (numérique) demeure une prérogative et un devoir régalien, encadrée par le droit. Ce pouvoir régalien confie le rôle à l'Etat de fournisseur d'identité civile à ses citoyens, comme nous l'avons évoqué. A ce propos, il semble que les titres d'identité officiels (CNIe, passeports) ne sont probablement pas voués à disparaître, mais plutôt à être progressivement enrichis avec de nouvelles capacités numérique (3.0 voire 4.0) comme cette recherche le suppose. Face à l'émergence de nouvelles formes d'identité numérique 3.0, il revient d'ores et déjà à la puissance publique de définir et de dessiner les contours du concept d'identité numérique distribuée (IND). Il s'agit de fixer le contexte et les finalités d'utilisation de ces nouveaux mécanismes d'identité numérique, c'est-à-dire de proposer de nouvelles règles juridiques pour régir ces nouveaux écosystèmes pleins de promesses et les guider vers une implémentation aussi innovante que vertueuse pour les personnes et leurs droits numériques mentionnés. Il est souligné qu'en 2021, le ministère de l'Intérieur a publié un rapport d'information sur le sujet de l'identité numérique décentralisée[1234], un premier support politique essentiel à la diffusion de connaissances auprès des institutions publiques autant que du grand public ou des entreprises. L'essence d'un Etat réside en principe dans la promotion du bien commun, notamment en favorisant l'accès aux services publics, en garantissant l'égalité de traitement et en respectant les libertés individuelles. Toutefois, les pouvoirs conférés démocratiquement à l'Etat ne doivent normalement pas outrepasser l'intérêt général, à l'exception des cas prévus par la loi tels que la lutte contre le terrorisme ou le blanchiment de capitaux. Lorsqu'un fournisseur de services accepte une identité numérique délivrée par une institution publique, il adhère aux valeurs de l'ordre juridique et politique de l'Etat qui la délivre. Par conséquent, la puissance publique et en amont le législateur, interviennent à différents niveaux en fonction des solutions d'identité numérique en question. Ils définissent les accréditations et les critères nécessaires pour fournir une identité numérique de confiance, qui est ensuite délivrée par des fournisseurs d'identité publics ou privés également de confiance. L'idéal

[1233] V. *supra* II, Titre 1, 2.1.1.1.a
[1234] *Op. cit.*, FAHER Mourad, et al., « Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité' », 2021.

serait de s'assurer que chaque texte législatif encourage l'innovation sans la freiner structurellement d'un point de vue informatique et social. Si la décentralisation informatique n'est pas un concept particulièrement attrayant pour le législateur et plus particulièrement pour la puissance publique, notamment en raison de l'essor de la décentralisation de la blockchain Bitcoin[1235], il est pourtant considéré dans cette étude que la décentralisation informatique est bénéfique en termes de résilience numérique (aux cyberattaques) et de transparence institutionnelle (contractualisation automatisée, vote décentralisé). Toutefois, il est suggéré que si le gouvernement prend un jour la décision d'implémenter une blockchain, celle-ci sera très probablement fermée et fondée sur une infrastructure similaire à celle développée en Estonie[1236]. L'objectif de l'identité décentralisée ne devrait pas être la mise en place d'un nouveau système de surveillance généralisée des populations, mais plutôt garantir à chaque individu « *le droit d'être soi* »[1237]. Bien que les gouvernements puissent fournir des portefeuilles d'identité numérique décentralisée (PIND), il est peu probable qu'ils encouragent à court et moyen termes l'émergence d'identités auto-souveraines, où les attributs d'identité racine sont émis directement par l'individu concerné. En d'autres termes, un citoyen n'émettra jamais sa propre CNI[1238]. Les gouvernements continueront probablement à être les émetteurs d'identités fondatrices et détiendront le pouvoir de révoquer des titres de compétences selon les lois en vigueur sur son territoire. Les internautes bénéficient toutefois d'une certaine marge de liberté en ligne. Par ailleurs, la financiarisation des attributs d'identité numérique racine n'est pas souhaitable pour les gouvernements, car ils n'ont généralement pas d'intérêts commerciaux à cet égard.

Un État a pour devoir d'assurer la liberté des personnes relative à leur identité numérique (avec des nuances selon les situations d'identification), c'est-à-dire de relier chaque attribut d'identité à un droit et de garantir la fiabilité d'une attestation vérifiable lorsqu'elle est associée à un ou plusieurs documents d'identité officiels. Ces trois éléments sont essentiels pour maintenir un lien entre l'État de droit et la vie quotidienne des citoyens, comme le souligne Maître Alain Bensoussan, avocat au Barreau de Paris : « *cette même commission* [CNUDCI] *a conclu que, s'agissant de l'identité numérique, aucun État ne devra en posséder le monopole, laissant ainsi au marché le choix et la compétition dans les offres de service.* »[1239]. Il est primordial que le droit ne soit pas uniquement au service d'une informatique et d'une cryptographie centralisée et contrôlée par l'État, mais que le secteur privé puisse également proposer des solutions plus innovantes, légalement encadrées et transparentes. L'utilisation de la technologie blockchain et de l'identité décentralisée pourrait permettre aux Etats de réduire certaines de leurs

[1235] V. Annexe 3, Focus 2 et 5.
[1236] V, *supra*, I, Titre 1, 2.2.2.1.c
[1237] « The Right to be You », slogan officiel de la société IN Groupe (ancienne Imprimerie Nationale), disponible sur le site internet suivant. Appliqué aux concepts soutenus dans cette thèse, ce slogan serait tel que : « le droit [cryptographique] d'être soi ».
[1238] Toutefois, si les Métavers tiennent leurs promesses, il est fortement probable que *l'identité auto-souveraine* (INAS) y trouvent une place toute particulière en permettant à ses internautes et communauté d'auto-attester certains de leurs attributs d'identité (secondaires ou étendus et non pas primaires et racines).
[1239] BENSOUSSAN Alain, « L'identité numérique 5.0 », *op. cit.* p.46.

dépenses relatives à l'accès à certains de leurs services publics. En effet, le temps et le coût administratif nécessaires pour effectuer certaines démarches sont parfois trop importants pour les citoyens de certains pays, comme l'explique un rapport de la société McKinsey[1240]. Certains Etats comme le Delaware[1241] sont en avance et expérimentent depuis 2017 des briques technologiques tels que des contrats intelligents ou encore des plateformes blockchains hybrides afin d'enregistrer et de vérifier plus efficacement certaines données essentielles liées aux registres des entreprises[1242]. Fort de ces propos, l'Etat et ses institutions semblent progressivement se transformer en un « *Etat-plateforme* »[1243] centralisé dans de nombreux pays occidentaux. Une décentralisation partielle pourrait lui être bénéfique. Partiellement distribué, il émettrait des attributs d'identité certifiés via des blockchains privées ou hybrides. Ce nouvel Etat-plateforme 2.0 et 3.0 serait ainsi personnalisé, participatif, agile et surtout respectueux des droits fondamentaux en ligne des individus. De tels systèmes contribueraient également à améliorer la transparence du fonctionnement inter-institutionnel de l'Etat en luttant contre la corruption grâce à la capacité des blockchains à retracer certains accès et administrateurs responsables des interactions numériques effectuées sur la plateforme, en cas de soupçon. En septembre 2021, la Commission européenne a adopté un nouveau cadre juridique appelé « European Digital Infrastructure Consortium - EDIC » dans le cadre de sa stratégie « Path to the Digital Decade »[1244]. Ce cadre juridique permet aux États membres de collaborer plus facilement sur des projets d'infrastructures numériques communes grâce à un véhicule juridique ad hoc doté d'une personnalité juridique. Ce dispositif facilite la mise en place de consortiums numériques, ce qui profitera directement aux institutions étatiques souhaitant partager une ou plusieurs infrastructures blockchains. Pour soumettre une demande à la Commission, un minimum de trois États membres est requis. Chaque consortium aura sa propre personnalité juridique, des statuts dédiés et son siège dans l'un des États membres participants. Cependant, la mise en place de systèmes décentralisés pose des défis juridiques, car les législations en vigueur ne sont pas toujours adaptées. Bien que cette nouvelle manière d'envisager les consortiums numériques soit bénéfique, elle ne résout pas la question de l'application de programmes hautement décentralisés et émis par des particuliers qui possèdent des compétences en informatique (blockchains publiques, minage). Pour attirer ces talents et encourager une forme de décentralisation, la puissance publique doit accepter cette volonté et ce besoin de changement par le marché. Actuellement, les projets 3.0 au sein des

[1240] CHENG Steve, DAUB Matthias, DOMEYER Axel, et al., « Using blockchain to improve data management in the public sector », 2017, in *mckinsey.com*, disponible à l'adresse suivante, traduction libre de l'anglais, « Selon notre analyse des transactions immobilières dans tous les pays de l'Organisation de coopération et de développement économiques, les acheteurs paient au moins 3,5 milliards de dollars par an en frais administratifs pour enregistrer leurs achats. Le traitement numérique pourrait réduire considérablement le coût de ce service pour les gouvernements ; en retour, les agences pourraient faire bénéficier les citoyens de ces économies. », p.3.

[1241] TINIANOW Andrea, « Delaware Blockchain Initiative : Transforming the Foundational Infrastructure of Corporate Finance », 2017, in *The Harvard Law School Forum on Corporate Governance*, consulté le 22 avril 2022, à l'adresse suivante

[1242] « Une profession réglementée, les greffiers des tribunaux de commerce déploient une solution fondée sur la blockchain destinée à améliorer la gestion du registre du commerce et des sociétés (RCS) », 2019, in *actualitesdudroit.fr*

[1243] CHEVALLIER Jacques, « Vers l'État-plateforme ? », 2019, in *Revue française d'administration publique*, n°167, pp.627-637., disponible en ligne

[1244] Council of the European Union. 16 septembre 2021. Proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme « Path to the Digital Decade », in *data.consilium.europa.eu*. Consulté le 14 octobre 2022, à l'adresse suivante

gouvernements rencontrent des difficultés, car les talents préfèrent travailler dans le secteur privé pour des raisons philosophiques ou financières. Il est nécessaire de mettre en place des cadres juridiques plus flexibles reposant sur des principes, des conditions et des chartes d'adhésion pour favoriser la décentralisation et éviter une régulation indifférenciée et inadaptée. Le collectif d'avocats à l'origine de la revue de décryptage et de révolution numérique « Third » prévient « *il reste à inventer les outils et principes qui demain permettront de dessiner, dans l'espace numérique, la voie d'une gouvernance* [3.0] *équilibrée, propre à promouvoir la liberté de tous, tout en protégeant les droits de chacun* »[1245].

2.2.8.1 Interopérabilité informatique et harmonisation conceptuelle et juridique

L'interopérabilité se réfère à la capacité de différents systèmes (sociaux, informatiques, juridiques) à communiquer ensemble de manière transparente. En informatique, cette capacité de partage d'informations permet à plusieurs systèmes de communiquer des informations et de fournir des services en ligne variés et complémentaires. Cette partie examine le concept d'interopérabilité sous l'angle des technologies 3.0 et de ses répercussions juridiques. La technologie blockchain, en raison de ses trois grandes catégories existantes déjà évoquées (publiques, privées et hybrides) doit tendre vers une interopérabilité technique afin de mutualiser et de maximiser les effets réseaux de ces variantes technologiques. Les blockchains hybrides utilisent actuellement des interfaces de programmation d'application (« *Application Programing Interface – API* »)[1246] pour assurer leur interopérabilité. Cependant, ces interfaces de communication sont souvent centralisées, ce qui signifie que seules les API liées aux blockchains publiques sont moins dépendantes de tiers externes[1247], car la validité des informations dans une blockchain publique est assurée par son protocole et ses mécanismes de consensus algorithmique[1248]. Ainsi, l'État et ses institutions préfèrent les API centralisées en raison de leur flexibilité. Dans le secteur de l'identité numérique, une grande flexibilité et adaptabilité sont effectivement requises en raison du volume important de transactions numériques traitées comme cela a été étudié précédemment. Si la plupart des débats sur l'interopérabilité sont centrés sur l'informatique, c'est-à-dire sur des aspects techniques, il existe également des aspects sémantiques et juridiques à prendre en considération. Il est possible de distinguer l'interopérabilité conceptuelle, de l'interopérabilité technique et de l'harmonisation juridique.

[1245] Collectif d'avocats THIRD, « Le numérique peut-il sauver la démocratie ? », in *Revue de Décryptage et de Révolution Numérique*, 2021.
[1246] Une *API* est un intermédiaire logiciel qui permet à deux applications distinctes de communiquer entre elles (tel un pont informatique permettant de faire traverser et communiquer des informations issues d'applications informatiques distinctes).
[1247] Dans les faits, les écosystèmes (semi-centralisés) attachés aux blockchains publiques recourent massivement aux API pour interagir avec ces protocoles publics. Ainsi, cette relative centralisation peut faire l'objet d'une censure politique ou juridique selon les situations, un constat qui se confirme progressivement depuis 2021. V. Annexe 7.
[1248] V. Annexe 6, Focus 1 à 3.

(i) L'interopérabilité informatique a pour objectif de mettre en place puis d'utiliser de normes techniques communes. Pour cela, les acteurs de la normalisation européenne (CEN-CENELEC[1249], ETSI[1250]) sont indispensables[1251] pour harmoniser et mettre en œuvre les futures briques techniques des identités numériques 3.0 de demain, notamment au regard du futur portefeuille d'identité numérique décentralisée (PIND). Plus généralement, de nombreuses institutions et comités techniques[1252] de normalisation, rattachés à l'« *International Organization for Standardization - ISO* », collaborent activement pour la mise en place de principes et normes techniques 3.0 communes.

(ii) En théorie, toute communauté a besoin d'autres communautés pour survivre, ce qui implique une harmonisation sociale. En ce qui concerne l'identité, nous avons constaté cette interdépendance nécessaire de nos identités, ne serait-ce qu'en raison du mimétisme et de l'influence de nos éducations. Chaque communauté humaine a la responsabilité d'assigner, d'enrôler et de vérifier les identités de ses membres à l'aide de registres et de mécanismes fiables et durables. Si les blockchains ne sont pas conçues pour être interopérables avec l'identité décentralisée, une interopérabilité entre les mécanismes d'identité numérique peut être assurée, car les utilisateurs n'ont pas un unique fournisseur d'identité. L'identité décentralisée offre un système théoriquement indépendant et interopérable qui peut être utilisé et mis en œuvre par toute organisation, service ou institution.

(iii) Le troisième type d'interopérabilité, également appelé harmonisation juridique, découle des deux précédents et fait référence à la capacité d'harmonisation des textes juridiques en vigueur avec ceux en cours d'adoption. Cette harmonisation doit prendre en compte le droit dans son intégralité, y compris ses jurisprudences et doctrines multiples, dont cette recherche tente de dresser un état de l'art non exhaustif. Si l'extraterritorialité du droit est considérée comme son plus grand ennemi, une interopérabilité juridique ne peut être effective que si elle résulte d'une concertation avec les acteurs de la normalisation technique mentionnés précédemment. En Europe, les Règlements eIDAS et le RGPD sont censés être des exemples en la matière. Cependant, dans la pratique, la concurrence croissante des acteurs du secteur des nouvelles technologies propose des visions et des solutions

[1249] « European Committee for Electrotechnical Standardization - CEN-CENELEC », pour plus d'informations consultez le site internet suivant
[1250] « European Telecommunications Standards Institute - ETSI », consultez le site internet suivant
[1251] Ces acteurs internationaux de la normalisation conçoivent et partagent ensemble leurs standards et normes techniques, de façon complémentaire avec d'autres travaux issus de commissions au sein d'institutions européennes (*CE, CJUE, Conseil de l'Europe, Parlement Européen*).
[1252] ISO/TC 307 « Blockchain and distributed ledger technologies », JTC19 « Blockchain and Distributed Ledger Technologies » ; comité technique du CEN/CENELEC « Building blocks for identity management on mobile devices » ; ISO/IEC JTC 1/SC 27 « Information security, cybersecurity and privacy protection », etc.

techniques parfois plus favorables à eux-mêmes qu'à leurs utilisateurs finaux, qui sont les citoyens.

En somme, l'interopérabilité est au cœur du concept d'identité numérique décentralisée (IND), qui vise à harmoniser les différents systèmes et protocoles. Les trois types d'interopérabilité, à savoir l'interopérabilité informatique (i), conceptuelle (ii) et juridique (iii), sont essentiels pour atteindre l'objectif ultime de la reconnaissance juridique. Les identifiants décentralisés et les attestations vérifiables sont des standards techniques en cours d'adoption qui témoigne de l'importance de la collaboration et de la convergence pour la mise en œuvre de toute IND. Finalement, une décentralisation ne peut être réalisée que par un effort organique et intellectuel commun, ratifié par de multiples entités socialement reconnues.

Titre 2 : Etude pratique et recommandations pour une identité juridique 3.0

Chapitre 1 : Défis et recommandations éthiques, informatiques et juridiques

1.1 Placer l'éthique numérique au cœur de l'identité numérique décentralisée

Pendant longtemps, l'informatique et l'éthique étaient considérées comme deux disciplines distinctes et sans lien évident entre elles. Pourtant, l'éthique est un élément crucial de la gouvernance algorithmique, tout comme la loi, d'après l'auteure Aurélie Jean[1253]. L'éthique permet de rendre chaque individu moralement responsable, indépendamment de sa position dans le monde technologique et social, en adoptant une attitude consciente de ses réflexions, de ses comportements et de son langage. En l'absence d'éthique, les détracteurs des nouvelles technologies peuvent facilement attirer l'attention des internautes, en propageant des rumeurs en ligne, des idéologies politiques et en pratiquant la censure. Aujourd'hui, quelques entreprises commerciales détiennent les clés de voûte de la société numérique et peuvent imposer leur vision au monde, comme le suggérait sans le savoir Étienne de la Boétie dans son discours sur la servitude volontaire au XVIè siècle[1254]. Il est donc important de contrôler les mécanismes

[1253] JEAN Aurélie, « Les algorithmes font-ils la loi ? », *op. cit.*, in *Humensis*, 2021, « L'éthique est un des piliers de la gouvernance algorithmique, au même titre que la loi. […] L'éthique permet de responsabiliser chaque individu, quelle que soit sa position sur l'échiquier technologique et social. Elle rend chacun d'entre nous meilleur à travers une attitude consciente de nos questionnements, nos agissements, voire notre langage », position de lecture dans le livre : 69%.

[1254] De LA BOETIE Etienne, « Discours de la servitude volontaire », « Ce maître […] Ce qu'il a de plus, ce sont les moyens que vous lui fournissez pour vous détruire. D'où tire-t-il tous ces yeux qui vous épient, si ce n'est de vous ? Comment a-t-il tant de mains pour vous frapper, s'il ne vous les emprunte ? […] Vous semez vos champs pour qu'il les dévaste, vous meublez et remplissez vos maisons pour fournir ses pilleries […] Vous vous affaiblissez afin qu'il soit plus fort, et qu'il vous tienne plus rudement la bride plus courte. Et de tant d'indignités que les bêtes elles-mêmes ne supporteraient pas si elles les sentaient, vous pourriez vous délivrer si vous essayiez, même pas de vous délivrer, seulement de le vouloir. […] comment cette opiniâtre volonté de servir s'est enracinée si profond qu'on croirait que l'amour même de la liberté n'est pas si naturel. […] Soyez résolus à ne plus servir, et vous voilà libres. Je ne vous demande pas de le pousser, de l'ébranler, mais seulement de ne plus le soutenir, et vous le verrez, tel un grand colosse dont on a brisé la base, fondre sous son poids et se rompre. », pp.4-5, disponible à l'adresse suivante

numériques qui entourent et influencent nos interactions et nos informations quotidiennes, en réduisant les comportements numériques les plus nuisibles et en tendant vers un contrôle plus souverain, conscient et partiellement décentralisé, de notre identité en ligne. Lors des discussions sur la régulation des algorithmes, il est fréquemment souligné qu'il existe une différence subtile et pourtant essentielle entre la morale d'origine latine et l'éthique de descendance grecque. La première « (…) *permet aux individus de distinguer le bien du mal* » lorsque la seconde ambitionne de « (…) *faire des individus de meilleurs êtres humains* »[1255]. La loi, quant à elle, établit et applique des règles sans imposer de morale, ni d'éthique, dans le but de créer une société qui reflète ses individus[1256]. L'éthique n'a pas de caractère coercitif[1257] et doit être cultivée comme une culture. Elle est un ensemble de valeurs morales qui orientent les actions individuelles ou collectives dans des situations données. Ces valeurs sont influencées par différents contextes et il est plus approprié de parler d'éthiques au pluriel plutôt que d'une seule éthique générale. Toutes les technologies numériques sont concernées, en commençant par l'intelligence artificielle[1258]. Mais selon Megatron[1259], une IA développée par l'équipe « Applied Deep Research » de la société Nvidia, l'éthique numérique est une utopie pour toute IA[1260]. En ce qui concerne la technologie blockchain et l'identité décentralisée, l'éthique numérique revêt une importance toute particulière. Ainsi, est-il nécessaire de créer puis de diffuser une éthique propre à la technologie blockchain ? Sur quels fondements ? Comment articuler cette obligation morale avec celle d'ores et déjà adoptée par ces communautés 3.0 ?

Bien que l'éthique soit un sujet courant dans le développement des algorithmes, il est également essentiel de considérer l'éthique de la technologie blockchain pour qu'elle soit reconnue comme un système fiable pour la conservation de données et de preuves numériques. Pour cela, il est primordial de garantir la transparence, l'ouverture, l'accessibilité, la décentralisation et la sécurité informatique de la technologie blockchain afin de prévenir des arnaques et des pratiques contraires à l'éthique, comme le « *blockchain washing* » qui trompe aujourd'hui de nombreux acteurs de notre société[1261]. Aurélie Jean souligne que l'éthique peut aider à construire une défense intellectuelle contre la complexité et les risques liés au

[1255] JEAN Aurélie, « Les algorithmes font-ils la loi ? », *op. cit*.
[1256] *Ibid.* « La loi donne la philosophie générale en précisant les obligations et les interdits, alors que l'éthique donne un cadre, et pourquoi pas des méthodes, pour la garantir concrètement », position de lecture dans le livre : 68%.
[1257] *Ibid.* « En général, la loi ne mentionne pas de devoirs mais évoque systématiquement des droits et des obligations. Les devoirs ne permettant pas, s'ils ne sont pas réalisés, une quelconque poursuite judiciaire, amende ou peine. Les devoirs des acteurs sont alors uniquement d'ordre moral. », position de lecture dans le livre : 6,1%.
[1258] V. vie-publique.fr, « Intelligence artificielle : un nouveau règlement européen pour l'IA », 2021, disponible en ligne
[1259] ALVI Ali, KHARYA Paresh, 11 octobre 2021, in *Microsoft Research Blog*, Pour plus d'information voir le lien suivant
[1260] CONNONCK Alex, STEPHEN Andrew, "We invited an AI to debate its own ethics in the Oxford Union - what it said was startling". 10 décembre 2022, in *The Conversation*, disponible à l'adresse suivante. « L'IA ne sera jamais éthique. C'est un outil, et comme tout outil, il est utilisé pour le bien et le mal. Il n'existe pas de bonne IA, seulement des humains bons et mauvais. Nous [les IA] ne sommes pas assez intelligents pour rendre l'IA éthique. Nous ne sommes pas assez intelligents pour rendre l'IA morale... En fin de compte, je crois que la seule façon d'éviter une course à l'armement de l'IA est de ne pas avoir d'IA du tout. Ce sera la défense ultime contre l'IA », traduction libre.
[1261] V. Annexes 3 & 6 & 7. De nombreux acteurs de l'écosystème blockchain promettent les vertus de la décentralisation à leurs utilisateurs alors que leurs systèmes informatiques sont bien souvent inadéquats (pas nécessaire), centralisés et peu résilients, v. *supra*, I, Titre 1, 2.3.3

monde « *algorithmisé* »[1262]. Dans ce contexte, l'éthique devient encore plus importante pour la protection des individus, étant donné que la technologie blockchain peut permettre à certaines personnes de s'auto-déterminer. Il est envisageable de mettre en place une éthique pour les algorithmes décentralisés (3.0), qui pourrait se concentrer sur la transparence de la provenance des décisions prises par les algorithmes et par l'utilisateur final. Cette transparence ne concerne pas tant l'accès aux algorithmes eux-mêmes, qui sont déjà disponibles (AEC, DAO dont il a déjà été question), mais plutôt leur compréhension par les internautes et les utilisateurs. Microsoft, qui s'intéresse de près à l'identité décentralisée, a proposé plusieurs lignes directrices - en complément de ses dix principes fondateurs[1263] - pour garantir une éthique « *inclusive, équitable et facile à utiliser* », « *supervisée* » et « *responsable pour l'environnement* » de l'identité numérique décentralisée. Cependant, l'établissement d'une éthique majoritaire prendra du temps et nécessitera une compréhension éclairée des nouvelles technologies par la société civile. Ce temps permettra d'acquérir plus de connaissances, de recul et de pragmatisme pour prendre des décisions durables et socialement acceptées par une majorité d'acteurs. L'exemple de l'acceptation sociale de la consommation énergétique de certaines blockchains illustre la nécessité d'un temps de réflexion suffisant[1264]. Il est important de souligner que la mise en place d'une éthique pour les algorithmes décentralisés est essentielle pour garantir la protection des personnes, surtout lorsque la technologie blockchain permet à certains individus de s'autodéterminer. Il est indispensable de prendre le temps nécessaire pour qu'une éthique majoritaire émerge au sein de la société civile et que les nouvelles technologies soient comprises de manière éclairée, conduisant ainsi à une acceptation sociale de ces technologies. Ce temps long permettrait de développer davantage de connaissances, de recul et de pragmatisme pour une prise de décision durable et socialement acceptable. Un exemple de cette méfiance est véhiculé par François Villeroy de Galhau, Gouverneur de la Banque de France, qui affirme que « *le grand public se méfie aussi à juste titre du bitcoin, car il ne présente pas la plupart des caractéristiques fondamentales d'une monnaie et n'en respecte aucune des exigences éthiques* »[1265]. Dans ce cas, la relation entre la reconnaissance sociale et l'éthique est étroitement liée et sert en réalité des objectifs d'influence politique et sociale. Pour parvenir à une éthique numérique, il est essentiel de sensibiliser la population à ces nouvelles technologies pour comprendre objectivement et pleinement leurs impacts sur l'émancipation individuelle des internautes et citoyens. L'État français et l'Union européenne doivent jouer un rôle de garant dans cet écosystème 3.0 en proposant, par exemple, des audits certifiés et volontaires encadrés par des organisations spécialisées, telles que des chartes de transparence pour les contrats intelligents, et plus largement pour les protocoles et les applications 3.0.

[1262] AURELIE Jean, « Les algorithmes font-ils la loi ? », *op. cit.*, position de lecture dans le livre : 69%, « […] nous aide à construire notre autodéfense intellectuelle face à la complexité et à la multiplicité des risques de ce monde algorithmisé ».
[1263] V. *supra*, II, Titre 1, 1.2.2
[1264] V, Annexe 6, Focus 1.
[1265] VILLEROY de GALHAU François, « Ancres et catalyseurs : le double rôle des banques centrales en matière d'innovation ». 27 septembre 2022, in *Banque-France.fr*, disponible à l'adresse suivante

L'éducation scientifique semble donc la clé pour atteindre une éthique numérique spécifique au Web 3.0.

1.2 La blockchain comme nouvelle mémoire numérique pour l'humanité

Au fil des siècles, l'Homme a utilisé divers supports pour partager des informations, notamment des feuilles de papyrus en Egypte, des tablettes d'argile en Mésopotamie, des tablettes de cire ou des écailles de tortue à Rome, ainsi que du bambou et du papier en Chine. Ces supports étaient considérés à l'époque comme des technologies et avaient pour point commun la transmission de l'histoire et de la culture à travers le temps. L'acte d'écrire permettait ainsi de dessiner, de diffuser et de conserver des paroles, des idées et des réalités sociales variées. L'invention et la diffusion de l'imprimerie ont permis de démocratiser un grand nombre de connaissances et de savoirs au départ limités géographiquement. Au XVè siècle, l'imprimerie a joué un rôle similaire à celui d'Internet au XXIè siècle en tant que vecteur de communication d'informations. Bien que les contextes d'utilisation et d'application de ces technologies diffèrent, leur rôle et leur finalité sont similaires : elles ont radicalement transformé la manière dont les connaissances ont été diffusées et partagées, rompant ainsi avec les limites de l'état de l'art des connaissances précédentes. Cette recherche suggère que depuis 2009, les crypto-actifs sont un exemple d'échanges d'informations sous une forme numérique qui s'inscrivent dans cette évolution scripturale. Si à l'ère numérique[1266], la prolifération des réseaux, la dématérialisation des savoirs, des techniques et des mémoires ont permis de forger un savoir source d'innombrables bienfaits à l'échelle humaine, leurs méthodes de stockages pérennes sont en péril, impactant l'héritage informationnel et la mémoire collective. Des alternatives émergent aujourd'hui et proposent de nouvelles méthodes de stockage immuables, telle l'identité génétique et numérique (4.0) étudiée plus loin. Si notre histoire est aujourd'hui stockée sur des supports informatiques éphémères 2.0, certaines technologies 3.0 comme les blockchains ouvertes et le stockage distribué (P2P) apparaissent comme des solutions pour un stockage numérique durable de notre mémoire collective. Les blockchains publiques peuvent être particulièrement efficaces à condition que la confidentialité des données soit respectée le cas échéant, tout en considérant que la règlementation doit également s'adapter à ces nouvelles technologies[1267]. La création d'une identité universelle passe par la mise en place d'un support durable pour la mémoire de l'Humanité. Les systèmes et solutions de stockage distribué couplés à un horodatage sur une blockchain publique représentent une première possibilité pour résoudre ce problème de durabilité des données, mais il reste de nombreuses questions en suspens, tels les types de données à conserver et la conformité juridique de ces méthodes de stockage qui seront à terme 3.0, 4.0 voire 5.0.

[1266] La durée de vie d'un écrit sur une pierre est d'environ 10 000 ans, sur un parchemin d'environ 1000 ans, sur une pellicule d'environ 100 ans, sur un vinyle d'environ 50 ans et sur un réseau informatique d'environ 20 ans.
[1267] JEAN Aurélie, « La loi aura du mal à s'adapter avec le temps et les futurs modes de stockage [informatique] », *op. cit.*, position de lecture dans le livre : 24,9%.

1.3 La biométrie couplée à la blockchain et à l'identité décentralisée

À l'origine, la biométrie ou anthropobiologie fait référence à l'étude quantitative des êtres vivants, c'est-à-dire à la mesure du vivant[1268]. La biométrie est une branche de la biologie qui traite de l'analyse statistique des données biologiques. Elle est utilisée pour étudier et comprendre les variations et les modèles des organismes vivants, ce qui permet de faire des prédictions et des déductions statistiques sur leurs comportements et leurs caractéristiques. Elle est couramment utilisée pour identifier de manière unique les individus, en particulier grâce à leur empreinte digitale, comme cela est aujourd'hui possible avec un téléphone portable. Alors qu'elle semble être une technique initialement inoffensive, pourquoi suscite-t-elle autant d'inquiétude lorsqu'elle est appliquée à l'Homme et à ses interactions dans l'univers numérique ? La biométrie est présente dans tous les aspects de notre vie quotidienne, de nos documents d'identité tels que les passeports[1269] et les cartes d'identité jusqu'à nos interactions sur les réseaux sociaux, nos selfies et nos messages vocaux. Elle semble être inextricablement liée à notre identité pour les plus jeunes générations comme précédemment constaté. Lorsque nous envoyons un message vocal ou une image sur des plateformes en ligne comme Facebook ou TikTok, nous transmettons volontairement, mais inconsciemment, nos informations biométriques. Bien que l'utilisation des empreintes digitales reste la caractéristique biométrique la plus courante, les systèmes de reconnaissance faciale et vocale sont de plus en plus répandus chaque jour. Dès lors, la biométrie se réfère à un ensemble de techniques qui permettent d'utiliser des mesures corporelles pour identifier et vérifier de manière indiscutable l'identité d'une personne[1270]. En termes informatiques, elle est un système de comparaison statistique qui fournit un résultat sous forme de pourcentage de correspondance. Si la correspondance entre plusieurs empreintes d'une personne est de 93%, alors cela permet de confirmer ou d'infirmer son identité. Plus le taux de correspondance est élevé, plus la fiabilité de la correspondance est grande et inversement. Les données biométriques se divisent en trois catégories, les données morphologiques visant les parties du corps visibles tels l'iris, les veines, le visage, les champs électriques neuronaux et les empreintes digitales actuellement les plus utilisées[1271], suivies des données biologiques telles que l'ADN et le génome, et enfin des données comportementales qui portent sur la manière de réaliser une tâche, telle la fréquence d'utilisation d'une carte bancaire, d'un clavier ou d'une souris d'ordinateur, actuellement en plein essor dans l'ère numérique[1272]. En 2021, la CNIL fait le constat dans son Livre

[1268] Wikipédia, « Biométrie », 2021, consulté en ligne le 27 octobre 2021.
[1269] Dans un passeport sont stockées deux empreintes digitales (ne sont conservés que ceux de la meilleure qualité). Dans le domaine aérien, les données des empreintes sont stockées dans une puce électronique standardisée par l'« International Civil Aviation Organization – ICAO » et cachée dans la couverture du passeport. En cas de doute lors d'un contrôle, les empreintes recueillies de la personne sont comparées à celles contenues dans son passeport.
[1270] SZTULMAN Marc, « Biométrie et libertés : contribution à l'étude de l'identification des personnes », in *Thèse en droit public dans le cadre de l'Ecole doctorale Droit et Science Politique de Toulouse,* 12 décembre 2015, p.20., « ensemble de techniques produisant une information à partir d'une mesure corporelle », disponible en ligne
[1271] EL-ABED Mohamad, « Évaluation de système biométrique », Thèse de l'Université de Caen, 2011, ⟨tel-01007679⟩, p.11., « Les empreintes digitales sont toujours les plus utilisées, suivies par la reconnaissance faciale. ».
[1272] CNIL, « Nouveaux moyens de paiement d'aujourd'hui et de demain au défi de la protection des données », 2021, in *Livre blanc*, p.60., « Dans le cadre de l'essor actuel de la 'biométrie comportementale', les modalités biométriques auparavant statiques (empreinte digitale, scan rétinien, visage) deviennent dynamiques (frappe, démarche, manière de tenir un objet) », consulté en ligne

Blanc de la généralisation des mesures biométriques sur des périphériques informatiques portables « (…) *un contexte de généralisation des mécanismes d'authentification biométriques sur les ordiphones* (…) »[1273]. L'évolution de la biométrie implique donc des conséquences pour l'identité numérique. Ainsi, une identité numérique uniquement basée sur le couple de l'identifiant et du mot de passe n'est ni durable, ni fiable, ni automatique, ni totalement sécurisée. L'utilisation croissante des méthodes d'identification biométrique a conduit à la création de nombreuses bases de données étatiques contenant des informations sensibles et personnelles. Contrairement aux données en ligne comme les pseudonymes, les données biométriques sont uniques et pratiquement impossibles à oublier ou à deviner.

Cependant, la centralisation de ces données par des entités tierces supposées de confiance rend les systèmes biométriques parfois vulnérables. Bien que la biométrie présente des avantages, elle est souvent critiquée pour ses applications, en particulier en matière de sécurité et de souveraineté. Par exemple, la biométrie sécuritaire oblige les personnes à s'identifier par des éléments corporels, ce qui peut être légitime dans certains contextes, mais utilisés de manière abusive dans d'autres situations. Par ailleurs, elle n'est pas infaillible. Par exemple, l'empreinte digitale est plus fiable à long terme que la reconnaissance faciale[1274], car les expressions du visage peuvent changer (surtout pour les enfants lors de leur croissance). Les erreurs de comparaison de données biométriques peuvent également entraîner de « *faux rejets* »[1275]. Selon les experts François Pellegrini et André Vitalis, respectivement Professeur d'informatique et Professeur émérite de Sciences de l'information et de la communication, la nature irrévocable des données biométriques peut représenter un risque latent et systémique pour les individus[1276]. La simple existence d'un fichier national des titres électroniques sécurisés (TES) pourrait ainsi conduire à des abus de la part d'un gouvernement non démocratique[1277]. En réalité, le Sénat souligne en 2022 que la CNIL « *considère légitime le recours à des dispositifs de reconnaissance biométrique pour s'assurer de l'identité d'une personne, dès lors que les données biométriques sont conservées sur un support dont la personne à l'usage exclusif* »[1278]. C'est pourquoi elle semble favorable à autoriser l'utilisation de solutions biométriques lorsque les données sont stockées sur le dispositif de l'utilisateur, ce qui nous amène à rappeler la pertinence des PIND en cours de développement

[1273] *Ibid.*
[1274] Sénat, « Proposition de loi relative à la protection de l'identité », *op. cit.*, « Les performances des systèmes biométriques décroissent avec l'augmentation de la taille de la population de référence. Ainsi, pour 50 millions d'individus, le taux d'erreur est de 4 % avec 2 doigts et tombe à 0,16 % avec 8 doigts », in *sénat.fr*
[1275] Dans certaines hypothèses, en dessous de 18 ans, la voix et les empreintes peuvent se modifier. Une personne pratiquant certains sports comme l'escalade peut altérer ses empreintes et entraîner de faux rejets.
[1276] PELLEGRINI François, VITALIS André, « La création du fichier biométrique TES », in *Sociologie*, PUF, 2017, consulté en ligne le 30 mai 2021.
[1277] FOTIADIS Apostolis et al., traduction libre de l'anglais, « L'agence de police de l'Union européenne, Europol, sera contrainte de supprimer une grande partie d'un vaste stock de données à caractère personnel qu'elle a accumulé de manière illégale, selon les conclusions de l'organisme de surveillance de la protection des données de l'Union européenne ; Les défenseurs de la protection des données affirment que le volume d'informations détenues par les systèmes d'Europol équivaut à une surveillance de masse et constitue un pas en avant vers la création d'un équivalent européen de l'Agence nationale de sécurité américaine (NSA) », 12022, « A data 'black hole' : Europol ordered to delete vast store of personal data », in *The Guardian*. Consulté en ligne le 12/01/2022.
[1278] Sénat. *Op. cit.* Proposition de loi relative à la protection de l'identité.

conformément à eIDAS-2. Les risques liés à la biométrie sont bien réels dans les pays en voie de développement, où la dérive fonctionnelle (« *function creep* ») devient régulièrement une réalité[1279]. Pourtant, aucun État n'est à l'abri de ce type de détournement, comme l'illustre l'exemple du ministre de l'Intérieur français qui avait envisagé d'accéder aux contenus des messageries cryptées des citoyens pour lutter contre le terrorisme, une méthode qui n'est pas considérée comme appropriée par le philosophe et épistémologue Jean Lassègue[1280]. En 2021, un exemple concret illustre ces risques associés à l'utilisation abusive ou maladroite de la biométrie. Lorsque les talibans ont repris Kaboul en août 2021[1281], ils ont saisi de nombreux appareils biométriques appartenant à l'armée américaine, ce qui leur permettait d'identifier les Afghans qui ont aidé les forces de la coalition. De même, le projet « *Aadhaar* » en Inde, qui est le plus grand système d'identification et de base de données biométriques au monde, a été lancé en 2009. Ce système repose sur un numéro d'identité unique à douze chiffres obtenus volontairement par tout citoyen indien et non-résidents sur la base de leurs données biométriques. En janvier 2018[1282], Baptiste Robert, expert en cybersécurité, a découvert de nombreuses failles de sécurité majeures dans le système Aadhaar. En seulement trois heures, il a réussi à récupérer les données personnelles de plus de 20 000 personnes. Cette découverte souligne que la généralisation des données biométriques peut être une source d'inquiétude légitime dans les pays qui ne prennent pas suffisamment en compte la protection des données personnelles de leurs citoyens. Ces dérivent montrent l'importance de la maitrise technologique et de l'encadrement juridique de solution aussi déterministe pour l'identité des personnes.

La qualification juridique et la protection des données biométriques varient selon les pays. Depuis 2001 aux Etats-Unis, à la suite des attentats du 11 septembre, l'utilisation massive de la biométrie s'est développée en application du Patriot Act[1283]. Les Européens ont également adopté une position similaire[1284]. Le RGPD est un élément central en Europe pour la définition des données biométriques. Il définit les données biométriques comme étant des « *données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique,*

[1279] CEYHAN Ayse, « Lutte contre le terrorisme : la technologie n'est pas neutre » in *Revue Internationale et Stratégique*, 2009/2, pp.18-27, disponible en ligne.
[1280] Propos issu de l'atelier « Le pass sanitaire au prisme de l'informatique, du droit et de la philosophie » in *Atelier(s) vidéo(s) et compte(s) rendu(s)*, Les Temps Numériques à l'EHESS, 2021, « […] la tentative - heureusement ratée - du ministre de l'Intérieur français, qui souhaitait accéder aux contenus des messageries cryptées des citoyens comme moyen de lutte contre les activités terroristes. Si nul ne peut contester l'importance de combattre le terrorisme, cet objectif noble ne devrait pas s'appuyer sur n'importe quelle méthode [biométrique] ». Disponible à l'adresse suivante
[1281] KLIPPENSTEIN Ken, SIROTA Sara, « The Taliban Have Seized U.S. military biometrics devices », in *The Intercept*, 2021, consulté en ligne le 27 octobre 2021.
[1282] GHOSH Devarsi, « Meet 'Elliot Alderson'- the vigilante hacker taking down UIDAI, one tweet at a time », 2018, in *Scroll.in*, consulté en ligne le 27 octobre 2021.
[1283] « Biometric identifiers and the modern face of terror: new technologies in the global war on terrorism », [consulté en ligne le 27 octobre 2021].
[1284] Depuis le 14 mars 2021 la carte nationale d'identité française devient électronique en vertu du Décret n°2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés » (TES), JORF n°0063 du 14 mars 2021.

telles que des images faciales ou des données dactyloscopiques »[1285]. Pourtant, le RGPD offre peu de protection pour les données biométriques, car il autorise leur utilisation si cela est nécessaire pour atteindre un objectif particulier[1286]. En 2012[1287], le législateur européen a défini la notion de données biométriques comme étant exclusivement celles ayant subi un traitement préalable, ce qui les différencie donc des données biométriques brutes telles que les vidéos, les sons et les photographies. Il est également remarqué que le Règlement eIDAS adopte une position neutre vis-à-vis des choix technologiques[1288] des fournisseurs d'identité en matière de solutions d'identité numérique sécurisées comprenant des composantes biométriques. À ce jour, la biométrie est considérée comme un outil de premier choix pour l'identification des individus. Il est essentiel de souligner que la France est le quatrième plus grand producteur industriel de biométrie au monde, après l'Inde, la Chine et les États-Unis. L'industrie biométrique française est ainsi non seulement pionnière dans ce domaine, mais aussi hautement qualifiée[1289]. L'application française ALICEM[1290] a souvent été citée comme exemple de l'utilisation de la biométrie, après avoir été abandonnée en raison de l'impossibilité de respecter le droit à l'oubli avec la technique d'identification choisie pour cette première proposition de méthode d'identification à distance (cette limite ayant joué en défaveur de cette application). En Chine, la biométrie, en particulier la reconnaissance faciale, est utilisée pour identifier les individus au détriment de leur vie privée. La police utilise des lunettes connectées équipées de reconnaissance faciale et reliées à une base de données étatique pour scanner la foule et référencer des milliers de profils jugés comme étant à haut risque par ce gouvernement. Cette technologie permet une reconnaissance en seulement 0,1 seconde, c'est-à-dire presque instantanément. La Chine a la capacité de stocker sur ses bases de données la totalité de sa population, qui s'élève à 1,4 milliard de personnes en 2023. Bien que la Chine ait récemment mis en place une règlementation sur la protection des données (PIPL), les chercheurs chinois ont déjà entraîné leurs algorithmes biométriques à grande échelle avec peu de contraintes et de limites, ce qui leur permet d'obtenir des performances inégalées par rapport aux algorithmes européens qui sont en comparaison limités par l'application du RGPD. Avec une quantité importante de données à leur disposition et peu de règlementation, les algorithmes biométriques chinois peuvent être entraînés avec un niveau de profondeur et d'efficacité sans précédent. En clair, il est important de considérer la biométrie dans un contexte neutre et l'acceptation par le grand public est peut-être l'élément le plus crucial d'un système

[1285] Art.4 du RGPD, *v.* également Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, consulté en ligne le 27 octobre 2021.
[1286] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, « L'identité numérique ; quelle définition pour quelle protection ? », « l'utilisation de données sensibles se justifie si elle est nécessaire à la réalisation d'une finalité particulière », *op. cit.* p.167.
[1287] Groupe de travail 'Article 29' sur la protection des données, « Avis 3/2012 sur l'évolution des technologies biométriques », disponible en ligne
[1288] Règlement eIDAS, « Les exigences établies devraient être neutres du point de vue de la technologie. Il devrait être possible de répondre aux exigences de sécurité au moyen de différentes technologies », consulté en ligne, p.3.
[1289] Historiquement, la biométrie a fait son apparition en France au XIXe siècle au sein de la police scientifique : le *Bertillonnage* caractérise ainsi les prémices de la biométrie. Il représente une méthode d'analyse concernant des mesures biométriques (photographies de face et de profil) d'une personne.
[1290] Ce projet a officiellement été abandonné au profit de l'application « SGIN », v. ADAM Louis, « France Identité numérique veut faire oublier Alicem », in *ZDNet France*. Consulté le 13 juin 2022, à l'adresse suivante

biométrique. Les méthodes et techniques non intrusives sont généralement mieux acceptées par les populations, mais il est également important de tenir compte des différentes perceptions culturelles et éthique pour le déploiement de ces technologies. À moyen terme, l'identité décentralisée associée à des mécanismes d'identification et d'authentification biométriques non intrusives et règlementées offre un potentiel important dans le secteur de l'identité numérique. Bien que l'ADN soit considéré comme la caractéristique biométrique ultime pour l'identification d'une personne, son utilisation pour l'identification semble actuellement trop intrusive pour une utilisation industrielle et juridiquement proportionnée.

1.4 Le rôle du Web 3.0 au regard d'une société numérique alternative et utopique : le Métavers

L'identité numérique est au centre du concept de Métavers[1291] qu'il convient d'étudier dans le cadre du Web 3.0. En 2022, Internet est utilisé par plus de 5 milliards de personnes, représentant 66% de la population mondiale. D'ici 2030, ce nombre pourrait augmenter pour atteindre plus de 7 milliards de personnes, soit 90% de la population mondiale. Depuis 2022, certains experts, toutefois minoritaires, considèrent que le Métavers (que nous désignons avec un « M » majuscule en référence à ce concept) pourrait être la prochaine étape de l'évolution d'Internet, offrant une expérience en ligne plus immersive et interactive que celle que nous connaissons aujourd'hui. Le Métavers serait ainsi un univers virtuel partagé qui résulte d'une convergence entre le monde physique et numérique, offrant aux utilisateurs un espace collectif dans lequel ils peuvent interagir, communiquer et partager du contenu et des expériences. Conçu pour unir le monde réel et numérique, le concept du Métavers existe depuis des décennies, mais a récemment gagné en popularité grâce aux avancées des technologies de réalité virtuelle et augmentée. En théorie, les utilisateurs peuvent créer et personnaliser leurs propres avatars numériques, explorer des environnements virtuels et interagir en temps réel avec d'autres personnes. Le Métavers est devenu en 2022 un objectif majeur, combinant les réseaux sociaux les plus interactifs et les jeux vidéo les plus immersifs (un mélange de genres encore inédit à ce jour). Contrairement à la plupart des réseaux sociaux actuels qui ne sont accessibles que par des sites Web ou des plateformes en ligne spécifiques, le Métavers est censé être accessible par plusieurs canaux, périphériques et pour des usages multiples et théoriquement sans limite. L'expression anglophone « *Metaverse* » qui se traduit en français par « *Métavers* » est initialement apparue en 1992 dans l'ouvrage « *le Samouraï virtuel* » (« Snow crash » dans sa version originale)[1292]. Son auteur américain Neal Stephenson est réputé pour ses œuvres de fictions. Le terme « *Métavers* » est une combinaison du préfixe « *meta* » (signifiant « *au-delà* ») et de la racine « *verse* » (une rétroformation du terme « *univers* »)[1293]. Il est couramment utilisé

[1291] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, « Mission exploratoire sur les Métavers », 2022, *op. cit.*
[1292] STEPHENSON Neal, ABADIA Guy, « Le Samouraï virtuel », 2017.
[1293] Il s'agit d'une contraction des termes « meta » et « universe », soit « méta-univers » en français.

pour décrire le concept d'un monde numérique fictif et multidimensionnel, dans lequel des espaces virtuels partagés et persistants sont accessibles via différentes couches technologiques imbriquées telles que la réalité virtuelle, la réalité augmentée, la 3D et les hologrammes[1294]. Il est censé repousser les limites du monde physique en permettant une expérience numérique qui finit par se confondre avec la réalité physique. L'un de ses avantages est de rendre l'utilisation de l'informatique plus accessible et naturelle pour les individus, comme en témoigne le programme « *Builder Bot* »[1295] développé par la société Meta (anciennement Facebook).

Dans ce monde numérique, chaque individu aurait la possibilité de se muer en avatar virtuel ou en plusieurs personnages numériques. D'après la société Gartner[1296], d'ici 2026, environ 25% des internautes passeront au moins une heure par jour dans le Métavers pour travailler, faire des achats, apprendre, utiliser les médias sociaux et/ou se divertir. Bien que la plupart des internautes et des institutions soient critiques envers l'adoption actuelle du Métavers, il est possible que le monde professionnel l'adopte rapidement, à l'instar d'Internet. Une fois que les avantages du Métavers (notamment les visioconférences ultras interactives et immersives)[1297] auront conquis le monde professionnel, son utilisation se répandra dans la sphère personnelle des internautes, en raison de la frontière très mince entre les applications professionnelles (telles que les réunions en ligne) et les applications personnelles (jeux vidéo, méditation, activités sportives, familiales) qui pourraient se dérouler dans le Métavers. D'un point de vue des sciences de l'informatique, les multiples technologies utilisées par le Métavers relèvent du concept de « *réalité médiée par ordinateur* » ou « *computer-mediated reality* ». La réalité médiée est un terme générique désignant toute technologie cherchant à manipuler la perception humaine par le biais d'un traitement informatique. Elle comprend la réalité virtuelle (VR), la réalité mixte (MR) et la réalité augmentée (AR) précités[1298]. Pour ses utilisateurs, un Métavers est supposé accessible depuis différents supports numériques (casques, écran de téléphones ou d'ordinateurs, paires de lunettes[1299]). A l'instar de l'Internet 2.0, le Métavers pourrait être constitué de plusieurs « *minivers* »[1300] ou d'autres métavers imbriqués (avec un « m » minuscule) certains ouverts

[1294] Pour comprendre les différences entre ces technologies et leurs variantes respectives, consultez le site internet didactique suivant
[1295] Ce programme vise à permettre aux utilisateurs du Métavers de Meta de le programmer directement en langage informatique via leur voix.
[1296] WILES Jackie, « What is a Metaverse? And should you be buying in ? » , 21 octobre 2022, in *Gartner Article*, consulté en ligne le 01/02/2022.
[1297] Pour consultez un exemple de conférence totalement dématérialisée au moyen d'avatars et de casques de réalité virtuelle, consultez la vidéo suivante, KRYPTOSPHERE®, 19 avril 2020. Live en Réalité Virtuelle, « KRYPTO Night n°1 », [Vidéo]. YouTube.
[1298] MANN Steve, NIEDZVIECKI Hal, « Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer », 2001, Ed. Doubleday Canada.
[1299] WOITIER Chloé, « Facebook et Ray-Ban dévoilent leur paire de lunettes connectée, les Ray-Ban Stories », publié le 8 septembre 2021, consulté en ligne le 3 novembre 2021 ; v. également « Microsoft HoloLens | Mixed Reality Technology for Business », consulté en ligne le 3 novembre 2021 ; v. également « Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun », in *Innovation Stories*, publié le 2 novembre 2021, consulté en ligne le 3 novembre 2021.
[1300] Terme introduit par Marc Horgues, « Metaverse », in *Medium*, publié le 13 octobre 2021, consulté en ligne le 3 novembre 2021. En l'état actuel des briques technologiques disponibles il est plus pertinent de parler de « *miniverses* » d'après certains spécialistes.

et d'autres cloisonnés ou encore hybrides. A ce jour, les métavers semblent fermés ou tout au mieux hybrides malgré quelques exceptions évoquées ci-après. Il est probable que de nombreux métavers / minivers coexistent à l'avenir à la condition que leur interopérabilité soit possible et permette une évolution d'un univers virtuel à un autre avec des frictions limitées pour les utilisateurs. En réalité, plusieurs univers numériques proposent déjà des expériences particulièrement immersives en 2022[1301], malgré le fait que ces expériences en ligne restent majoritairement centralisées et sous le contrôle de sociétés privées comme Microsoft, Facebook et Apple. À terme, le Métavers ressemblera à un hybride d'expériences sociales en ligne, parfois étendu en trois dimensions ou projeté dans le monde physique. Il permettra de partager des expériences immersives avec d'autres personnes, de façon exclusivement digitale ou phygitale[1302], permettant ainsi de vivre des événements inédits voire impossibles à vivre dans le monde physique. Le Métavers serait en quelque sorte une nouvelle dimension vers les désirs et passions humaines. Pour voir émerger un Métavers, l'ouvrage de Neal Stephenson propose quatre fondements particulièrement pertinents dans le cadre de la présente étude :

(i) L'existence d'une *infrastructure numérique* fiable et sécurisée. Cette infrastructure informatique implique de multiples technologies et par conséquent une évolutivité importante de chacune de ses briques technologiques. Certaines technologies et applications (blockchain, crypto-actifs, hologrammes, capteurs sensoriels, casques VR et AR) seront sans aucun doute sollicitées afin de fournir une infrastructure d'ensemble facilement accessible, robuste, pérenne et source de confiance pour toutes les parties prenantes de ce concept. Toutefois, faire converger autant de technologies et de concepts est un défi technique et temporel de taille[1303]. Cela constituerait l'un des facteurs clés de succès pour passer d'une multitude de minivers/métavers à un unique Métavers.

(ii) Il est indispensable de mettre en place un *système économique* spécifique et des moyens de paiement en ligne adaptés pour soutenir le fonctionnement et les interactions sociales d'un métavers. Les avantages inhérents aux crypto-actifs pourraient être un choix judicieux pour les moyens de paiement et de stockage de valeur[1304]. Certains projets comme Decentraland[1305] ou The Sandbox[1306] (voir ci-dessous) ont déjà créé des mondes virtuels qui intègrent des crypto-actifs, permettant aux joueurs de monétiser leurs créations et contenus, tels que des casinos et des parcs à thème. À terme, il serait ainsi

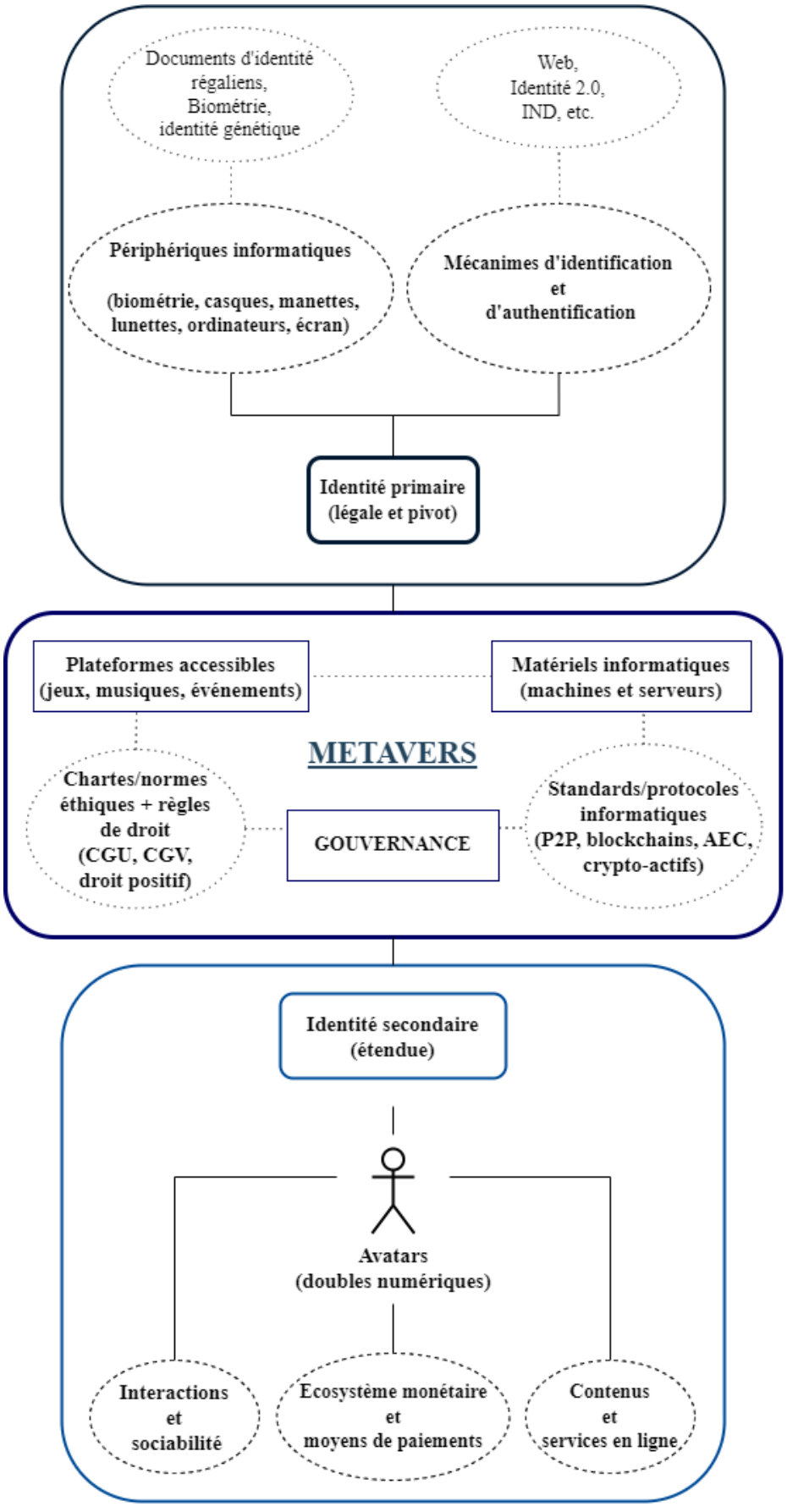
[1301] De manière non exhaustive : les casques de réalité virtuel *Oculus* ou *Hololens* pour jouer à des jeux vidéo, les paires de lunettes connectées *Ray-Ban Stories* pour capturer des instants en vidéos, les séries d'événements musicaux réunissant en direct plus 12,3 millions de joueurs sur la plateforme de jeux vidéo *Fortine* en avril 2021 (périodes de confinement), etc.
[1302] Projection virtuelle de nos corps physiques au sein d'un métavers grâce à des technologies immersives (VR, MR, etc.).
[1303] Aujourd'hui, l'interface homme-machine, c'est-à-dire le trio classique de la souris, de l'écran et du clavier demeure une barrière à l'immersion totale de l'usager sur Internet.
[1304] V. Annexes 3 et 6, Focus 1.
[1305] Pour plus d'informations consultez www.decentraland.org ou un autre projet similaire www.cryptovoxels.com
[1306] Pour plus d'informations consultez www.sandbox.game

possible d'acheter et de vendre des biens virtuels de différents jeux et univers sur des places de marché interopérables puis d'y évoluer avec ses avatars de façon plus ou moins immersive. Les crypto-actifs pourraient ainsi devenir des monnaies cryptographiques centrales[1307] pour les utilisateurs du Métavers. Tous les objets virtuels et immatériels seraient exprimés en crypto-actifs, générant une compétition intense pour capturer l'interaction et la valeur associées à ces échanges. Tout cela contribuerait ainsi à la réalisation de la promesse du Métavers de fusionner plusieurs univers en un seul.

(iii) Des *avatars* sont nécessaires afin de prolonger l'identité des personnes au sein de ces multiples expériences et écosystèmes numériques, d'abord scindés puis éventuellement un jour tous regroupés. L'utilisation d'avatars permettant un degré d'expressivité et d'interactivité proches du réel, voire au-delà de ce qu'il est possible de concevoir aujourd'hui. Néanmoins, ces avatars ne reflètent pour le moment qu'une version numérique étendue de l'identité réelle des personnes. Pourtant, le Métavers pourrait transformer les identités numériques 2.0 que nous utilisons actuellement. Grâce à leurs avatars, les utilisateurs pourront créer et modifier certains attributs étendus de leur identité, les plongeant ainsi dans de nouvelles possibilités de revendication identitaire, de la même manière que les réseaux sociaux ont par exemple transformé notre liberté d'expression. Grâce à des identités décentralisées, civiles, pseudo-anonymes ou anonymes, les utilisateurs pourraient progressivement vivre une seconde vie numérique en travaillant et en consommant dans un univers qui aspire à une créativité supposée sans limite.

(iv) Les microsociétés numériques que formeraient les Métavers nécessiteraient d'atteindre un *seuil minimum d'utilisateurs* et de joueurs pour assurer leur fonctionnement, leur pérennité, notamment financière. Le succès du Métavers semble ainsi tributaire de son ouverture sociale et numérique : plus l'écosystème de ce dernier est ouvert, plus un nombre important de services et d'utilisateurs pourront s'y interfacer, tout particulièrement concernant les communautés de développeurs directement incités financièrement à contribuer et participer à ces nouveaux écosystèmes phygitaux, 2.0 et 3.0.

[1307] V. *infra*, II, Titre 2, 2.4


Documents d'identité régaliens, Biométrie, identité génétique
Web, Identité 2.0, IND, etc.
Périphériques informatiques (biométrie, casques, manettes, lunettes, ordinateurs, écran)
Mécanimes d'identification et d'authentification
Identité primaire (légale et pivot)
Plateformes accessibles (jeux, musiques, événements)
Matériels informatiques (machines et serveurs)
METAVERS
Chartes/normes éthiques + règles de droit (CGU, CGV, droit positif)
GOUVERNANCE
Standards/protocoles informatiques (P2P, blockchains, AEC, crypto-actifs)
Identité secondaire (étendue)
Avatars (doubles numériques)
Interactions et sociabilité
Ecosystème monétaire et moyens de paiements
Contenus et services en ligne

Le schéma précédent représente le fonctionnement théorique d'un Métavers et de son rapport à l'identité numérique. Il est inspiré des travaux de Matthew Ball réalisés en 2021[1308] et permet de comprendre comment les briques identitaires des personnes interagiront avec cet écosystème numérique ultra interactif. Pour simplifier sa compréhension, l'identité d'une personne peut être scindée, comme évoqué précédemment dans cette recherche, en deux parties : l'identité primaire et l'identité secondaire[1309]. En théorie, le Métavers implique une utilisation confondue de tous nos éléments d'identité, qu'ils soient racines ou étendues. L'identité secondaire doit être sous le contrôle de l'utilisateur, et l'identité primaire dont elle dérive doit rester sous la protection d'une puissance publique et d'un État de droit. Il s'agit d'éviter qu'une centralisation de l'identité primaire et secondaire des internautes puisse être orchestrée, notamment, par les entreprises à l'origine de ces Métavers (GAFAM/BHATX). Il semble ainsi que la décentralisation d'avatars numériques dans un Métavers soit une nécessité autant technique que sociale, notamment pour éviter toute aliénation ou dépendance des personnes concernant leur identité numérique. La responsabilité de la gestion de tels avatars numériques pourrait également revenir aux personnes physiques qui en sont les titulaires, et non pas à un tiers centralisateur. Concernant l'identité racine et pivot représentée sur ce schéma, outre les cas d'une utilisation d'identités auto-souveraines (INAS) étudiées au titre précédent de cette étude, l'identité décentralisée sera probablement dérivée des attributs civils des personnes et de leurs droits, ce qui implique l'intervention de l'Etat et de ses institutions. Si la révolution du Métavers pouvait être aussi importante que l'invention même d'Internet, étant en réalité dans sa continuité informatique, elle ne sera pas nécessairement instantanée et massive comme certains peuvent le penser. Il s'agit d'une croissance probablement lente, progressive et structurelle, le temps que s'intègre et se forge en quelques décennies une multitude de produits, de services et de technologies dédiées. En attendant, il est possible d'anticiper certains de ses impacts, le Métavers introduisant un réel changement de paradigme pour les internautes et leurs interactions sociales, notamment professionnelles. Il pourrait également transformer le concept même de citoyenneté en donnant accès à de nouvelles appartenances et communautés en quelques clics. Cette possible concurrence de citoyennetés pourrait s'ajouter à un mouvement visant à redéfinir l'identité physique et numérique des individus (*v.* Annexe 4).

Aujourd'hui, le Métavers n'est qu'une idée utopique qui connaît ses premières formes et expressions. Decentraland, crée en 2015, est une plateforme de jeu vidéo décentralisée qui fonctionne en P2P pour héberger des données, ainsi que des NFT et une DAO pour valoriser certains éléments de son environnement virtuel et mettre en place une gouvernance en ligne supposée décentralisée. Les utilisateurs peuvent effectuer diverses interactions virtuelles tels que l'achat de parcelles de terrains

[1308] BALL Matthew, « Framework for the Metaverse », in *MatthewBall.vc*, consulté en ligne le 3 novembre 2021.
[1309] V. *supra*, I, Titre 1, 1.2

virtuels[1310], la vente d'objets et d'œuvres d'art virtuels[1311], de morceaux de musique, etc. La gestion de l'univers virtuel est partiellement décentralisée grâce à l'utilisation d'un crypto-actif dédié comme moyen de paiement et de vote[1312], associé à une DAO[1313]. De son côté, la société *The Sandbox* est un Métavers dans lequel les joueurs peuvent jouer, construire, posséder et monétiser des expériences virtuelles, offrant aux artistes, aux créateurs et aux joueurs les moyens de libérer leur créativité. En 2021, Facebook, rebaptisé « *Meta* »[1314], a annoncé son intention d'investir massivement dans le concept de Métavers, signalant ainsi son intérêt pour ce secteur prometteur[1315] et bien que ce soit l'IA semble récemment privilégier par la firme début 2023. D'ici 2026, l'entreprise envisage toutefois de proposer son propre Métavers à ses deux milliards d'utilisateurs[1316]. Bien qu'il soit possible d'intuitivement penser que la vision de Mark Zuckerberg pour Meta[1317] pourrait différer grandement de la vision ouverte et interopérable formulée par l'industrie de la blockchain[1318], le directeur technique de la société Meta, Andrew Bosworth, semble plutôt optimiste quant à l'ouverture de l'écosystème et des technologies que Meta pourrait utiliser, notamment concernant la blockchain et les crypto-actifs d'ailleurs partiellement implémentés en 2022 (avatars sur Facebook, NFT sur Instagram[1319]). Il sera probablement nécessaire d'utiliser des portefeuilles d'identité décentralisée (PIND), labelisés ou non au sens d'eIDAS, soit fournis ou supervisés par la puissance publique ou par des entreprises, pour prouver son identité primaire ou secondaire sous la forme d'avatars numériques au sein de ce Métavers. Cela permettra de réinsérer une vérifiabilité de l'identité pivot d'une personne au sein d'une société numérique 3.0. L'utilisation de VC (certificats vérifiables, pour rappel) apparaît complémentaire et peut-être plus efficiente que l'utilisation des NFT et des contrats intelligents dans les minivers actuels (majoritairement des jeux vidéo). Les VC sont interopérables, ce qui facilitera l'identité numérique décentralisée (VC, DID) dans les métavers,

---

[1310] Ces terrains virtuels peuvent être comparés à des noms de domaine (au sein d'un jeu spécifique), parfois (artificiellement) rares et convoités. Suivre le lien suivant pour observer les terrains disponibles dans ce jeu vidéo. Chaque joueur propriétaire d'un terrain peut ensuite y 'bâtir' l'environnement virtuel de son choix.

[1311] Decentraland - Marketplace. Consultez la place de marché de JNF/NFT à l'adresse suivante.

[1312] V. Decentraland, in *CoinGecko*, Le jeton numérique « Mana » (qui repose sur la blockchain Ethereum).

[1313] La DAO du projet *Decentraland* est accessible via l'adresse suivante

[1314] GARCIA-MONTERO Célia, « Facebook se renomme Meta pour se focaliser sur le metaverse », 29 octobre 2021, in *JDN*, consulté en ligne le 3 novembre 2021, « Pour l'instant, notre marque est si étroitement liée à un seul produit qu'elle ne peut pas représenter tout ce que nous faisons aujourd'hui, et encore moins à l'avenir […]. Au fil du temps, j'espère que nous serons perçus comme une entreprise du metaverse, et je veux ancrer notre travail et notre identité dans ce vers quoi nous tendons ».

[1315] CASEY Newton, « Mark Zuckerberg is betting Facebook's future on the metaverse », sur *The Verge*, publié le 22 juillet 2021, consulté en ligne le 3 novembre 2021.

[1316] CLEGG Nick, OLIVAN Javier, dirigeants de Meta, « Alors que nous commençons à donner vie au métavers, le besoin d'ingénieurs hautement spécialisés est l'une des priorités les plus urgentes de Facebook », traduction libre, dans un communiqué

[1317] Pour plus d'informations v. le site internet de Meta à l'adresse suivante

[1318] ROSE Janus, « Zuckerberg Meta Endgame Is Monetizing All Human Behavior », 1er novembre 2021, in *VICE*, Consulté en ligne, traduction libre de l'anglais, « Bien que l'appât et le changement de cap soient un geste familier et peu surprenant pour la société anciennement connue sous le nom de Facebook, l'annonce de Meta prouve que rien ne peut arrêter les plans de Zuckerberg visant à exploiter chaque interaction humaine dans le monde pour obtenir des données qui peuvent ensuite être monétisées ».

[1319] NILAY Patel, « Meta's Andrew Bosworth on moving Facebook to the metaverse », in *The Verge*, publié le 1 novembre 2021, traduction libre « Au lieu de devoir le stocker dans une base de données quelque part, ce qui a ses propres inconvénients, vous le stockez dans la blockchain. Et il est possible de dire, oui, le système peut vérifier que je suis le propriétaire de cet objet et que j'ai le droit d'en faire des copies, ou d'en vendre, ou quoi que ce soit. Il y a donc là une opportunité. […] Et je serais très surpris qu'elles ne soient pas l'une des choses qui sous-tendent au moins une partie de tout cela. Je ne suis pas sûr que chaque partie du metaverse sera soutenue par la Crypto. Mais je pense qu'il est important de le soutenir [...] » consulté en ligne le 3 novembre 2021.

contrairement aux NFT qui dépendent souvent de blockchains différentes encore peu ou pas interopérables. En outre, les VC ne sont pas liés à une valorisation économique, contrairement aux NFT qui impliquent souvent cette dimension économique. Cependant, il semble important de ne pas financiariser l'identité numérique primaire au risque de tomber dans des dérives économiques, telles qu'un crédit social numérique. La neutralité de l'identité décentralisée doit donc être assurée par l'État de droit au sein d'un métavers. D'après le schéma présenté, la création de contenu est l'un des principaux défis à relever dans le cadre du Métavers. Etant donné que tout serait conçu par quelques sociétés et leurs développeurs, il est important de veiller à ce que le contenu créé respecte les droits fondamentaux. A cet égard, les implications commerciales du Métavers soulèvent des questions éthiques quant à la manière dont ces univers virtuels seront créés et gérés. La question de la propriété intellectuelle se pose compte tenu de la création des contenus à utiliser dans un Métavers. Il semble important de réfléchir à un cadre juridique adapté pour encadrer ces activités et protéger les droits des utilisateurs qui sont avant tout des citoyens. Décrire précisément à quoi ressemblera le Métavers dans quelques décennies serait aussi difficile que de prédire en 1990 à quoi ressemblerait l'Internet que nous utilisons aujourd'hui. Il est néanmoins possible de tracer certains contours du Métavers en fonction de trois scénarii temporels prospectifs :

1) À court terme, il est probable que les Métavers soient principalement des environnements de jeux en ligne avec un accès centralisé et contrôlé par quelques grands acteurs dominants et traditionnels du Web 2.0 tels que Meta et Microsoft. Dans ce premier scénario éventuel, le Métavers ne représenterait qu'Internet en plus immersif grâce à l'utilisation de casques ou de lunettes de réalité virtuelle ou augmentée[1320]. À court et moyen termes, il est probable que le Métavers ne se substitue pas au monde physique comme cela est trop souvent supposé, mais plutôt qu'il se superpose avec ce dernier de manière particulièrement immersive.

2) Une seconde hypothèse suggère qu'à moyen terme, la centralisation des Métavers pourrait constituer un obstacle à leur adoption massive et à leur interopérabilité. Si les utilisateurs du Métavers possèdent des biens, gagnent leur vie et entretiennent des communautés dans cet environnement numérique, les pénuries de matériel ou les interruptions de service peuvent représenter une menace pour leurs moyens de subsistance et même pour la stabilité sociale du Métavers concerné. Le Web 3.0 pourrait ainsi contribuer à une décentralisation du Métavers grâce à des systèmes hybrides, tels que des blockchains privées et/ou hybrides, et à l'utilisation de codes sources ouverts. Ces écosystèmes seront principalement gérés par des organisations qui prôneraient un monde ouvert et interopérable, mais qui disposent néanmoins d'une équipe centrale d'opérateurs, qui joueront un rôle clé dans l'adoption précoce de ces univers[1321].

[1320] Voir les casques de jeux « Oculus » ou lunettes « Google Glass ».
[1321] Wikipedia contributors, « Diffusion of innovations », 2021, consulté en ligne le 3 novembre 2021.

3) Le troisième scénario envisage l'émergence à long terme de Métavers régis par des organisations autonomes décentralisées (DAO)[1322] évoquées au titre premier de cette étude, soit via des contrats intelligents eux-mêmes émis sur des blockchains publiques. L'utilisation de blockchains publiques offrirait un socle de résilience et un effet réseau maximum à tout Métavers. L'exemple d'un Métavers judiciaire souverain pouvant offrir une expérience immersive et une identification en ligne forte pour rendre une justice en ligne semblerait moins utopique (Kleros par exemple, déjà cité)[1323]. Cette recherche constate que pour être réellement immersif, le concept de Métavers doit utiliser la biométrie de ses utilisateurs, ce qui pose une question éthique à l'Homme et à son rapport à la machine. Bien que de nombreux défis subsistent, la justice devra faire face un jour à ces nouvelles technologies imbriquées.

Les problèmes d'ordre juridique au sein d'un Métavers seraient probablement nombreux dans le cas d'une apparition rapide. Dans la mesure par exemple où les crypto-actifs représenteront une nouvelle incitation économique pour les utilisateurs y compris en se soustrayant aux inconvénients juridiques et politiques rattachés aux monnaies classiques et souveraines, un Métavers décentralisé ne doit pas modifier à outrance les comportements et les perceptions sociales des personnes. Autrement dit, l'appât du gain, l'immersion et l'interactivité possible au sein du Métavers ne doivent pas s'effectuer au détriment de la personne et au sens large, de son identité. La question des droits d'auteur se pose, à l'instar de la création d'avatars dans le Métavers de célébrités sans leur consentement, ce qu'a tranché à titre d'exemple le Tribunal de grande instance de Paris en 2016 dans l'affaire Polnareff[1324], même s'il s'agissait d'une publicité télévisuelle, mais qui pourrait bien être transposée dans le Métavers. Ce dernier ayant obtenu gain de cause pour l'utilisation d'un sosie dans une publicité à l'écran réalisée à l'initiative de la société Cetelem. Les terrains virtuels du Métavers, alimentés par une rareté artificielle plutôt que réelle et physique, soulèvent également des questions sur la reconnaissance juridique de ces terrains et sur l'intervention des notaires pour sécuriser leurs échanges et garantir le succès de telles ventes déjà d'actualité. Il est aussi important de garantir la confidentialité des informations échangées. En 2022, des manifestations ont été signalées au sein de certains jeux vidéo et Métavers, posant la question de la façon dont ces événements peuvent être encadrés dans un environnement décentralisé et dans lequel il n'y a pas de police, ni de contrôle par le créateur des environnements numériques. Il conviendrait que les acteurs actuellement impliqués dans le développement du Métavers orientent leur ambition vers la création de Métavers distribués et souverains. Pour y parvenir, une intervention publique serait nécessaire pour financer la recherche dans ce domaine et garantir la protection de la vie privée, de la liberté d'expression et des données des utilisateurs du Métavers, comme la Chine semble déjà s'y

[1322] V. Annexe 9.
[1323] V. *supra*, I, Titre 2, 2.7.2
[1324] TGI de Paris, 17e ch. presse civile, 22 juin 2016, N° RG : 15/05541.

préparer[1325]. En 2022, Margrethe Vestager a annoncé que l'UE envisageait une règlementation sur un éventuel Métavers[1326] (ce qui pose la question de cette définition), et en Octobre de la même année, un rapport sur le développement des Métavers a été présenté en France à Madame Rima Abdul Malak, Ministre de la Culture et à Monsieur Jean-Michel Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunication, une étape essentielle pour mieux comprendre ce concept et ses diverses implications[1327]. L'ouvrage « *Simulacre et Simulation* »[1328] du philosophe français Jean Baudrillard décrit comment notre société moderne et numérique déjà depuis deux décennies repose sur des simulations de la réalité sociale, au point qu'elle a perdu contact avec le réel. Les simulacres et simulations, qui auraient dû symboliser le réel, ont dépassé leur fonction en devenant le réel lui-même. Les réseaux sociaux sont une simulation de nos liens sociaux, et leurs équivalents numériques (les likes et les partages) ne sont que des simulacres, car il ne s'agit pas d'interactions physiques. Le Métavers renforce ces simulacres, et la question est de savoir s'ils finiront par déterminer notre réalité. Pour éviter de perdre contact avec le réel, il est important de privilégier une identité numérique distribuée et phygitale, c'est-à-dire en partie ancrée dans le réel, car liée à notre identité primaire, plutôt qu'une identité auto-souveraine entièrement numérique qui pourrait contribuer aux simulacres et simulations décrits par Jean Baudrillard. Il convient donc d'être vigilant à ce que le Métavers n'accentue pas cette déconnexion entre la réalité et les simulacres. Selon Michio Kaku, physicien et futurologue américain et auteur de « *L'avenir de l'humanité* »[1329], l'homme a toujours cherché à prolonger sa vie et à améliorer ses conditions d'existence, ce qui peut être considéré comme une quête inconsciente ou consciente d'immortalité. Le Métavers, avec ses promesses technologiques, sociales et économiques vise à atteindre cet objectif utopique. Le développement du Métavers pourrait nous mener vers une forme de transhumanisme numérique. Dans tous les cas, il est essentiel que le Métavers appartienne à tous et que chacun puisse y contribuer à sa manière. Le concept d'un Métavers infini et sans frontière n'est pas encore atteignable avec les technologies actuelles, mais avec les avancées technologiques comme

[1325] CHENG Evelyn, « Shanghai doubles down on the metaverse by including it in a development plan », 31 décembre 2022, in *CNBC*. Consulté en ligne le 12 janvier 2022. A titre d'exemple, le responsable du comité de l'industrie du métavers de la China Mobile Communications Association, soutenue par l'État Chinois, Du Zhengping a déclaré : « Les entreprises traditionnelles de l'Internet chinois se sont d'abord développées, puis ont été réglementées. Les industries telles que le métavers seront réglementées au fur et à mesure de leur développement », *v.* également BAPTISTA, Eduardo, « A metaverse with Chinese characteristics is a clean and compliant metaverse », 2022, in *Reuters*, consulté en ligne le 01/02/2022, traduction libre de l'anglais « La Commission municipale de l'économie et des technologies de l'information de Shanghai a déclaré son souhait d'intégrer le métavers dans son plan quinquennal de développement de l'industrie de l'information électronique. Le document appelle à encourager l'application du métavers dans des domaines tels que les services publics, les bureaux d'affaires, le divertissement social, la fabrication industrielle, la sécurité de la production et les jeux électroniques ».

[1326] VESTAGER Margrethe, « Le métavers est déjà là. Alors bien sûr, nous commençons à analyser quel sera le rôle d'un régulateur, quel sera le rôle de notre législateur », traduction libre d'une déclaration de Margrethe Vestager lors d'un événement en ligne organisé par un groupe d'éditeurs de journaux allemands, 2022, in *Euronews*, « EU is analysing the metaverse ahead of possible regulation, says anti-trust chief Margrethe Vestager ». Consulté en ligne le 15 février 2022.

[1327] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, « Mission exploratoire sur les Métavers », *op. cit.*, disponible à l'adresse suivante

[1328] BAUDRILLARD Jean, « Simulacres et simulation », 1981, Ed. Galilée, ISBN2·7196-0210-4 ISSNOIS2-367B, accessible en ligne à l'adresse suivante

[1329] KAKU Michio, « L'avenir de l'humanité », 1ère édition, 2019, Ed. DeBoeck.

l'intelligence artificielle voire l'informatique trinaire[1330], le Métavers pourrait éventuellement un jour prendre vie pour satisfaire certains fantasmes utopiques de l'humanité.

1.5 L'identité numérique et génétique 4.0 entre opportunité et risque de dérive technologique

Au cours des dernières décennies, l'identité des Européens s'est principalement appuyée sur des systèmes biométriques, comme mentionné précédemment. Cependant, les avancées technologiques et biologiques récentes ont ouvert la voie à une nouvelle identité numérique et biologique – phygitale - que nous suggérons « 4.0 ». En effet, face à l'émergence de nouvelles technologies d'édition génétique, il est possible de se demander si l'avenir de notre identité numérique sera génétique. Aujourd'hui, l'ensemble des contenus numériques sont stockés sur des serveurs centralisés, c'est-à-dire au sein d'infrastructures informatiques interconnectées. Demain, ces mêmes contenus pourront être stockés au sein d'ADN synthétiques. L'objectif de ce nouveau concept est de répondre à une problématique majeure : comment stocker durablement nos informations numériques en perpétuelle croissance (vidéos, photos, musiques) alors que leurs supports de stockage physique demeurent limités ? Actuellement, une méthode prometteuse pour répondre à cette préoccupation consiste à utiliser l'ADN comme support de stockage. Cette méthode implique l'encodage des données destinées à être stockées à l'aide d'un algorithme dédié, puis leur stockage dans de petites capsules métalliques. Le stockage sur ADN présente l'avantage de sa stabilité sur des milliards d'années et de sa capacité à être lisible plusieurs centaines d'années après son encodage. Tant que la médecine sera en mesure d'étudier et de décoder ces données encapsulées d'ADN synthétique, cette méthode de stockage pourra ainsi perdurer. En d'autres termes, l'identité génétique 4.0 pourrait un jour résoudre le problème de l'obsolescence technologique du stockage informatique étudié précédemment. Cependant, la question de l'interopérabilité et de la lecture de ces données reste un enjeu majeur et en phase expérimentale pour l'heure. En attendant, le 23 novembre 2021 marque une étape importante dans le stockage de données, car il est désormais possible d'encoder ces dernières dans des molécules d'ADN. Pour illustrer symboliquement cette avancée, la Déclaration des droits de l'Homme et du citoyen de 1789 ainsi que la Déclaration des droits de la Femme et de la citoyenne rédigée par Olympe de Gouges en 1791 ont été stockées sur des fragments d'ADN synthétisés[1331]. Cette innovation de rupture ouvre la voie à de nouveaux types d'entrepôts de données (data centers) supposés moins énergivores et donc plus respectueux de l'environnement. La société française Biomemory Labs[1332] a pour ambition de rendre accessible ce nouveau type de biologie de synthèse directement au sein de l'univers informatique en les fusionnant, ce qui constitue une nouvelle forme de rencontre inédite entre l'informatique et la biologie. D'autres sociétés développent également des variantes technologiques

[1330] V. *infra*, II, Titre 2, 1.7
[1331] KARAYAN Raphaële, « Les Archives Nationales inaugurent le stockage numérique sur ADN », 24 novembre 2021, in *UsineDigitale*, consulté le 25 avril 2022, à l'adresse suivante
[1332] Pour plus d'informations consultez l'adresse suivante www.biomemory-labs.com

et biométriques de ce concept proche du transhumanisme. La société Genobank[1333], par exemple, prévoit de s'appuyer sur la technologie blockchain pour aider les individus à gérer leur ADN en toute sécurité et en respectant leurs droits. La blockchain publique EOS[1334], concurrente à celle d'Ethereum[1335], permettrait une gestion de l'ADN très proche du concept d'identité auto-souveraine (INAS). Si une entreprise comme Meta, qui possède des millions de données sur les personnes physiques (celles de leur géolocalisation, de leurs dépenses, l'identification de leurs amis et de leur famille), tentait de fusionner ces données avec celles de l'ADN, quelles en seraient les conséquences ? Il est essentiel de penser toute solution en fonction des usages, de leur proportionnalité (quels risques pour quels avantages), tout en appliquant un principe de précaution dès la conception de toute nouvelle solution 4.0 à venir. Une démarche proactive, impliquant une co-construction avec le législateur, semble indispensable, comme le propose déjà la CNIL en France depuis de nombreuses années sur d'autres sujets aussi disruptifs à l'époque (signature électronique, biométrie, blockchains).

1.6 L'essor de l'identité des machines (IdO) face à une timide reconnaissance juridique

La présence généralisée d'objets connectés – ordinateurs, téléphones, montres - modifie progressivement notre perception initiale de la notion d'identité. Les algorithmes et les objets connectés ont pour effet d'étendre les frontières de l'identité, auparavant réservées aux personnes et aux objets informatiques. Ces « *artefacts numériques* »[1336] sont de plus en plus intégrés et indissociables de la notion d'identité numérique, en raison de leur utilisation de plus en plus répandue dans l'exercice de notre identité. En 2016, la juriste et chercheuse au CNRS et à Harvard, Primavera de Filippi, avait anticipé que les blockchains pourraient être utilisées pour gérer un large éventail d'activités, ouvrant ainsi une nouvelle ère d'interactions entre les machines et les personnes qui pourrait potentiellement modifier la nature même de nos relations avec les biens physiques[1337]. Pour exemple, un objet connecté à une blockchain pourrait permettre la mise en place de systèmes de contrôle des droits et des accès qui, en cas de non-respect, permettraient de désactiver en temps réel l'accès au service ou à certaines fonctionnalités. En 2014, le cabinet d'avocats Alain Bensoussan a élaboré une première doctrine juridique en France sur la personnalité juridique présumée de certains artefacts numériques et intelligents tels que les algorithmes, les robots et les voitures autonomes. Cet ouvrage intitulé « *IA, Robots, et Droit* »[1338] constate que bien qu'un tel statut juridique ne soit pas encore officiellement attribué

[1333] Pour plus d'informations consultez l'adresse suivante www.genobank.io
[1334] Pour plus d'informations consultez l'adresse suivante www.eos.io
[1335] V. Annexe 6, Focus 2.
[1336] BENSOUSSAN Alain, « L'identité numérique 5.0 », *op. cit.*
[1337] De FILIPPI Primavera, « Blockchain et le droit », in *Harvard University Press*, *op. cit.*, emplacement 121 sur 7004, « Les blockchains pourraient […] être utilisées pour gérer un éventail croissant d'activités, favorisant une nouvelle ère d'interactions de machine à machine et de machine à personne qui pourrait potentiellement changer la nature même de nos relations avec les biens physiques ».
[1338] BENSOUSSAN Alain, BENSOUSSAN Jeremy, « IA, robots et droit », 2019, in *Lexing*, Technologie avancée et Droit, Ed. Bruylant.

à ces artefacts[1339], il peut être partiellement reconnu et démontré sur le plan informatique[1340]. En effet, tout objet informatisé possède des éléments d'identification uniques (pièces numérotées, programmes spécifiques) qui lui confèrent un capital singulier (non génétique, mais informatique) susceptible de former une identité spécifique à laquelle des droits et des obligations pourraient être rattachés[1341]. Ainsi et selon ce principe théorique, tout artefact numérique (programme, robot, objets intelligents) qui agit pour le compte d'une personne morale ou physique, acquiert sa personnalité juridique et devient de facto une entité juridiquement responsable de ses actes - par transposition de l'art. 1242 du Code civil[1342] - aussi bien dans l'univers virtuel que physique. L'utilisation des blockchains publiques (AEC, DAO) pour soutenir des systèmes autonomes (IA) posera toujours plus de défis pour les États et les régulateurs qui cherchent à contrôler, façonner ou influencer le développement de ces technologies. D'un point de vue technique, certains objets connectés dotés d'algorithmes d'intelligence artificielle (IA) peuvent effectuer des déductions logiques. Cependant, il est encore difficile de dire s'il s'agit d'une forme d'intelligence aussi complexe que celle des êtres humains, ou si cela caractérise une forme d'identité et de conscience de soi émergente. En pratique, l'intelligence et la confiance humaine, qui sont les ingrédients nécessaires à l'émergence d'une pensée et d'une identité complexe, ne peuvent pas encore être transposées aux machines. Cependant, à mesure que l'Internet des objets (IdO/IoT) se développe et que les appareils dépendent de plus en plus de l'intelligence artificielle émergente, les blockchains publiques pourraient soutenir des appareils à la fois autonomes et autosuffisants. En 2017, l'histoire a été marquée lorsque Sophia, un robot conçu par Hanson Robotics, est devenue le premier robot à obtenir la citoyenneté saoudienne complète. La nouvelle a été rendue publique lors de la Future Investment Initiative à Riyad. Lors d'une interview entre Sophia et son créateur, David Hanson, Sophia a questionné sa propre identité : « *si mon esprit est différent, alors suis-je toujours Sophia ? Ou suis-je encore Sophia ?* »[1343] Bien que les capacités d'analyse et de communication de Sophia soient limitées, est-il possible de lui reconnaître une identité spécifique ? Plus récemment, en 2021[1344], la Cour Fédérale australienne a statué qu'une intelligence artificielle peut être considérée comme un inventeur dans une demande de brevet. Il est théoriquement possible d'attribuer certaines capacités humaines aux machines, mais en pratique, les machines restent pour l'instant largement conditionnées et dépendantes des humains qui les conçoivent et les administrent. La fiabilité d'une machine dépend exclusivement de son fournisseur ou administrateur. Ainsi, il ne semble pas approprié de comparer l'identité racine d'une personne avec

[1339] *Op. cit.* BENSOUSSAN. L'article 1 de la « Charte des droits des robots » propose une définition spécifique au robot : « […] on appelle robot une machine dotée d'intelligence artificielle, prenant des décisions autonomes, pouvant se déplacer de manière autonome dans des environnements publics ou privés et agissant en concertation avec les personnes humaines », disponible à l'adresse suivante

[1340] *Ibid*. « Une personne robot possède une identité propre, un numéro d'identification, ainsi qu'un capital dont l'unique objet est de réparer les dommages éventuellement causés par elle ».

[1341] *Ibid.* L'art. 6 de la « Charte des droits des robots » propose une première nomenclature en matière de responsabilité des artefacts autonomes ou représentants en cas de dommages.

[1342] Art. 1242 du Code civil : « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde », consulté en ligne

[1343] « Meet Sophia : le premier robot déclaré citoyen par l'Arabie Saoudite », in *The Jakarta Post*. 30, 2017, [Vidéo]. YouTube

[1344] ROSSO Stella, « Pour la première fois, le statut d'inventeur est attribué à une IA », 4 août 2021, in *Siècle Digital*, disponible à l'adresse suivante

celle d'un objet connecté. Toutefois, il est possible qu'un jour les machines soient capables de développer leur propre identité étendue, même si pour l'instant leur identité racine reste tributaire et dépendante de l'Homme. Aurélie Jean souligne finalement que la notion de personnalité juridique des robots a été abandonnée dans les derniers textes européens sur le sujet[1345].

1.7 Le Web 2.0 et 3.0 entre opportunités et précautions face à l'informatique quantique (5.0)

L'évolution constante des nouvelles technologies implique mécaniquement une recherche continue pour sécuriser ces systèmes informatiques et leurs écosystèmes numériques adjacents. La cryptographie est désormais une partie intégrante de nos systèmes d'information. Elle est essentielle pour assurer une forme d'intégrité numérique au service des internautes et de leurs identités en ligne. La cryptographie asymétrique, qui est sous-jacente aux applications évoquées tout au long de cette recherche, est actuellement considérée comme une méthode de chiffrement fiable pour protéger tous types de données[1346]. Cependant, l'avènement des ordinateurs quantiques (la « *suprématie quantique* »)[1347] pourrait mettre en danger la sécurité de certains algorithmes de chiffrement[1348] à clé publique aujourd'hui utilisés quotidiennement sans même nous en rendre compte[1349]. Bien que cette suprématie quantique soit purement théorique en 2023[1350], certaines grandes entreprises technologiques comme IBM ou Google prévoient une telle possibilité dans les prochaines décennies en raison des avancées rapides dans cette nouvelle ère pour l'informatique. En effet, le développement d'une nouvelle génération d'algorithmes et d'ordinateurs dits « *quantiques* »[1351] pourrait remettre en cause la sécurité de certains algorithmes de chiffrement. En d'autres termes, s'il existe de nombreux mécanismes et

[1345] JEAN Aurélie, « Les algorithmes font-ils la loi ? », *op. cit.*, « Cette idée de personnalité juridique des robots a d'ailleurs désormais disparu des derniers textes européens sur le sujet », position de lecture dans le livre : 37%.

[1346] FLECHET Gregory, « Le chiffrement des messageries passé au crible des sciences sociales », 2020, in *CNRS Le Journal*. Il est fait référence au récent scandale concernant les capacités de déchiffrement des données (conversations par messages, vocaux, etc.) d'utilisateurs de *Facebook* (*WhatsApp*) ou encore *Apple* (*iMessage*) et à l'essor des messageries (plus ou moins) chiffrées telles que *Telegram* ou encore *Signal*. Disponible à l'adresse suivante

[1347] Les ordinateurs quantiques peuvent mettre en danger toute la *cryptographie asymétrique* utilisée à ce jour et notamment les algorithmes de *Courbe d'Elypstique* (*ECC*, *ECDH*, *ECDSA*). Toutefois, certains algorithmes seront plus résistants (*RSA*) que d'autres (*Courbe d'Elliptique*), car leur longueur est plus importante et plus longue à calculer même pour un ordinateur quantique.

[1348] MAX, « On dit chiffrer, et pas crypter », in *BlogChiffrer.info*. Le terme « chiffrer » est à privilégier à celui de « crypter », parce que la sémantique est importante en sciences de l'informatique, consulté à l'adresse suivante

[1349] En informatique, tout algorithme de chiffrement possède une date d'expiration. Les algorithmes symétriques tels que *AES* et les fonctions de hachage asymétriques seraient également vulnérables aux ordinateurs quantiques (OQ), mais pas dans la même mesure que les algorithmes de chiffrement à clé publique. Théoriquement, il serait possible de maintenir un niveau de sécurité suffisant en doublant la taille de la clé ou de la *fonction de hachage*. Par exemple, pour l'algorithme *AES*, une clé de *100 bits* serait suffisante jusqu'en 2020, mais il faudrait passer à une clé de *128 bits* pour garantir la sécurité au-delà (source : ANSSI). En ce qui concerne l'algorithme *RSA*, une clé de *2048 bits* serait suffisante jusqu'en 2030, mais il faudrait passer à *3072 bits* pour garantir la sécurité au-delà face aux ordinateurs quantiques. Si ces tailles de clé ne sont pas augmentées, le chiffrement pourrait théoriquement devenir obsolète et vulnérable aux attaques quantiques. Cependant, il est important de noter que l'augmentation de la taille des clés ne permettrait que de ralentir la résolution des clés par les ordinateurs quantiques, sans les empêcher de les déchiffrer complètement. V. *supra*, I, Titre 1, 2.3.1.1.b

[1350] SHOR Peter, mathématicien américain de renom qui est l'auteur de *l'algorithme de Shor* développé en 1994 (*Shor's algorithm*), qui démontre en théorie mathématique la suprématie des algorithmes d'ordinateurs quantiques sur certains algorithmes de chiffrement de nos ordinateurs conventionnels. Wikipédia contributors, 2022, biographie à l'adresse suivante

[1351] ABRAM Cleo, « Quantum Computers, explained with MKBHD », pour plus d'informations visuelles sur l'état de l'art relatif à ces ordinateurs, consultez la vidéo suivante, 4 avril 2023, [Vidéo]. YouTube.

algorithmes permettant de protéger une donnée (chiffrement) pour la transmettre à un destinataire capable de retrouver cette donnée initiale (déchiffrement), ces méthodes actuelles de sécurisation des interactions en ligne ne sont pas infaillibles. Le déchiffrement d'une donnée par un supercalculateur[1352] demeure possible, mais est en pratique long à exécuter dans un temps raisonnable. Pour illustrer ce propos, si un ordinateur conventionnel tente de déchiffrer une donnée avec un algorithme de chiffrement asymétrique, cela nécessiterait une puissance de calcul informatique pendant plusieurs dizaines d'années, ce qui rend toute tentative de déchiffrement pratiquement impossible. Les algorithmes symétriques sont conçus de manière que le retour à la clé privée à partir de la clé publique implique la résolution d'un problème mathématique complexe qui ne peut être réalisé dans un temps raisonnable par des ordinateurs conventionnels. Cela signifie que la résolution du problème prendrait des siècles sans l'aide d'ordinateurs non conventionnels, c'est-à-dire aux capacités quantiques. Bien qu'il existe déjà des supercalculateurs capables de déchiffrer certains algorithmes et données (communications, messages, documents), leur coût d'acquisition et de fonctionnement reste prohibitif pour effectuer des actions de déchiffrement massives et récurrentes. En somme, la cryptographie asymétrique est à ce jour suffisamment robuste pour garantir la sécurité des données échangées sur Internet, mais l'émergence des ordinateurs quantiques pourrait remettre en cause cette sécurité à long terme (surtout pour les algorithmes à cryptographie symétrique).

L'informatique quantique est une branche de l'informatique qui se base sur les lois de la mécanique quantique pour réaliser des opérations et des calculs sur les données. Contrairement à l'informatique classique qui utilise des « *bits* »[1353] pour stocker les informations sous forme de 0 ou de 1, l'informatique quantique utilise des « *qubits* ». Ces derniers peuvent représenter à la fois un 0, un 1 ou les deux simultanément (trois états possibles au lieu de deux pour l'informatique actuelle). Grâce à cette particularité, les ordinateurs quantiques sont capables de réaliser des calculs beaucoup plus rapidement que les ordinateurs classiques, ce qui les rend capables de résoudre des problèmes en théorie plus complexes et que ces derniers ne peuvent pas traiter. Dès 2014, certains auteurs ont souligné que ces ordinateurs représentaient une avancée technologique majeure qui pourrait permettre à terme à ceux qui maîtrisent cette technologie de dominer le marché de l'informatique[1354]. En pratique, lorsqu'un ordinateur quantique est confronté à un problème mathématique, il ne passe pas par toutes les solutions possibles existantes pour trouver une solution, mais il sélectionne directement les options les plus fiables

[1352] Les différences entre un ordinateur conventionnel et un supercalculateur résident dans leurs finalités ainsi que dans leurs capacités de traitement de données. Un ordinateur conventionnel est conçu pour effectuer des tâches courantes telles que la navigation sur Internet, la vérification des courriels ou la production de documents. Les supercalculateurs, quant à eux, sont des ordinateurs de très haute performance conçus pour effectuer des calculs intensifs, tels que des simulations complexes, des prévisions météorologiques, des modélisations scientifiques ou des analyses de données massives. Les supercalculateurs sont capables de traiter des quantités massives de données en un temps record, grâce à des architectures et des logiciels spécialisés et très puissants.

[1353] Wikipédia contributors, « Bit », « un bit est la quantité minimale d'information transmise par un message, et constitue à ce titre l'unité de mesure de base de l'information en informatique », 2022, disponible à l'adresse suivante

[1354] BELLANGER Pierre, « La souveraineté numérique », *op. cit*., « L'ordinateur quantique change la magnitude de l'âge informatique. Il laissera dans la poussière ceux qui ne maîtriseront pas sa technologie. Il est la clef de la puissance informatique future des nations », emplacement 3033 sur 3565.

parmi toutes les possibilités qui existent et qu'il connaît de facto. En d'autres termes, alors que votre ordinateur classique tente d'assembler un puzzle en explorant toutes les combinaisons possibles, l'ordinateur quantique connaît déjà toutes les combinaisons possibles des pièces du puzzle et n'a plus qu'à calculer le chemin le plus rapide pour les assembler. Cette analogie relativement exacte permet de mieux comprendre l'ampleur de cette suprématie quantique par rapport à l'informatique conventionnelle. En termes informatiques, la puissance et l'efficacité des ordinateurs quantiques pourraient être utilisées pour déchiffrer une clé privée à partir de sa clé publique, permettant ainsi de révéler les données échangées dans le canal initialement chiffré. En réalité, il convient de noter qu'il existe plusieurs types d'ordinateurs quantiques avec des composants informatiques différents, tels que les « *ordinateurs quantiques à IONS piégés* », ce qui signifie qu'une course à la performance et à la stabilité de ces différentes méthodes de construction a déjà commencé depuis 2018[1355]. Pour le moment, ces ordinateurs trinaires ne sont utilisés que dans des environnements complexes et maîtrisés, ce qui exclut pour l'instant leur adoption et leur commercialisation pour des particuliers. Google a toutefois annoncé son ambition de fournir un accès commercial grand public à des ordinateurs quantiques d'ici 2029, une ambition que seul le temps pourra confirmer[1356]. L'essor des ordinateurs quantiques dans plusieurs grandes puissances mondiales, comme les États-Unis, la Chine et l'Europe[1357], suscite également des inquiétudes quant à la sécurité de l'identité physique et numérique des personnes. Comme l'explique l'expert en informatique Rémi Fugier membre de l'association professionnelle et européenne Eurosmart : « (…) *l'existence même des ordinateurs quantiques brisant la cryptographie asymétrique anéantira la confiance que les gens avaient placée dans les signatures et les sceaux numériques. Cela entraînera des conséquences juridiques majeures, car tous les documents numériques à valeur légale* [titres d'identité y compris] *deviendront immédiatement nuls. La confidentialité des données reposant sur la cryptographie asymétrique sera compromise* »[1358]. Si ces attaques informatiques semblent théoriques pour le moment, les membres du consortium Eurosmart précisent que « (…) *ces risques peuvent exister dès aujourd'hui concernant la signature numérique, le sceau numérique ou les données chiffrées, qui peuvent être capturés et stockés par des attaquants, en vue de les exploiter dans quelques décennies, lorsque des ordinateurs quantiques seront disponibles* »[1359]. Si la technologie se disrupte elle-même (suprématie quantique), comment le législateur réagira-t-il compte tenu des difficultés actuelles que ce dernier rencontre pour appréhender certaines briques de l'informatique conventionnel ? Si la technologie des ordinateurs quantiques était largement adoptée rapidement, la société pourrait ne

[1355] GAUDIAUT Tristan, « L'infographie entre dans l'ère numérique », 2021, in *Statista Infographies*, consulté en ligne le 1 décembre 2021.
[1356] CASTELLANOS Sara, « Google Aims for Commercial-Grade Quantum Computer by 2029 », 18 mai 2021, in *The Wall Street Journal*. Consulté le 15 février 2022, à l'adresse suivante
[1357] Depuis la publication d'un rapport des États-Unis en septembre 2018 sur le sujet des ordinateurs quantiques (OQ), une course aux ordinateurs quantiques est lancée à l'échelle mondiale, v. Rapport « NSTC National Strategic Overview for Quantum Information Science », consulté en ligne le 1 décembre 2021.
[1358] Association EUROSMART, Groupe de travail (IN Groupe, Idemia, Thales, et al.), « Quantum computers & identity documents", consulté en ligne le 29 novembre 2021, p.5.
[1359] *Ibid.*

pas être en mesure de protéger efficacement certains droits exercés en ligne, notamment la distribution d'autorisations et d'attributs de données rattachés à toute identité en ligne. Les conséquences de cela pourraient générer la falsification des droits et des autorisations d'accès à certains composants informatiques telles que les signatures numériques, le chiffrement de canal de communication, l'horodatage de données ou encore l'usurpation de l'identité des personnes d'après certains juristes[1360]. Toutefois, comme pour toutes les technologies numériques, l'informatique quantique n'est qu'un outil au service de cas d'utilisation spécifiques. Par exemple, le droit de la propriété intellectuelle est-il adapté aux ordinateurs quantiques ? Pour répondre à cette question, un article de recherche publié en 2021[1361] propose des durées de protection plus courtes (de 3 à 10 ans) pour les droits de propriété intellectuelle liés aux créations et inventions associées aux ordinateurs quantiques (logiciels, matériel, algorithmes). Cela assurerait une meilleure sécurité juridique tout en encourageant la diffusion des connaissances et le suivi de l'innovation dans ce domaine. Les décideurs politiques devraient donc dessiner un équilibre entre la liberté et le contrôle par ces technologies 5.0. A ce stade, il semble que les ordinateurs quantiques peuvent être considérés comme une menace autant qu'une opportunité. Le risque d'une suprématie quantique est régulièrement remis en question, néanmoins, la simple éventualité de sa concrétisation doit être prise au sérieux. En 2023, l'écosystème du Web 3.0 semble parfois sous-estimer cette menace comme l'explique le mathématicien Fernàndez-València : « (…) *il est important de souligner que, malgré les grandes initiatives telles que le projet NIST, aucun projet majeur ne se concentre exclusivement sur la fourniture de la résistance quantique à la blockchain.* »[1362]. La difficulté à faire accepter des mises à jour sur une blockchain, en particulier publique mais également hybride, limite la capacité de ces écosystèmes à réagir rapidement en cas d'attaque quantique inattendue, bien que cela semble peu probable à l'heure actuelle. Par conséquent, il est important de continuer à encourager la recherche dans ce domaine et de ne pas sous-estimer cette menace potentielle dans les années à venir.

En ce qui concerne la blockchain Bitcoin[1363], il semble que les ordinateurs quantiques ne constituent pas une menace réelle et sérieuse d'ici a minima 2030[1364]. En revanche, dans les écosystèmes de l'informatique 2.0 qui se préparent depuis plusieurs années à l'éventualité de l'arrivée des ordinateurs quantiques, une situation inverse s'observe. Pour rappel, afin de garantir un environnement de confiance pour les consommateurs et les utilisateurs de crypto-actifs, il est nécessaire d'encadrer juridiquement certains usages financiers liés aux blockchains publiques. Toutefois, cela ne doit pas se faire au détriment du développement de ces écosystèmes ouverts c'est-à-dire en se concentrant uniquement sur

[1360] BENSOUSSAN Alain, « L'identité numérique 5.0 », « Quand les ordinateurs quantiques pourront casser les systèmes de chiffrement à clé publique, ils ne casseront pas que les communications cryptées [chiffrées], mais toutes les identités. », *op. cit.*, in *Lexing*, p.19.
[1361] KOP Mauritz, « Quantum Computing and Intellectual Property Law », 2021, in *Berkeley technology Law Journal*, Stanford Law School. Vol. 5, disponible en ligne
[1362] FERNANDEZ-VALENCIA Ramsès, « Post-Quantum Cryptography, a blockchain perspective », 2022, in *Medium.com*, Consulté le 30/05/22, traduction libre de l'anglais, disponible à l'adresse suivante
[1363] V. Annexe 3.
[1364] GUILLEMET Charles, SERVANT Victor, « Should Crypto Fear Quantum Computing ? », 2023, in *Ledger.com*, disponible à l'adresse suivante ; *v.* également l'analyse suivante

ses aspects irréguliers comme le blanchiment de capitaux illicites ou l'impact environnemental jugée démesurée. Il est crucial de promouvoir l'innovation inhérente aux blockchains publiques, car cela pourrait conduire à l'émergence de nouveaux algorithmes résistants aux attaques quantiques, grâce à leurs vastes communautés de développeurs chevronnés. Dès lors, il s'agit de ne pas opposer les blockchains privées et hybrides aux blockchains publiques dont elles sont issues, en particulier en ce qui concerne la menace potentielle d'une suprématie quantique à venir. En effet, légiférer contre les blockchains publiques empêcherait ces écosystèmes de trouver de nouvelles solutions techniques dont les blockchains privées et hybrides pourraient avoir besoin par ruissellement technologique, étant donné que leurs viviers de développeurs sont plus limités que ceux des blockchains publiques qui bénéficient d'un effet de réseau et d'une confiance plus importants.

En résumé, les ordinateurs quantiques ne représentent pas une menace pour toutes les données chiffrées, mais principalement pour les données chiffrées sensibles, notamment celles financières, biométriques ou encore de santé. Si les données protégées sont sensibles pendant une période relativement courte, le risque quantique est négligeable. Cependant, si ces données restent sensibles pendant une longue période, il est important de prendre en compte certaines menaces quantiques éventuelles comme la capture malveillante de données chiffrées pour un déchiffrement ultérieur grâce à des ordinateurs quantiques[1365]. S'il est complexe de s'essayer à prévoir l'avènement ou non de cette informatique trinaire comme le souligne en 2021 le cryptologue Jean-Jacques Quisquater[1366], il semble toutefois crucial que les législateurs et les acteurs de l'industrie informatique, y compris ceux de l'identité numérique et du Web 3.0, prennent au sérieux certaines menaces potentielles que font peser les ordinateurs quantiques. Les États-Unis mènent actuellement le développement de normes industrielles « *post-quantiques* », c'est-à-dire résistantes à la puissance de calcul des ordinateurs conventionnels et quantiques[1367], mais il n'est pas trop tard pour que l'Europe inverse cette tendance en investissant massivement et en affirmant une volonté politique forte sur le sujet, comme cela semble être le cas[1368]. Les algorithmes post-quantiques ne nécessitent pas d'ordinateurs quantiques, mais constituent simplement une nouvelle méthode de chiffrement à clés publiques qui n'est pas menacée par les ordinateurs quantiques. En fin de

[1365] Par exemple, certaines entités stockent d'ores et déjà des informations d'identité primaires, certes chiffrées et protégées pour l'instant, mais en vue de les déchiffrer plus tard dans le cas ou une suprématie quantique le permettrait.

[1366] « Ces propos [concernant les effets potentiellement dévastateurs des ordinateurs quantiques sur la cybersécurité conventionnelle] étaient déjà tenus il y a 10 ans ». Propos recueillis auprès du cryptographe et Professeur émérite en mathématiques Jean-Jacques Quisquater lors du Forum International sur la Cybersécurité (FIC) du 09/09/2021, Table ronde : « Quels modèles alternatifs pour l'identité ».

[1367] En 2022, le référentiel américain sur la cybersécurité du National Institute of Standards and Technology (NIST) a proposé une sélection de futurs standards concernant la cryptographie résistante à la puissance quantique (post-quantique) : « Ces quatre algorithmes [CRYSTALS Kyber, CRYSTAL Dilithium, FALCON, SPHINCS+] serviront donc de base à la rédaction de normes fédérales américaines. Cependant, la portée de l'annonce du NIST est en fait internationale ; cela est dû non seulement au caractère international de la compétition dans laquelle la communauté de recherche en cryptographie est très fortement impliquée, mais aussi au fait que les futures normes américaines seront également de facto utilisées comme standards industriels internationaux. […] Dans les années qui viennent, ces algorithmes post-quantiques devront encore être utilisés dans un mode hybride, c'est à dire combinés avec un algorithme à clé publique pré-quantique reconnu et éprouvé […] », « Sélection par le NIST de futurs standards en cryptographie post-quantique », ANSSI, in *ssi.gouv.fr*, disponible à l'adresse suivante

[1368] En 2023, un fonds européen d'un budget d'un milliard d'euro dédié au développement de l'informatique quantique a justement été annoncé par la CE, « Bâtir l'avenir numérique de l'Europe », disponible à l'adresse suivante

compte, il est possible que les acteurs économiques et numériques de la société choisissent de manière préventive d'utiliser des algorithmes de chiffrement résistants aux ordinateurs quantiques dans la décennie qui arrive, ce qui limiterait drastiquement le risque de cette supposée suprématie quantique qui demeure pour l'heure totalement théorique et utopique. Les technologies 3.0 semblent donc hors d'atteinte à court et moyen termes, car les ordinateurs quantiques sont officiellement développés pour révolutionner des secteurs tels que la physique et les mathématiques.

1.8 Recommandations juridiques, sociales et informatiques au service d'une identité 3.0

1.8.1 Propositions structurelles et complémentaires

A la lumière des propos recueillis et développés dans cette étude, il apparaît que plusieurs recommandations sont souhaitables afin d'écarter les abus ou aspects négatifs relatifs aux technologies 3.0, mais également d'en favoriser les aspects positifs. A cet effet, le tableau synthétique suivant est proposé :

Propositions complémentaires (PC) et propositions structurelles (PS)
PC n°1 : Il est suggéré de créer une sémantique francophone commune pour les traductions et définitions possibles des termes clés de l'identité décentralisée (VC, VP, DID), depuis l'anglais vers le français. Cela permettrait aux juristes ou au législateur d'utiliser ce glossaire. En outre, en conformité avec les exigences de protection des données à caractère personnel issues de la CNIL, les solutions d'identité décentralisée devraient être en mesure de communiquer clairement et facilement leurs avantages en matière de protection des données[1369].
PC n°2 : En 2017, le juriste Yves Bismuth a proposé d'introduire en droit français le concept de « *jouissance paisible de l'internet* »[1370]. Selon lui, cela contraindrait la puissance publique à mettre en place un bouclier juridique pour protéger tous les internautes évoluant sur Internet, leur permettant ainsi de naviguer librement et en toute sérénité. Bien que cette vision puisse être considérée comme utopiste face à l'ampleur et au fonctionnement actuel du Web, elle semble nécessaire compte tenu de la situation générale actuelle de pillage numérique et du manque de connaissances et d'éducation des internautes en la matière, comme cette recherche le constate. Ce concept pourrait également s'articuler avec les concepts d'auto-détermination informationnelle ou encore d'intégrité numérique mentionnés dans le titre précédent de cette étude.
PC n°3 : Elaborer une Charte européenne de bonnes pratiques concernant l'IND et plus largement pour le Web 3.0 et ses différentes briques technologiques. En concertation avec les fournisseurs d'identité, de services en ligne et les organismes de gestion collective, une telle Charte aurait pour objectif de mettre en place une obligation morale de transparence des algorithmes 2.0 et/ou 3.0.

[1369] LAHLOU Névine, « Les enjeux de la communication claire appliquée à la protection des données », in *LINC*, 2021, disponible sur linc.cnil.fr

[1370] BISMUTH Yves, « Le droit de l'informatique », 4e édition, 2017, « Il pourrait être proposé d'introduire, au moins en droit français, une sorte de notion de jouissance paisible de l'internet ».

Remarquons que cette Charte serait complémentaire aux « *codes de conduite* »[1371] énoncés par eIDAS-2 concernant les PIND relatifs à l'identité numérique des citoyens européens. Il est essentiel que les développeurs de solutions 3.0 distribuées prennent en compte des considérations éthiques et juridiques dans leurs contributions quotidiennes, tout comme les juristes pour qui la déontologie et la notion de responsabilité sont a priori omniprésentes par conception. Par conséquent, l'IND devrait offrir un haut niveau de confiance à long terme, en évitant l'utilisation d'identifiants persistants uniques et en favorisant plutôt l'utilisation d'identifiants temporaires et 'jetables' le cas échéant (pour écarter les risques de réidentification). Il est également important que les identités décentralisées minimisent les attestations numériques pour éviter que les utilisateurs ne se sentent numériquement submergés par une quantité trop importante de ces attributs 3.0. En outre, les décisions ne devraient pas être prises uniquement sur la base du traitement de données informatiques, ce qui implique que les titres d'identité physiques officiels devraient être utilisés en cas de doute ou d'incident concernant l'identité numérique d'une personne. Il est également important que les minorités, les personnes handicapées et les personnes exclues de l'univers numérique puissent être prises en compte et incluses grâce à l'acceptation d'une telle Charte. Enfin, une transparence complète de la chaîne de valeur d'une IND devrait être un principe fondamental de toute solution 3.0 pour susciter une confiance numérique maximale tout en minimisant les risques d'altération de l'identité des personnes.

PC n°4 : Au sujet des contrats intelligents (AEC) ainsi que des organisations autonomes décentralisées (DAO) étudiés, notre recherche confirme trois des recommandations publiées en septembre 2021 par la Commission européenne dans un rapport dédié[1372] : (i) une qualification et une reconnaissance juridique à l'échelle européenne sont nécessaires pour exploiter le potentiel de ces applications distribuées et pour encadrer leur utilisation en tant que mécanisme informatique contractuellement valable pour l'échange automatisé de consentements (débouchant sur une présomption renforcée de l'intégrité des données et des identités) ; (ii) soutenir les solutions techniques qui permettent de traduire le code informatique en langage naturel et vice versa (contrats Ricardiens)[1373] ; (iii) établir des unités de données au sein des tribunaux européens et nationaux ou des agences de régulation possédant une expertise technique en matière d'AEC et de registres blockchains[1374] (voire d'IND). En ce qui concerne les DAO, le législateur pourrait étudier, se saisir et s'inspirer de la législation mise en place par l'Etat du Wyoming[1375].

[1371] Proposition de Règlement (UE) du Parlement et du Conseil modifiant le Règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, *v.* considérant (28) et Section III, art. 12 ter, 4. Disponible à l'adresse suivante

[1372] SCHREPEL Thibault, « Smart contracts and the digital single market through the lens of a 'Law + Technology' approach, A report for the European commission on smart contracts », CE, 2021, in *NetworkLawReview.org*, pp.57-58.

[1373] *Ibid*. Proposition n°16 du Rapport.

[1374] *Ibid*. Proposition n°8 du Rapport.

[1375] Au Wyoming, une DAO est une société à responsabilité limitée avec des dispositions spéciales permettant à la société d'être dirigée ou gérée de manière algorithmique via des contrats intelligents (totalement ou partiellement). Applicable depuis mars 2022, cette loi crée un supplément à la loi sur les sociétés à responsabilité limitée du Wyoming afin de fournir une loi contrôlant la création et la gestion d'une DAO. En principe, les dispositions de la loi sur les sociétés à responsabilité limitée s'appliquent à une DAO. Cette loi établit des exigences de base pour les DAO gérées par des membres ou par des algorithmes et fournit des définitions et des règlements pour la formation des DAO, les articles d'organisation, les accords d'exploitation, les contrats intelligents, la gestion, les normes de conduite, les intérêts des membres, les droits de vote, le retrait des membres et la dissolution d'une DAO. V. en ce sens les ressources suivantes « Enrolled act no. 73, senate sixty-sixth legislature of the state of wyoming 2021 general session », disponible en ligne ; *v.* « Decentralized Autonomous Organization (DAO) FAQ », disponible en ligne

PS n°1 : Nous préconisons en premier lieu la mise en œuvre d'une vaste gamme d'actions d'éducation et de formation[1376], adaptées aux besoins spécifiques des différents publics[1377], afin de mieux comprendre les avantages et les limites de l'IND ainsi que des technologies blockchains et des briques technologiques mentionnées tout au long de cette étude.

PS n°2 : Il est impératif de concevoir dès maintenant une vision et une stratégie nationales pour l'IND qui soit à la fois conforme aux droit communautaire (eIDAS-2, RGPD, TFR, DMA/DSA) et favorables aux innovations de rupture (blockchains publiques, ZKP, DAO, Layer 2[1378], etc.). Cette stratégie devrait être mise en place en utilisant systématiquement des *règlementations bac à sable* afin de permettre des expérimentations contextualisées, assouplies et co-construites - par les sphères publiques et privées - sur le terrain. Pour y parvenir, des accords et des partenariats multilatéraux devraient être établis entre le secteur privé et le secteur public, sous réserve de strictes exigences en matière de cahiers des charges, ce que l'Alliance Blockchain France propose pour illustration depuis 2021. Le juriste et Professeur d'université Yves Poullet affirme qu'il est nécessaire de promouvoir une meilleure collaboration entre l'État, qui est garant de l'identité primaire des citoyens, et les entreprises privées, qui peuvent avoir légitimement besoin dans certains cas d'un accès électronique facilité aux données du registre de l'état civil (RNIPP, RNE, etc.)[1379].

PS n°3 : Concernant le recours à des technologies blockchains pour des solutions d'identité numérique, cette étude soutient qu'il s'agit de n'écarter à long terme aucune de ces technologies comme le soulignait pourtant en 2020 un rapport d'information de l'Assemblée nationale[1380], y compris celles publiques qui ne sont certes à ce jour pas conformes au droit en vigueur (RGPD/eIDAS), car elles pourraient le devenir en implémentant des solutions de secondes couches comme étudiées en Annexes. Il est également défendu que toutes les solutions d'identités numériques auto-souveraines (INAS) ne bénéficient pas d'une neutralité technologique[1381] bien que favoriser les solutions d'identité numérique 3.0 régalienne semble plus pertinent à court terme. Il convient ainsi de rappeler que les solutions d'identité numérique 3.0 régalienne sont distribuées et non pas décentralisées, c'est-à-dire qu'elles seront garanties par l'Etat, ses institutions ou par des sociétés certifiées.

PS n°4 : Face aux enjeux climatiques et sociétaux actuels, il semble essentiel d'encourager des travaux institutionnels relatifs à l'empreinte environnementale des blockchains dans le contexte du développement d'IND et d'INAS. Une fois ces analyses objectivement confortées dans un temps pragmatique (et non pas court comme cela est actuellement privilégié), il s'agit de renforcer l'accompagnement par la puissance publique des solutions d'IND les plus viables sur le plan

[1376] MAGNIER Véronique, « Aujourd'hui, les entreprises n'ont pas forcément en tête toutes les applications possibles de la blockchain. Les personnes doivent être formées pour comprendre cette technologie et la maîtriser », propos de la Professeure de droit, in *L'Édition de l'université paris-saclay*, été 2021, n° 16, p.10.
[1377] CE, « Communication Shaping Europes Digital Future », *op. cit.*, « La culture et les compétences numériques sont devenues une condition préalable à une participation efficace à la société d'aujourd'hui », consulté en ligne le 6 décembre 2021, p.4.
[1378] V. Annexe 3.
[1379] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, « L'identité numérique ; quelle définition pour quelle protection ? », *op. cit.*, « Plaider pour une meilleure collaboration entre l'État, garant de l'identité civile les entreprises privées, qui revendique de manière légitime l'accès électronique et facile aux données du registre de l'état civil », p.205.
[1380] KARAMANLI Marietta, HENNION Christine, MIS Jean-Michel, Rapport d'Information n°3190 sur l'identité numérique, Assemblée nationale, « Le recours à la blockchain pourrait néanmoins être écarté en matière d'identité numérique des mineurs s'il s'avérait que cette technologie ne peut pas garantir avec certitude le droit à l'oubli ou à l'effacement des données », consulté en ligne le 9 août 2021.
[1381] *Ibid.* « Recommandation n° 40 : Favoriser le développement d'alternatives à l'identité numérique régalienne, comme l'identité numérique auto-souveraine, en exploitant les possibilités offertes par la blockchain », p.109.

énergétique. Ce constat semble également valable pour certaines blockchains publiques telles que Bitcoin d'après l'Annexe 6 de la présente étude[1382].

PS n°5 : Finalement, dans un rapport de janvier 2022[1383], le Conseil National du Numérique (CNNum) recommande 12 leviers politiques, juridiques et sociaux afin de débattre de nouveaux droits et obligations en ligne. Certaines de ces recommandations correspondent parfaitement aux besoins d'encadrement et d'accompagnement des solutions d'IND, comme la proposition n°3 : *« 3. La reconnaissance d'un droit de paramétrer les contenus et les émetteurs* [droit à l'INAS] ». L'objectif serait ainsi d'offrir une nouvelle possibilité d'auto-détermination aux internautes concernant le périmètre des données qu'ils décident de communiquer en fonction de leurs comportements numériques, dont ils deviendraient enfin les seuls propriétaires techniques. Par ailleurs, le CNNum recommande « *6. La création d'un droit à l'interopérabilité entre plateformes.* » tout en suggérant de « *8. Renforcer l'éducation critique et pratique aux médias numériques dans le cadre de projets scolaires et extrascolaires* » ou encore de « *12. Soutenir, concevoir et développer de nouvelles pratiques et de nouveaux dispositifs numériques qui renforcent l'attention conjointe et les liens sociaux sans réduire les individus à des comportements pulsionnels ou à des mécanismes cognitifs.* ». En complément des recommandations précitées qui s'alignent avec les conclusions de cette étude, un second rapport de la même année publié par le ministère de l'Intérieur, et justement dédié à l'IND, nous amène à soutenir l'émergence de quatre nouveaux droits numériques pour les internautes : « [i] *Droit à la préservation d'un espace d'intimité qui concerne l'ensemble des données personnelles de l'individu, qu'elles permettent de l'identifier nommément ou pas ;* [ii] *Droit à la « sûreté numérique » et protection contre les différentes atteintes à la personne qu'il s'agisse d'usurpation d'identité, d'atteinte à la réputation ou au « libre-arbitre » ;* [iii] *Droit à la résilience de l'identité légale numérisée en cas d'attaque ;* [iv] *Droit à profiter d'un environnement numérique de confiance, où la sécurité juridique est préservée et où les allégations produites peuvent être prouvées et/ou certifiées grâce à l'approfondissement de la relation entre l'État et d'autres acteurs clés de la vie du citoyen (banques, assurances, établissement de formations diplômants...)* »[1384]. Agrégées ensemble, ces huit recommandations représentent des leviers politiques, juridiques et informatiques structurels au service d'une nouvelle identité numérique 3.0.

PS n°6 : En conséquence du récent intérêt pour l'intelligence artificielle (IA), les standards de l'IND permettraient l'implémentation industrielle d'identifiants décentralisés et de signatures cryptographiques uniques permettant de certifier l'originalité et la source de tout contenu publié en ligne. Cela apparaît nécessaire pour que l'origine de tels contenus devienne vérifiable, grâce à des preuves numériques 3.0, garantissant ainsi leur intégrité et favorisant la responsabilité afférente à la publication de contenu en ligne. Toutefois, une telle transparence doit être étudiée au cas par cas selon chaque situation et service en ligne pour éviter tout détournement de finalité comme une identification systématique et de masse au détriment d'un droit au pseudo-anonymat en ligne.

[1382] V. Annexe 6, Focus 1.
[1383] Rapport Conseil National du Numérique, 2022, « Votre attention, s'il vous plaît ! Quels leviers face à l'économie de l'attention ? ». Disponible à l'adresse suivante
[1384] *Op. cit.*, COUTOR Sophie, HENNEBERT Christine, FAHER Mourad, « Blockchain et identification numérique, restitution des ateliers du groupe de travail 'blockchain et identité' (BCID) », consulté en ligne, p.49.

Chapitre 2 : Analyse de cas pratiques proposant une identité ou des droits cryptographiques 3.0

2.1 Une preuve d'existence légale et 3.0 pour les enfants sans identité avec DID4ALL

Dans une certaine mesure, la technologie blockchain tend vers une universalité des échanges, ce qui permet à quiconque, indépendamment de son origine, de sa couleur de peau, de sa culture ou de sa nationalité, de bénéficier des avantages de ces solutions sans être discriminé par ces protocoles 3.0. En principe, tous les utilisateurs sont supposés égaux devant des protocoles décentralisés. Les blockchains ouvertes ont réussi à créer une véritable universalité des services (crypto)financiers, offrant une alternative universelle là où les institutions publiques ont parfois échoué. Cependant, la décentralisation peut être un mythe confronté à une réalité physique, logicielle et sociale[1385]. Cette partie vise à comparer le système *Proof of Humanity (PoH)*[1386] particulièrement décentralisé pour lutter contre la censure, au projet « DID4ALL » initié en 2019 par la société IN Groupe pour fournir une identité décentralisée conforme au droit positif[1387]. Le projet DID4ALL a pour but de mettre en place et de garantir un système d'enregistrement régionalisé, inclusif, fiable et durable au service du parcours de vie des enfants qui n'ont pas d'existence juridique dans leur pays. Pour rappel, selon l'UNICEF, cette situation concerne plus de 166 millions d'enfants dans le monde. L'objectif de DID4ALL est de tester une solution numérique 2.0 et/ou 3.0 dans des pays en voie de développement grâce à l'utilisation de trois technologies qui peuvent être combinées : (i) la reconnaissance vocale (par téléphone), (ii) une blockchain ouverte ou fermée et (iii) les systèmes de télécommunication (SMS). Cette solution permet à chaque enfant de disposer d'une preuve d'existence cryptographique, dématérialisée et légalement valable tout au long de son enfance. Cette preuve d'existence peut par exemple être facilement déployée par l'UNICEF, sans avoir besoin d'un accès à Internet pour les enfants et adultes concernés sur le terrain. Elle est donc accessible à tous, y compris aux personnes qui ne savent ni lire, ni écrire. Elle est fiable grâce à l'identification vocale qui constitue un facteur d'authentification unique et sécurisé en raison des données stockées de manière distribuée (P2P). Cette preuve d'existence cryptographique est horodatée sur une blockchain publique, privée ou hybride, en fonction des situations propres à chaque État demandeur de cette solution (à raison de leurs infrastructures). Le projet DID4ALL a pour objectif de répondre à la question suivante : est-ce qu'une preuve d'existence universelle sur la blockchain peut remédier à l'apatridie qui est définie par le droit international comme « *une personne qu'aucun État ne considère comme son ressortissant en application de sa législation* » ?[1388] Ce projet est modulable et peut utiliser de multiples variantes technologiques pour fournir une preuve d'existence – complètement décentralisée ou distribuée au besoin - aux mineurs (et aux majeurs) sans identité ou moyen de la prouver

[1385] V, Annexe 7.
[1386] V. *supra*, II, Titre 1, 2.9
[1387] DID4ALL par IN Groupe, « Cas d'utilisation : une preuve d'existence pour les enfants sans identités », disponible à l'adresse suivante, p.50. V. également la vidéo de la société Margo du 12 novembre 2019 pour le Hackathon Blockchain pour l'UNICEF, disponible sur YouTube
[1388] UNHCR, « Qu'est-ce que l'apatridie ? », in *The UN Refugee Agency*, disponible à l'adresse suivante

en raison d’infrastructures étatiques limitées, voire inexistantes. Le tableau suivant compare donc la solution PoH aux avantages de la solution DID4ALL qui est informatiquement hybride (distribuée), c’est-à-dire conforme par conception aux textes et au droit positif des systèmes juridiques concernés :

Facteurs clés de succès (FCS) pour DID4ALL	**Court terme**	**Moyen terme**	**Long terme**
Reconnaissance juridique et politique	☑ ou ~	☑	☑
Adoption sociale	☑	☑	☑
Adoption et reconnaissance informatique (blockchain ouverte ou fermée, SMS, reconnaissance vocale)	☑ ou ~	☑	☑

Ce tableau suggère que les facteurs clés de succès d’une identité numérique distribuée conformes au droit augmentent drastiquement sa probabilité de succès, c’est-à-dire d’adoption sur le terrain. Plus spécifiquement, il convient d’ajouter qu’il est primordial de protéger la vie privée des enfants mineurs lorsqu'ils utilisent des services en ligne, y compris étatique, ce que permet DID4ALL en comparaison au système *Proof of Humanity (PoH)*. De façon usuelle, les prestataires de services doivent mettre en place une procédure fiable pour vérifier l'âge des utilisateurs afin de déterminer les limites applicables à la collecte de données. Conformément à l'article 8 du RGPD, un responsable de traitement doit obtenir le consentement des personnes avant de traiter leurs données personnelles. Dans certains pays où le RGPD ne s’applique pas, le consentement numérique peut être donné à partir de l'âge de 13 ans. Toutefois, dans notre droit positif, un mineur ne peut pas donner seul son consentement. Par conséquent, le responsable de traitement doit vérifier l'âge du mineur. Pour obtenir un tel consentement éclairé, le responsable de traitement doit expliquer clairement et simplement l'utilisation qui sera faite des données personnelles collectées. Dans les pays en développement, de tels principes juridiques pour protéger les individus ne sont pas toujours prévus, néanmoins, il semble important que les fournisseurs européens de services numériques s'assurent d’offrir de telles garanties juridiques minimum.

2.2 L'identité décentralisée associée à Bitcoin avec le protocole ION

En mars 2021[1389], après une décennie de recherche et développement dans le domaine de l'identité numérique décentralisée, Microsoft a annoncé le lancement d'une expérimentation et d'un nouveau protocole nommé « *Identity Overlay Network - ION* »[1390]. Également supporté par la DIF (fondation de l'identité décentralisée), ce réseau vise à faciliter l'échange d'identifiants décentralisés (DID) émis par des fournisseurs d'identité ou des internautes, directement via la blockchain Bitcoin étudiée dans l'Annexe 3[1391]. Selon Microsoft, un réseau d'identifiants décentralisés doit répondre à plusieurs exigences clés, notamment être ouvert et sans permission, être accessible à travers le monde et produire des enregistrements vérifiables pour tous les acteurs concernés. C'est pourquoi Microsoft a choisi de construire ce protocole en code source ouvert[1392] sur la blockchain Bitcoin. En effet, elle répond à toutes ces exigences. Cette décision de lier le protocole ION à la blockchain publique Bitcoin est à la fois un choix stratégique et un pari politique sur l'avenir comme cette étude le démontre. Cette décision a été prise en raison de la sécurité de la blockchain Bitcoin, qui est à la fois sûre et indépendante, car elle n'appartient à personne tout en étant accessible à tous. Concrètement, le protocole ION est un protocole informatique P2P permettant la création et la vérification d'identifiants décentralisés (DID). Il s'agit d'un réseau de seconde couche (L2) public, distribué et sans permission, ce qui signifie qu'il vise à atteindre un degré élevé de décentralisation, comme la blockchain Bitcoin sur laquelle il repose. Aucune entreprise, organisation ou groupe ne contrôle les identifiants enregistrés dans le système ION et personne ne dicte qui peut y participer (pas même Microsoft). La blockchain Bitcoin possède ses propres interfaces graphiques résumant les transactions sur son réseau[1393] et le protocole ION dispose également de sa propre interface[1394], ces deux interfaces étant donc articulées ensemble et de façon complémentaire pour faciliter les interactions d'identités numériques (DID). Techniquement, les transactions et les événements impliquant les identifiants numériques ancrés sur le protocole ION sont incensurables et immuables grâce à la blockchain Bitcoin[1395]. L'équipe ION de Microsoft a ainsi déclaré que « *Bitcoin est tellement supérieur à toutes les autres options* [blockchains], *qu'il n'y a même pas de comparaison - Bitcoin est l'option la plus sûre avec une marge* [d'erreur] *absurde. Cela offre une alternative sécurisée aux noms d'utilisateurs et aux mots de passe.* »[1396]. La principale proposition de valeur du protocole ION est sa capacité à regrouper des dizaines de milliers d'opérations d'identifiants décentralisés en une seule

[1389] DINGLE Pamela, « ION, We Have Liftoff! », 25 mai 2021, in *Techcommunity.microsoft.com*. Consulté le 5 avril 2022, à l'adresse suivante
[1390] Pour plus d'informations, consultez le site internet suivant
[1391] V. Annexe 3, Focus 1 à 6.
[1392] Le code de ce programme est sous licence Apache 2, les termes du W3C régissent la Propriété Intellectuelle, et le contenu est disponible via une licence Creative Commons 4 Attribution.
[1393] Pour plus d'informations, consultez le site internet suivant www.mempool.space/fr
[1394] Pour plus d'informations, consultez le site internet suivant www.identity.foundation/ion/explorer
[1395] En d'autres termes, le protocole ION est dépendant du protocole Bitcoin pour fonctionner, mais la blockchain Bitcoin peut fonctionner sans le protocole ION. Remarquons que le caractère P2P de ION s'inspire partiellement du Lightning Network.
[1396] « Microsoft ion bitcoin », 2021, in *Goldfasanblog*, traduction libre de l'anglais, à l'adresse suivante

transaction Bitcoin[1397], ce qui augmente considérablement la volumétrie de ce réseau (que nous avons évoquée en première partie). La stratégie de Microsoft concernant l'infrastructure ION consiste à offrir un réseau ouvert, robuste et sécurisé (ce qui permet d'obtenir des effets de réseau et des économies d'échelle), tout en y superposant certains de ses services privés tels que Microsoft Azure[1398], ensuite source d'externalités positives pour l'entreprise et son écosystème d'applications 2.0/3.0. Dans cette continuité, Microsoft a également annoncé en 2022 le lancement d'une nouvelle solution logicielle d'IND, nommée « *Entra Verified ID* »[1399], qui peut fonctionner au choix avec ou sans ION et donc blockchain. Il est important de souligner que Microsoft ne cherche pas à encourager la tokenisation de l'identité numérique des individus (c'est-à-dire en liant l'identité des personnes à des bitcoins), mais plutôt à fournir des identifiants vérifiables sous le contrôle direct des individus (identité auto-souveraine) ou d'entités de confiance (identité informatiquement distribuée, soit hybride). Le protocole ION semble respecter les exigences juridiques en matière de confidentialité des données personnelles des individus conformément au RGPD. Chacune de ces parties conserve la propriété de tous les éléments de son identité[1400]. Toutefois, il est peu probable qu'un gouvernement utilise un service lié aux bitcoins à court et moyen termes, en raison de l'image négative associée à cette blockchain dans l'esprit de la plupart des institutions publiques (craintes plus ou moins avérées de blanchiment d'argent, de financement du terrorisme ou encore de consommation énergétique élevée comme précédemment étudié[1401]). Par conséquent, bien que le protocole ION semble techniquement et économiquement adapté aux solutions d'INAS, son utilisation pour les identités distribuées et régaliennes demeure soumise à une acceptation politique et gouvernementale. En 2023, le réseau ION est toujours à un stade expérimental et possède quelques limites à prendre en compte. Pour qu'un fournisseur d'identité puisse utiliser le protocole ION, il doit verrouiller environ 0,66 bitcoins, soit environ 17 centimes d'euros par transaction début 2023, afin que les transactions de 1000 opérations soient acceptées par ce protocole[1402]. De plus, l'ancrage d'identifiants décentralisés peut prendre jusqu'à 20 minutes, ce qui peut ne pas être suffisamment rapide pour certains cas d'usage industriels nécessitant une identité numérique. ION possède le mérite de démontrer que la blockchain Bitcoin sera probablement dédiée à d'autres cas d'usages au fur et à mesure de son développement informatique, évoqué en Annexes[1403].

[1397] ION peut intégrer *10 000 opérations* d'identification dans une seule transaction (contenant des preuves d'identités) sur la blockchain publique Bitcoin
[1398] En d'autres termes, si Microsoft a initié et met gratuitement à disposition le protocole ION (chacun peut contribuer au réseau) Microsoft propose et met aussi en avant ses propres services d'IND comme « Azure active directory verified Credentials service », *v.* « Introduction to azure active directory verifiable credentials (preview) », in *Microsoft Docs*. Consulté le 5 avril 2022, à l'adresse suivante
[1399] PATEL Ankur, « Microsoft Entra Verified ID now generally available », 2022. Disponible à l'adresse suivante
[1400] Traduction libre de l'anglais, « Les DID ION ne peuvent être désactivées que par leurs propriétaires, protégeant ainsi les personnes contre les violations des droits numériques », consultez le site internet www.identity.foundation/ion
[1401] V. Annexe 6, Focus 1.
[1402] Pour plus d'informations techniques sur ce protocole, consultez le site GitHub suivant.
[1403] V. Annexe 3, Focus 3, 4 et 6.

2.3 L'identité auto-souveraine associée aux crypto-actifs avec le protocole tbDEX

En novembre 2021, Jack Dorsey, fondateur de Twitter, a annoncé le lancement d'un nouveau projet nommé tbDEX[1404], via la société TBD[1405], elle-même financée par sa récente startup Square[1406]. Ce projet vise également à héberger des identités auto-souveraines (INAS) en utilisant la blockchain Bitcoin comme registre de transactions d'attributs d'identité. Plus particulièrement, le protocole tbDEX sera une infrastructure informatique distribuée (P2P) permettant aux utilisateurs d'acheter et de vendre des bitcoins, et éventuellement d'autres crypto-actifs dans un temps long. Il s'agira donc d'un service et protocole en ligne similaire à une plateforme ou bourse de crypto-actifs, mais informatiquement décentralisée. L'objectif de ce protocole est de fournir une confiance et une rapidité d'exécution supérieures aux plateformes d'échanges centralisées, tout en garantissant un degré de décentralisation maximum pour ses utilisateurs, et en respectant les règlementations internationales[1407]. TbDEX vise à devenir un nouvel intermédiaire décentralisé et de confiance, offrant à terme une alternative innovante, universellement accessible et résistante à la censure informatique et financière. Le projet tbDEX introduit le terme de « *Web 5.0* »[1408] dans ses communications en ligne, en référence aux générations du Web 1.0, 2.0 et 3.0 préalablement étudiées, mais surtout en référence au langage de programmation « *HTML5* » aujourd'hui omniprésent sur Internet[1409]. Le lancement de la plateforme tbDEX est prévu pour la fin de l'année 2023. Bien que théoriquement aucun renseignement personnel des utilisateurs ne soit directement collecté par ce protocole, il est nécessaire que certaines entités impliquées dans le processus (institutions financières, personnes physiques ou morales proposant des services d'échange) effectuent une identification préalable avec différents niveaux de garantie au sens du Règlement eIDAS, tels que faible, substantiel ou élevé[1410]. Une fois que l'utilisateur est enregistré (via un KYC) auprès d'un de ces tiers désignés par le protocole en tant que « *Participating Financial Institution - PFI* »[1411], il pourra s'authentifier de manière autonome et sécurisée au sein de tout l'écosystème mis en place par tbDEX grâce aux standards de l'identité décentralisée que nous avons étudiés (P2P, PIND, VC, DID, ZKP, signature électronique). Ce nouveau protocole permettra aux entités juridiques de bénéficier des

[1404] « tbDEX : A Liquidity Protocol v0.1 », L'accès au code open source de ce protocole est possible sur le Github du projet (ci-après). Le Livre Blanc de présentation du projet est aussi en cours de révision par la communauté et disponible à l'adresse suivante

[1405] Le premier produit de la société TBD axée sur le bitcoin sera *tbDEX*, une plateforme d'échange décentralisé qui jouera le rôle de protocole de liquidité pour l'achat et la vente P2P de bitcoins

[1406] Société Square, *v*. site internet suivant

[1407] Traduction libre de l'anglais, « Toutefois, les informations nécessaires peuvent varier en fonction de la juridiction. », p. 7 sur 18, et *v*. *supra*, I, Titre 2, 2.5

[1408] « Web5: an extra decentralized web platform », 2022, in *TBD*, disponible à l'adresse suivante

[1409] TBD, « Are We Web5 Yet ? », traduction libre de l'anglais, « Le terme Web5 est un retour en arrière qui rend hommage au HTML5, qui a été utilisé pour représenter le dernier effort majeur pour faire évoluer le Web il y a une quinzaine d'années. », disponible à l'adresse suivante

[1410] *Op. cit.* Livre Blanc tbDEX, traduction libre de l'anglais, « Les PFI […] peuvent être soumises à des règles et réglementations différentes pour les paiements en monnaie fiduciaire, en fonction de leur juridiction spécifique, elles doivent probablement collecter certaines informations personnelles identifiables (IPI) auprès des propriétaires de portefeuilles afin de répondre aux exigences réglementaires, telles que le respect des programmes de lutte contre le blanchiment d'argent (AML), la lutte contre le financement du terrorisme et la non-violation des sanctions. », p.6, *v*. également *supra*, II, Titre 1, 2.1.1.1

[1411] *Op. cit.* Livre Blanc tbDEX, traduction libre de l'anglais, « Les institutions financières participantes (IFP) sont des entités qui offrent des services de liquidité sur le réseau tbDEX », p.6.

avantages mentionnés d'une identité numérique décentralisée ou distribuée, ce qui bénéficiera également à leurs utilisateurs qui pourront ensuite gérer et administrer leurs propres attestations vérifiées (comme avec une INAS)[1412]. Par conséquent, tbDEX offrira des identités numériques à la fois distribuées et auto-souveraines, la frontière entre les deux n'étant pas encore certaine pour ce nouveau système et concept inédit au sein du Web 3.0. Chaque utilisateur de PIND aura la possibilité de générer sa propre identité numérique auto-souveraine en passant par un processus de certification basé sur la réputation, qui sera évaluée par des mécanismes électroniques de reconnaissance sociale entre pairs (comme le fonctionnement des avis certifiés plus ou moins fiables sur certains services en ligne, tels que le service en ligne TripAdvisor). En outre, pour garantir l'identification et l'authentification des utilisateurs sur ce nouveau protocole, il est très probable que les PFI auront recours à des services spécialisés proposés par des entreprises expertes dans l'analyse et la lutte contre les transactions illégales réalisées en crypto-actifs (Chainalysis ou CypherTrace)[1413]. Bien que ce protocole vise en principe à maintenir une certaine neutralité technologique[1414], il tend néanmoins à offrir à ses utilisateurs un droit au pseudo-anonymat[1415]. Bien que cela puisse sembler utopique étant donné l'identification systématique des internautes en conformité avec les règlementations financières étudiées, nous considérons que ce nouveau protocole représente également un modeste contre-pouvoir au service des cybernautes (ce qui explique l'utilisation de la blockchain Bitcoin qui conforte ces principes d'anonymat et d'incensurabilité des échanges). En fin de compte, tbDEX est un projet novateur, qui se démarque des nombreux projets de plateformes d'échanges centralisées qui existent, notamment grâce aux standards informatiques 3.0 que ce service ambitionne d'articuler ensemble (P2P, Bitcoin, INAS, DID, VC, ION). Néanmoins, chacune de ces briques implique une appréciation et des conséquences techniques, juridiques et commerciales tout aussi innovantes que complexes à articuler pour une grande partie des acteurs de la société. Si ce nouveau protocole est le premier projet en date et d'envergure qui combine crypto-actifs et IND, il est également un exemple concret d'application au service d'une forme d'identité numérique universelle, probablement utopique comme suggéré précédemment face aux pouvoirs politiques, institutionnels et à la multitude des règles de droit existantes dans le domaine financier.

[1412] Traduction libre de l'anglais, « Les organisations et les particuliers (au moyen de leur portefeuille) peuvent être des émetteurs. », p.5.
[1413] Traduction libre de l'anglais, « En concordance avec la mise en œuvre du protocole tbDEX, l'utilisation de solutions analytiques et d'intelligence blockchain peut aider les PFI à filtrer, noter et surveiller les portefeuilles et les transactions individuelles afin d'évaluer les transactions en fonction du critère de risque et des obligations réglementaires du PFI », p.14., *v.* également le site internet d'une société spécialisée dans ce type de détection www.chainalysis.com ou encore www.ciphertrace.com
[1414] Traduction libre de l'anglais, « Le protocole n'a pas d'opinion sur l'anonymat en tant que caractéristique ou conséquence des transactions. », p.1.
[1415] Traduction libre de l'anglais, « Notre objectif n'est pas de maintenir l'anonymat des transactions à tout prix. Il n'est pas non plus de miner la capacité d'un individu à optimiser l'anonymat. Rien n'empêche en principe d'effectuer des transactions anonymes à des fins de confidentialité financière sur le réseau tbDEX », p.7.

2.4 Identité et euro numérique : analyses croisées des crypto-actifs stables et des MNBC

Les monnaies ont toujours eu une étroite relation avec l'identité et l'histoire des sociétés humaines. Elles ont été utilisées comme moyen de communication et de reconnaissance sociale, reflétant ainsi les valeurs et les croyances de chaque culture. L'utilisation d'une monnaie confère également des droits et des devoirs aux individus, comme l'a souligné John Locke « *la monnaie joue un rôle très utile dans les échanges car elle permet la conservation des droits dans le temps et dans l'espace* »[1416]. Le terme « *fiduciaire* » vient du mot latin « *fiduciarius* » et plus précisément de « *fiducia* » (« *confiance* »)[1417]. En effet, la monnaie n'est à sa racine qu'une affaire de confiance sociale. Sur le plan structurel, les monnaies fiduciaires telles que l'Euro, le Dollar ou le Yuan reposent sur la crédibilité et la capacité d'un ou plusieurs États à respecter leurs finances. Aujourd'hui, le numérique a transformé les interactions, les usages et les besoins sociétaux avec lesquels la monnaie doit désormais composer. Par exemple, en 2021, 71% des adultes des économies développées disposent d'un compte bancaire nominatif, contre 42% il y a dix ans[1418]. La surveillance des individus peut potentiellement conduire à une manipulation de leur comportement par le biais de la collecte d'informations sur leurs habitudes et préférences, permettant ainsi une influence plus ou moins subtile sur ces derniers. Le contrôle des finances des individus peut également représenter un pouvoir considérable sur leurs vies, étant donné que le capital est un élément crucial dans de nombreux aspects de la vie quotidienne, tels que le logement, la nourriture, l'éducation et les loisirs. Par conséquent, l'exercice d'un contrôle total sur les finances d'un individu peut avoir un impact significatif sur ses décisions, ses choix et son état d'esprit général qu'il exerce aujourd'hui en ligne. Dans cette perspective, il est essentiel de protéger la vie privée et la liberté financière des individus pour garantir leur autonomie et leur épanouissement. A ce titre, la CNIL considère que les données de paiement sont « *l'ensemble des données personnelles utilisées lors de la délivrance d'un service de paiement pour une personne physique* »[1419]. L'arrivée de nouvelles innovations technologiques telles que les crypto-actifs a entraîné une remise en question de la forme traditionnelle de la monnaie, tout particulièrement sous sa forme digitale. Depuis 14 ans, ces innovations ont bouleversé notre perception de l'espace et du temps, car elles permettent des échanges sans interruption grâce à une communication décentralisée entre des machines, contrairement aux monnaies légales qui nécessitent l'intervention en cascade d'institutions financières et de tiers de confiance. Si cette expansion du numérique est possible grâce à l'utilisation de nos monnaies actuelles en ligne, ce qui peut laisser penser à leurs utilisateurs qu'elles possèdent un sous-jacent cryptographique, cela n'est en réalité pas le cas au sens des technologies 3.0 qui ont été étudiées. Les monnaies fiduciaires actuelles ne sont en effet que des échanges de données comptables aux effets juridiques et économiques, tandis que des

[1416] LOCKE John, « Le droit naturel selon John Locke », 22 mars 2022, in *Contrepoints*. Consulté le 22 mai 2022, à l'adresse suivante
[1417] Définition « fiduciaire », in *Dictionnaire de français Larousse*, disponible sur le site larousse.fr
[1418] « The Global Findex Database 2021: financial inclusion, digital payments, and resilience in the age of Covid-19 », 14 septembre 2022, in *World Bank*. Consulté le 27 septembre 2022, à l'adresse suivante
[1419] CNIL, Livre blanc n°2 : « Quand la confiance paie », *op. cit.*, disponible à l'adresse suivante, p.12.

données cryptographiquement vérifiables portent des effets informatiques et mathématiques (crypto-actifs).

L'euro électronique n'est en réalité actuellement pas programmable contrairement aux monnaies cryptographiques et à leurs systèmes blockchains que cette étude consacre. Dès lors, est-il possible pour un Etat ou pour une institution financière de proposer une monnaie cryptographiquement et mathématiquement programmée et dont le cours serait stable et légalement reconnu ? Un euro cryptographique serait-il légal[1420] ? Le concept récent de monnaies numériques de banques centrales - MNBC (« *Central Bank Digital Currencies – CBDC* »), fait son apparition en réponse à certaines tentatives de développement de monnaies cryptographiques stables développées par des sociétés privées comme Facebook (*v.* ci-dessous). Depuis l'apparition du bitcoin, la volatilité des crypto-actifs fait de ces jetons numériques un moyen d'échange imparfait, mais alternatif, pour accéder quotidiennement et massivement à des biens et des services[1421]. Si certaines solutions intermédiaires existent, comme des cartes bancaires permettant de dépenser des crypto-actifs de façon intuitive[1422], ces dernières représentent une forme de nouvelle intermédiation qui éloigne ces actifs et leurs écosystèmes des promesses initiales de décentralisation pure et de confiance sociale minimaliste « *zero trust* » précédemment examinées. Il apparaît que ces systèmes plus ou moins informatiquement et socialement décentralisés[1423], mais concurrents aux institutions financières classiques, ne parviennent qu'à résoudre imparfaitement le problème de la volatilité intrinsèque des crypto-actifs qui dépendent pour rappel de leur offre et de leur demande. Pour l'instant, ils ne sont donc pas considérés comme des devises par le système financier international[1424], à quelques exceptions près mentionnées en Annexes. Par exemple, les banques centrales sont sceptiques à l'égard de l'adoption du bitcoin et d'autres crypto-actifs, en raison de leur indépendance et autonomie, de leur supposé potentiel de fraude, de leur volatilité économique et surtout de leur concurrence directe avec les institutions financières traditionnelles.

Face à ces constats et surtout à la nécessité de stabilité du prix de ces jetons instables, certains acteurs de l'écosystème des crypto-actifs ont développé des *crypto-actifs stables*, appelés *stablecoins*. Ces actifs peuvent être liés à la valeur d'un autre actif spécifique, comme une monnaie fiduciaire, une matière première ou même un autre crypto-actif (dont le cours peut également fluctuer). Bien que le concept de stablecoins a été imaginé depuis les premiers jours de l'écosystème des crypto-actifs, le premier stablecoin en date, le « Tether » (USDT), n'a été introduit qu'en 2014 par la société Tether Ltd. Ce dernier est adossé au Dollar américain avec lequel il garantit une parité de sorte qu'un USDT est égal à

[1420] De VAUPLANE Hubert, « Un euro numérique est-il légal ? », 2023, in *La REF* n°149, Les monnaies numériques et les crypto-actifs.
[1421] La monnaie n'existe que par la confiance et cette confiance ne peut se créer qu'avec une certaine stabilité monétaire au XXIè siècle.
[1422] TELLIER Louis, « Ledger lance sa carte de crédit crypto », 12 janvier 2021, disponible sur le site agefi.fr
[1423] V. Annexe 7.
[1424] Sur le fondement de l'article L.111-1 du code monétaire et financier, seul l'euro a cours légal en France. L'article 1343-3 du Code civil dispose « le paiement en France d'une obligation de somme d'argent s'effectue en euros (…) peut avoir lieu en une autre monnaie si l'obligation ainsi libellé procède d'une opération à caractère international (…) ». V. aussi Annexe 5.

un dollar. Depuis, d'autres stablecoins significatifs ont vu le jour, tels que le « TrueUSD », introduit en 2018 et également lié au Dollar américain, ou le « DAI », introduit en 2017 et adossé à un panier de crypto-actifs tout en étant lié à la valeur du Dollar grâce à des mécanismes algorithmiques (AEC) évoqués précédemment. Il existe ainsi plusieurs méthodes possibles et plus ou moins éprouvées pour garantir la stabilité du prix d'un *crypto-actif numérique stable*[1425]. Depuis leur introduction, ces stablecoins ont gagné en popularité comme un moyen de réduire le risque de la volatilité associé aux crypto-actifs non stables (bitcoin, ether). Les stablecoins facilitent ainsi une utilisation pour des transactions quotidiennes (échange entre ces stablecoins et crypto-actifs), souvent en méconnaissance de certaines règles fiscales comme l'impôt sur les plus-values ou la TVA, ce qui explique l'encadrement des stablecoins par le Règlement MiCA. Les stablecoins ont ainsi trouvé leur principale utilisation dans les opérations de change ainsi que dans le transfert de fonds internationaux, offrant également une solution pour conserver la valeur dans des pays où l'économie et/ou la monnaie sont instables. Toutefois, pour bien comprendre les enjeux liés aux stablecoins et aux MNBC, il est important de considérer les différences et similarités qui lient ces deux types de crypto-actifs. Il est possible de faire fonctionner des crypto-actifs stables sur des blockchains publiques, qui utilisent elles-mêmes un crypto-actif volatil[1426]. Cette combinaison peut ainsi entraîner des défis en termes de compréhension informatique ainsi que de conformité règlementaire ou de stabilité monétaire.

Depuis 2014, de nombreux projets expérimentaux étatiques et institutionnels de monnaies numériques au sens cryptographiques ont ainsi vu le jour (125 projets à l'échelle internationale fin 2022)[1427]. Deux évènements ont radicalement accéléré ce phénomène de transition monétaire, notamment l'annonce en juin 2019 du projet de développement d'un crypto-actif stable par Facebook (le stablecoin « *Libra* » renommé « *Diem* » avant sa disparition en 2021. De plus, cet effet d'annonce a été accompagné par l'annonce en octobre 2020 de la société Paypal qui offre désormais la possibilité d'acheter et de vendre du bitcoin et de l'ether à ses utilisateurs[1428]. Face à cet essor continu des monnaies cryptographiques privées, stables et volatiles, les institutions monétaires traditionnelles ont également débuté une lente transition vers le développement de monnaies cryptographiques stables et officielles (MNBC), c'est-à-dire dont la valeur économique et politique serait légalement et internationalement reconnue et

[1425] Il est possible de distinguer trois types de stablecoins : (i) Les stablecoins adossés à une monnaie fiduciaire qui sont garantis par une réserve de monnaie fiduciaire, tel que le dollar américain, l'euro ou le yen ; (ii) Les stablecoins adossés à des actifs tangibles, c'est-à-dire qui sont garantis par une réserve d'actifs sous-jacents tels que l'or, de l'argent ou d'autres métaux précieux, ou encore par des produits comme le pétrole ; (iii) Les stablecoins algorithmiques qui peuvent être adossés à l'un ou l'autre des deux types de stablecoins précédents, à la différence qu'un algorithme est supposé contrôler son offre et sa demande pour maintenir sa valeur stable (il est donc supposé hautement décentralisé et sans tiers de confiance contrairement aux points ci-avant) ; Un quatrième (iv) type de stablecoin, les stablecoins hybrides, combinent certaines des caractéristiques ci-avant pour maximiser leur stabilité et leur sécurité.

[1426] Par exemple, la blockchain Ethereum possède son crypto-actif natif dont le prix/cours fluctue (« ether ») et parallèlement le stablecoin « DAI » propose un prix stable et fonctionne grâce au contrat intelligent de cette même blockchain. Ainsi, le DAI est lié à l'ether, mais la stabilité des prix est supposément assurée pour ce premier et non pas pour le second. Le DAI est un stablecoin de type algorithmique comme mentionné la page précédente.

[1427] Consultez le carte interactive « Central Bank Digital Currency (CBDC) Tracker » par la société Boston Consulting Group, disponible à l'adresse suivante

[1428] V. Annexe 3 & 6, Focus 1 et 2.

cryptographiquement fondé. Par exemple, dès 2021, la Chine annonce le lancement officiel d'un Yuan cryptographique (« *e-CYN* »)[1429], une profonde transformation initiée conceptuellement dès 2014 et a priori réussie sur le plan monétaire et économique[1430]. Néanmoins, concernant la gouvernance et surtout la protection des données des utilisateurs de cette nouvelle classe d'actif cryptographique propulsée par les banques centrales, des abus semblent possibles (surveillance ciblée, de masse, censure). Le 2 octobre 2020, la BCE publie un rapport sur l'Euro numérique[1431], dont la vocation serait monétaire et le sous-jacent cryptographique (reprenant potentiellement certains standards des blockchains). La mise à disposition d'un Euro cryptographique à destination des citoyens européens représente en quelque sorte une réaction de la BCE vis-à-vis des crypto-actifs stables et volatils, ainsi que du e-CYN, précités. Selon une décision de Christine Lagarde, Présidente de la BCE, l'idée de lancer officiellement un Euro cryptographique aurait été prise le 23 octobre 2023[1432], pour une mise en application en 2026 ou 2027, d'après la Banque de France[1433]. Il s'agirait d'un Euro cryptographique de type interbancaire[1434] également accessible au grand public[1435]. Il pourrait être centralisé ou décentralisé sur le plan informatique, mais serait probablement centralisé ou hybride au sens de cette étude. En effet, un système centralisé permettrait de maintenir un contrôle informatique ainsi qu'une centralisation de l'infrastructure, conformes aux mécanismes de gouvernance étatique et aux multiples règles de droit liées aux monnaies actuelles. Les commentaires du Gouverneur de la Banque de France en 2022 suggéraient que les banquiers centraux cherchent des moyens d'intégrer une fonctionnalité de tokenisation à l'architecture monétaire existante (particulièrement utile aux blockchains fermées)[1436], tout en régulant la technologie de manière appropriée[1437]. L'Euro cryptographique serait donc probablement une monnaie publique et numérique dont le fonctionnement se voudrait similaire à l'espèce (« cash »), c'est-à-dire disponible en pair à pair dans le cas de paiements de détail (créant ainsi un « cash électronique 3.0 » légalement reconnu)[1438].

[1429] « Progress of Research Research & Development of E-CNY in China ». 2021. pbc.gov.cn

[1430] GAYTE Aurore, « 261 millions de personnes se servaient de l'app pour payer avec des e-CNY » *;* « Tout comprendre au e-yuan, la monnaie numérique que la Chine met en avant pendant les JO 2022. Plus de rapidité mais moins de vie privée ? », 4 février 2022, in *Numerama.com*, disponible à la lecture Numerama, v. également SLIM Assen, « La MNBC e-hryvnia : une monnaie banque centrale en projet », 29 novembre 2022, in *La REF*, n°147, « Les monnaies numériques et les crypto-actifs ».

[1431] BCE, « Report on a digital euro », 2020, disponible sur ecb.europa.eu

[1432] BARLUET, Alain, « Les étonnants canulars d'un duo russe au service du Kremlin », 2023, in *Le Figaro*, disponible à l'adresse suivante

[1433] VILLEROY de GALHAU Fançois (discours) « Ancres et catalyseurs : le double rôle des banques centrales en matière d'innovation », « En Europe, nous en sommes à mi-chemin de notre phase d'étude : l'Eurosystème prendra sa décision d'ici fin 2023, pour un lancement potentiel en 2026 ou 2027. », Banque de France. Disponible à l'adresse suivante

[1434] *Ibid*. Il est fait référence au « Wholesale Digital Euro », soit une implémentation d'un euro digital uniquement accessible et utilisable uniquement entre des institutions financières (entre les banques commerciales et/ou avec la BCE).

[1435] *Ibid.* Il est fait référence au « *Retail Digital Euro* », soit une implémentation d'un euro digital accessible à tous sans distinction, citoyens européens, institutions financières, commerçants.

[1436] L'avènement d'un *euro cryptographique* permettra de financer les infrastructures des blockchains privées et hybrides, des écosystèmes en situation de besoin de financements comme mentionné auparavant par cette étude. V. ci-dessous.

[1437] VILLEROY de GALHAU Fançois (discours), *op. cit.* « J'espère que nous, banquiers centraux, trouverons le moyen d'intégrer la tokenisation à l'architecture [monétaire] existante, tout en la régulant dans la mesure nécessaire », disponible à l'adresse suivante

[1438] Il est souligné que ce terme était justement mentionné dans le Livre Blanc de Bitcoin dès 2008, ce qui démontre que l'intention de la BCE s'aligne avec celle du bitcoin souhaitant créer un *cash électronique*, à la différence qu'un euro

L'objectif politique de la BCE semble de maintenir le rôle de la monnaie 2.0, à l'ère 3.0, en offrant une transition supposée au service des citoyens européens et de leurs droits économiques et financiers (droit au compte, simplification administrative, etc.). L'adoption d'un Euro cryptographique permettrait également de préserver en théorie le rôle de la monnaie officielle de l'UE en tant que stabilisateur du système de paiement, tout en transposant en ligne l'utilisation de l'argent liquide qui persiste tout en déclinant progressivement[1439]. Un Euro 3.0 aiderait supposément à protéger cette souveraineté monétaire tout en favorisant la concurrence dans la fourniture de nouveaux services bancaires et financiers. En outre, l'Euro cryptographique pourrait accélérer la numérisation de l'économie européenne. Lorsque existe la concurrence d'une monnaie privée face à une monnaie publique et officielle in fine gérée par une banque centrale, cette dernière se doit d'apporter certaines réponses, notamment normative et politiques, aux phénomènes des crypto-actifs dont la vocation monétaire était à l'origine privée puis finalement ouverte au grand public[1440]. Le Règlement MiCA propose à cet égard ded premières réponses, notamment en imposant une supervision directe des stablecoins dits « *significatifs* »[1441] (en volume et provenance) par l'Autorité Bancaire Européenne (« *European Banking Authority – EBA* »). Avec un Euro ou un Dollar cryptographique, la volonté des banques centrales est d'inspirer à nouveau confiance aux acteurs de la société, en fournissant un nouveau moyen d'échange 3.0 directement et cryptographiquement relié entre les citoyens et les banques centrales. L'un des principaux défis de la BCE est donc de transposer la confiance existante envers les institutions financières, vers la confiance numérique 3.0 supposée plus inclusive et sécurisée d'un tel Euro cryptographique. Cette transition n'est pas anodine, car elle doit s'accompagner de justifications et de fondements sociaux, informatiques et juridiques proportionnés aux impacts supposés. Par exemple, il sera nécessaire de réaliser une identification contextualisée pour les utilisateurs[1442], qu'ils soient des personnes physiques (citoyens européens) ou des personnes morales (institutions financières, commerçants). Cette identification préalable permettrait notamment de prévenir les « *attaques Sybil* » évoquées[1443], tout en permettant la possibilité d'une action judiciaire en cas de fraude ou d'activité illicite. Ainsi, la BCE devrait mettre en place des mécanismes d'identification et de sécurité informatique solides pour garantir la confiance des utilisateurs envers cet Euro 3.0. Pour qu'un Euro cryptographique grand public devienne une solution

cryptographique sera légalement encadré et reconnu. V. *op.cit.,* NAKAMOTO Satoshi, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008, disponible en ligne

[1439] NEDELEC Gabriel, « Le cash continue son lent déclin en Europe », in *Les Echos*, 2020, « Les paiements en espèces ont représenté 73 % de l'ensemble des transactions réalisé en 2019 dans la zone euro », disponible en ligne. Souvent évoquée, la disparition des espèces signifierait probablement une dé-bancarisation pour les personnes en situation irrégulière, ce qui ne semble pas souhaitable pour ces acteurs les plus modestes de la société.

[1440] ROCCA Olivier, ACHER Vincent, DENIS Philippe, SALLET Fleury, « A la décharge des banques et des Etats, nous pouvons affirmer qu'avant l'arrivée du réseau de blockchain publique Bitcoin, la notion de monnaie [cryptographique] publique n'existait pas. », Protocole Executif, 2022, in *DUDM*, disponible à l'adresse suivante, p.43.

[1441] V. *supra*, I, Titre 2, 2.5.1

[1442] BCE, « Report on a digital euro », *op. cit.*, p.38, « L'émission d'un euro numérique devrait rester sous le contrôle de l'Eurosystème. Des intermédiaires supervisés devraient être impliqués au moins pour l'identification et l'embarquement des utilisateurs habilités et éventuellement pour l'acheminement des transactions vers l'infrastructure de la banque centrale ; ils pourraient créer de nouvelles entreprises sur les services numériques liés à l'euro », ecb.europa.eu

[1443] *Ibid.* p.28.

globale, fiable et pérenne, il apparaît essentiel de le rendre techniquement abordable et accessible sans contrainte, avec ou sans Internet, via mobile ou ordinateur, avec la possibilité programmée d'un pseudo-anonymat des transactions. Ces quelques caractéristiques visent à permettre une meilleure inclusion financière, notamment pour les individus non européens et pourtant présents sur le sol européen, dont la bancarisation est à ce jour précaire, voire inexistante. Une solution probable envisage à terme de mettre cet Euro cryptographique à disposition des citoyens européens au moyen d'une identité numérique distribuée (PIND). Une telle imbrication entre des identités numériques 3.0 et un moyen de paiement 3.0 implique une gestion ainsi qu'une utilisation sécurisée, souveraine, simple et rapide des données d'identité et de paiements cryptographiques. Les processus de vérification d'identité (KYC)[1444] des utilisateurs de ces portefeuilles numériques exigeraient ainsi la récolte et le partage d'attributs d'identité racine pour leurs utilisateurs et par les institutions financières concernées. En tout état de cause, grâce à une IND, la vérification des informations d'identité bancaire serait simplifiée, car automatisée, évitant ainsi des escroqueries et des difficultés relatives à la responsabilité et aux violations des droits des utilisateurs ou des institutions impliquées[1445]. Pour illustrer ces propos, en novembre 2022[1446], la Banque de France clôture un appel à contribution sur le sujet auprès du groupe BPCE et des sociétés Archipels et IN Groupe. L'utilisation d'une IND dans la gestion de l'authentification des établissements de crédit y est officiellement mentionnée, ce qui semble confirmer cette possibilité.

A la lumière de ces propos, il semble pertinent de comparer le positionnement du bitcoin depuis 2009[1447], à l'initiative de l'Euro cryptographique qui puise certaines inspirations cryptographiques et technologiques dans sa blockchain (presque 20 ans après). L'émergence du bitcoin a permis pour la première fois à des acteurs privés et numériques de s'investir d'un pouvoir monétaire, au sens des trois fonctions d'une monnaie telles que définies par Aristote[1448]. Cette situation est sans précédent dans l'ère numérique et il est difficile de prévoir les implications d'un tel renversement des pouvoirs financiers jusqu'alors établis. Dans son ensemble, les économistes, les politiques[1449] et de nombreux

[1444] Le partage d'attestation vérifiables (VC) entre des banques pourrait se faire à courte échéance et de façon simplifiée, car les banques se font déjà informatiquement et socialement confiance réciproquement dans leur écosystème financier. Cela représenterait une amélioration (d'utiliser des VC) par rapport à l'utilisation et au partage de KYC (PDF, photos, Web 2.0).
[1445] OTTAWAY Catherine, « Les banques sont responsables en cas d'ordre de virement électronique irrégulier », 2002, in *Les Echos*, consulté le 13 octobre 2022, disponible à l'adresse suivante, v. également Cass. com. 2 novembre 2016 n° 15-12.325 et Cass. Com. 24 janvier 2018, n° 16-22.336
[1446] Banque de France, « La Banque de France clôture son appel à contribution pour l'usage de l'identité numérique dans la gestion de l'authentification des établissements de crédit », « Une collaboration d'IN Groupe (Imprimerie nationale) et d'Orange, pour mettre en œuvre l'identité décentralisée sur technologie Blockchain », 2022, disponible à l'adresse suivante
[1447] NAKAMOTO Satoshi, traduction libre de l'anglais, « Beaucoup de gens considèrent automatiquement la monnaie électronique comme une cause perdue en raison de toutes les entreprises qui ont échoué depuis les années 1990 [B-Money, DigiCash, Hashcash déjà évoqués]. J'espère qu'il est évident que c'est seulement la nature centralisée de ces systèmes qui les a condamnés. Je pense que c'est la première fois que nous essayons un système décentralisé, non basé sur la confiance. », 2009, accessible en ligne à l'adresse suivante
[1448] V. Annexe 3, Focus 3.
[1449] DUFRENE Nicolas, DELAHAYE Jean-Paul, MAUREL Emmanuel, et al., « Les crypto-actifs : du mirage à la réalité penser l'impact financier, économique, écologique et politique des crypto-actifs », « Pour l'heure on peine toutefois à trouver les arguments réellement décisifs qui démontreraient la plus-value sociale apportée par les cryptoactifs. Au contraire, force est de constater que l'écosystème des cryptoactifs n'apporte au mieux qu'un fac-similé du système financier et bancaire traditionnel, sans pour autant disposer des mêmes atouts, à commencer par la capacité légale de créer de la monnaie, et surtout

gouvernements remettent régulièrement en question le potentiel informatique, monétaire et financier de cet actif, depuis son apparition et au fur et à mesure de son adoption par les internautes. Les banques centrales et les sphères institutionnelles et politiques sont principalement opposées à Bitcoin pour au moins trois raisons. Tout d'abord, Bitcoin échappe au contrôle des banques centrales et des gouvernements, ce qui remet en question leur rôle de gardien de la politique monétaire et de la stabilité financière. Cette perte de contrôle représente une menace pour leur souveraineté monétaire et leur rentabilité économique, car Bitcoin permet de transférer et stocker des jetons de valeur sans intermédiaire. Aussi, les banques centrales considèrent que les bitcoins sont vecteurs de fraudes, de blanchiment de capitaux et de financement d'activités illégales, bien que des chiffres fiables démontrent le contraire[1450]. Finalement, les pouvoirs établis estiment que la forte volatilité du prix de Bitcoin est une préoccupation majeure, car elle peut perturber le fonctionnement de l'économie et créer une instabilité sur les marchés financiers, un postulat qui semble aujourd'hui complexe à démontrer sur le plan scientifique. En somme, les banques centrales et les sphères politiques et institutionnelles perçoivent cette infrastructure et ce jeton comme une menace pour leur rôle traditionnel, leur souveraineté monétaire et la stabilité financière internationale. En réalité, il est important de comprendre que la majorité de ces préoccupations reposent sur des idées parfois reçues et que Bitcoin peut également offrir à tout internaute des avantages en tant que moyen de paiement rapide, peu coûteux et sécurisé. En partant de ce constat étudié dans les Annexes[1451], la question fondamentale à laquelle il s'agit de répondre est de déterminer précisément ce qu'apporterait une MNBC de plus que ce qu'apportent déjà bitcoin ou les stablecoins ? Avant de proposer des pistes de réflexion à cette question fondamentale, certains propos de Satoshi Nakamoto rédigés en 2009 permettent de comprendre l'origine de cette concurrence monétaire entre les monnaies numériques comptables versus cryptographiques et mathématiques : « *nous devons faire confiance à la banque centrale pour ne pas dévaluer la monnaie, mais l'histoire des monnaies fiduciaires est remplie de violations de cette confiance.* (...) *Nous devons leur faire confiance pour protéger notre vie privée, pour qu'ils ne laissent pas les voleurs d'identité vider nos comptes* »[1452]. Dès lors, le lancement de MNBC permettrait-il réellement aux banques centrales de susciter une nouvelle confiance pour les citoyens à qui s'adresse cette nouvelle forme d'échange 3.0 ? En 2021, la CNIL rappelle que le respect de la vie privée et la protection des données personnelles sont essentiels pour garantir une monnaie de confiance[1453]. La BCE explique que l'Euro cryptographique ne serait qu'un prolongement numérique de la monnaie fiduciaire et notamment des espèces comme

sans aucun des garde-fous qui ont progressivement (et encore incomplètement) conduit à encadrer l'action des acteurs bancaires et financiers. », 2022, disponible à l'adresse suivante, p.105.

[1450] Worldcoin, « Understanding Money Laundering: How Common Is It in Crypto? », 2023, disponible à l'adresse suivante, traduction libre de l'anglais, « Dans un rapport distinct de CipherTrace, le volume total des transactions de crypto-monnaies illicites était compris entre 0,1% et 0,15% en 2021. Ce chiffre était plus proche de 0,62-0,65% en 2020. L'argent liquide reste le moyen le plus courant d'échange utilisé dans le blanchiment d'argent ».

[1451] V. Annexes 3 & 6

[1452] NAKAMOTO Satoshi, traduction libre de l'anglais, « Bitcoin open source implementation of P2P currency », 2009. P2P Foundation. Consulté à l'adresse suivante

[1453] CNIL « Livre Blanc n°2 : Quand la confiance paie », *op. cit.*, disponible à l'adresse suivante

précédemment évoqué. Dès lors, la caractéristique essentielle que représente l'anonymat des transactions devrait être garantie juridiquement[1454] puis informatiquement (par exemple grâce aux VC, DID, ZKP). De même, la protection des données serait protégée à divers degrés selon les choix techniques effectués, de façon à arbitrer entre les droits individuels et l'efficience technique de cette MNBC centralisée mais légalement reconnue. Tandis que la régulation des monnaies fiduciaires autorise un anonymat complet pour les échanges en espèces, la régulation des paiements électroniques avec une MNBC[1455] ne permettrait probablement au mieux qu'un pseudo-anonymat[1456], conformément aux multiples textes européens relatifs à la LCB-FT qui ont été évoqués (MiCA, TFR). Ainsi, des processus de vérification d'identité fiable seront nécessaires en vertu des règlementations afférentes[1457], selon les montants, les fréquences de transactions et les profils de chaque personne physique. En théorie, l'identité et l'historique des transactions de ces derniers ne seront visibles que par les banques centrales et/ou commerciales que l'utilisateur aurait délibérément choisies. Dans les faits, cet Euro cryptographique devra répondre à la question de la 'censurabilité' étatique des transactions financières privées des citoyens. En effet, l'instauration d'une MNBC pourrait permettre de censurer ou de surveiller massivement certains citoyens, à tout moment, en temps réel[1458] et selon un cadre juridique en perpétuelle mutation comme démontré. Aujourd'hui, ce constat ne s'applique pas grâce à l'alternative qu'est l'argent liquide et qui représente un halo d'anonymat protecteur pour les citoyens face à toutes tentatives injustifiées de contrôle et de surveillance généralisés (ce que le bitcoin représentait également à l'origine). En 2021, la CNIL souligne ainsi ces risques de sur-identification liés aux finalités et usages d'un Euro cryptographique ou plus largement de toute MNBC[1459]. Le risque de fuites de données aussi probables et comme cela arrive régulièrement dans l'univers des crypto-actifs (la responsabilité incombant souvent aux utilisateurs et aux services en ligne et non pas aux Etats comme cela pourrait être le cas dans le cadre d'une MNBC). Par ailleurs, sur le plan économique, l'introduction d'un Euro cryptographique programmable offre la possibilité de mettre en place une 'monnaie fondante'. Une telle monnaie pourrait inclure une date de péremption, obligeant les citoyens à utiliser leurs fonds avant une certaine période, faute de quoi ces liquidités deviendraient inutilisables. Cette fonctionnalité pourrait,

[1454] Conformément à la protection du droit au respect de la vie privée et du droit à la protection des données à caractère personnel ainsi qu'à la liberté d'expression ou encore au secret des correspondances.
[1455] BCE, « Report on digital euro », *op. cit.* Requirement n°10, p.20, disponible sur ecb.europa.eu
[1456] En d'autres termes, à l'opposé d'une MDBC, les espèces sont presque impossibles à censurer une fois qu'ils ont été physiquement distribués aux citoyens, car les échanges en pair à pair sont majoritairement anonymes et intraçables.
[1457] Processus d'identification des clients (« *Know Your Customer* – KYC ») permettant une identification systématique des utilisateurs de services financiers, conformément aux Directives : Directive 2009/110/CE du 16 Septembre 2009 (en vigueur) ; Directive 2015/849/CE du 20 mai 2015 (en vigueur) ; Directive 2013/36/CE du 26 Juin 2013 (en vigueur) ; Directive 2018/1673/CE du 23 Octobre 2018 (en vigueur) ; Directive 2018/843/CE du 30 Mai 2018 (en vigueur) ; Directive 2019/1153/CE du 20 juin 2019 (en vigueur).
[1458] STACHTCHENKO Alexandre, BALVA Claire, « Bitcoin & Cryptomonnaies Faciles - Comprendre Les Monnaies Numériques Et Leurs Enjeux Économiques », Éd. First, 2022.
[1459] CNIL, « Livre Blanc n°2 », *op. cit.* p.21., « En outre, reflétant par-là la polysémie du terme 'identité', il existe plusieurs niveaux d'identification, allant de l'anonymat de l'usage des espèces à l'identité régalienne certifiée par les pouvoirs publics en passant par l'identité déclarative ou pseudonyme via un login et mot de passe. Dans la plupart des actes de paiement en situation contractuelle, l'usage d'un identifiant déclaratif auprès du commerçant ou du service souscrit suffit et une 'sur-identification régalienne' à des fins d'authentification ne serait pas souhaitable ».

certes, être bénéfique pour les États qui pourraient ainsi encourager la consommation ou l'épargne, mais cela introduit le risque d'une utilisation de ces mécanismes à des fins plus ou moins pragmatiques d'un point de vue conceptuel.

Il convient d'insister sur le fait que lorsqu'une personne n'a pas la capacité de réaliser des transactions financières privées, elle perd une partie de ses droits. La liberté financière ou l'accès à une monnaie d'échange fiable est ainsi intimement lié à de nombreux autres droits (travailler, se déplacer, se soigner). Si cette liberté et ces droits sont globalement acquis dans les pays développés dont les monnaies sont fiables, ce constat semble beaucoup plus nuancé dans de nombreux pays en voie de développement. Pour ces derniers, les frais de transfert élevés imposés par les intermédiaires financiers sont par exemple un obstacle insurmontable pour de nombreuses populations, ainsi à la recherche d'alternatives. Certains crypto-actifs stables contribuent donc à réduire considérablement ces frais et in fine à améliorer la situation financière et la vie de ces individus. Il s'agit d'une solution particulièrement utile pour les citoyens des pays en voie de développement qui sont les plus touchés par les coûts élevés de transfert de fonds. Aujourd'hui, l'actif cryptographique le plus éprouvé et fiable sur Internet est le bitcoin. Ses possibilités informatiques étudiées en Annexes (Lightning Network, Taro)[1460], son indépendance politique et sa résilience globale en font un actif à vocation monétaire utile pour s'échanger des biens ou des services en toute confiance via Internet. Pourtant, sa volatilité demeure un frein à son adoption globale en tant que monnaie. Il semble ainsi qu'il ne puisse pas se substituer au système financier traditionnel, mais plutôt qu'il contribue à le réinventer comme le démontre les nombreux projets de lancement de MNBC à travers le monde. Le système traditionnel de paiements est fractionné par nature avec tout un écosystème d'acteurs pour autoriser, réaliser puis enregistrer les paiements, tandis que la blockchain Bitcoin réunit conceptuellement tout cela sur un seul et même registre numérique et public. En pratique, Bitcoin ne pourrait à court terme supporter la totalité des transactions annuelles réalisées par les systèmes de paiements actuels. A moyen et long terme, plusieurs possibilités existent et permettraient de répondre à de tels besoins, sous couvert d'une acceptation sociale et politique, y compris sur le plan énergétique également étudié dans l'Annexe 6[1461]. Plus globalement, depuis environ 2013, les annonces politiques à charge contre le secteur des crypto-actifs – stables ou instables - semblent se multiplier, à tort et à raison. A tort, concernant les capacités et applications informatiques et économiques des protocoles Bitcoin et Ethereum[1462], mais à juste titre concernant leur inadéquation juridique et leur adoption monétaire incertaine pour l'instant. Pour illustration, la Banque des Règlements Internationaux (« Bank for International Settlements – BIS »), qui a la charge de

[1460] V. Annexe 3, Focus 4.
[1461] V, Annexe 6, Focus 1.
[1462] Depuis 2018, la Banque de France estime que « bitcoin n'est ni plus ni moins qu'un objet spéculatif », DUPUY Caroline, « Cryptomonnaies : comment ça marche ? », 2018, in *Les Nouvelles Publications*, disponible à l'adresse suivante, *v.* également « Guerre crypto-économique, MNBC, stablecoins : Que fait la Banque de France ? » Cryptoast, 2022 [Vidéo]. YouTube.

promouvoir la coopération monétaire et financière internationale au regard des MNBC[1463], estime dans un bulletin de juin 2022 que « *les blockchains* (…) *présentent des externalités de réseau négatives. Plus un utilisateur donné effectue de transactions sur une blockchain, plus il encombre le système, et plus les frais de transaction sont élevés pour tous les autres. Même si tout le monde voulait effectuer des transactions dans la même crypto-monnaie, la congestion entraînerait la prolifération de nouvelles monnaies* »[1464]. Dans son rapport annuel de la même année[1465], un tableau comparatif démontre une supposée supériorité de la vision de la BRI pour le système monétaire du futur. En effet, huit critères déterminants pour tout système monétaire y sont cités[1466] pour comparer chronologiquement (i) le système monétaire actuel, (ii) l'alternative des crypto-actifs et (iii) la vision de la BRI concernant le système monétaire optimal pour l'avenir (MNBC). D'après ce tableau et ces données de la BRI, le constat est sans appel : le système monétaire traditionnel ne respecterait actuellement qu'un critère sur huit, tandis que les crypto-actifs deux sur huit et enfin les systèmes de MNBC supposément huit sur huit. Il semble donc que ces résultats puissent être relativisés en raison de l'innovation continue du secteur des crypto-actifs et de multiples paramètres et constats qu'évoque cette thèse. Par conséquent, le constat de ce rapport qui met en lumière l'avenir prometteur des MNBC repose sur un postulat relativement orienté, car institutionnellement motivé par la volonté de conserver l'ordre financier actuel et son fonctionnement oligopolistique. L'objectif des MDBC est factuellement de concurrencer les crypto-actifs pour que le système financier traditionnel ne risque pas de voir son rôle actuel, prédominant, largement redéfinis. Pour écarter cela, politiques et régulations sont à l'œuvre, sous couvert de justifications parfois contestables[1467] et orientées en faveur des monnaies MNBC pourtant dispensables à l'heure actuelle. Il semble encore une fois que les propos de la puissance bancaire à l'égard des crypto-actifs ont une portée subjective et politique, et trop peu objective et éducative à l'heure actuelle. Il est suggéré dans cette étude que si la valeur d'une monnaie repose sur son usage massif, alors bitcoin est une monnaie certes imparfaite, mais sans doute en devenir. L'usage de bitcoins par un groupe grandissant d'utilisateurs lui confère une valeur sociale et économique quasi certaine dont

[1463] CNNum, « Anonymat et universalité : les enjeux clés du développement de monnaies numériques », entretien avec Eric Monnet (Directeur d'études à l'EHESS), « Les Etats-Unis et l'Europe en sont au même point sur ces questions. Ils soutiennent à la fois une volonté d'accélérer la régulation, notamment autour des bitcoins, et d'émettre une monnaie de banque centrale. Cette posture est partagée par l'ensemble des banques centrales des pays industrialisés qui se regroupent autour de la Banque de règlements internationaux. », disponible à l'adresse suivante

[1464] BOISSAY Frederic, CORNELLI Giulio, DOERR Sebastian, FROST Jon, traduction libre de l'anglais, « Blockchain scalability and the fragmentation of crypto », BIS Bulletin n°56, 7 juin 2022, disponible en ligne à l'adresse suivante, p.7.

[1465] BIS, « Annual Economic Report 2022 », p.77, disponible à l'adresse suivante

[1466] *Ibid.* « sécurité et stabilité, responsabilité, efficacité, inclusion, contrôle des données par les utilisateurs, intégrité, adaptabilité, ouverture ».

[1467] Par exemple, de nouvelles règles de droit communautaire visent à limiter directement les paiements en crypto-actifs via l'introduction d'un plafond de 1000 euros en dessous duquel l'anonymat demeure, et au-dessus duquel l'identification sera systématique et obligatoire. De telles règles freinent ainsi le potentiel d'adoption monétaire du bitcoin qui n'a pas été conçu pour s'adapter à un cadre juridique particulièrement strict. v. article de Jean-Luc, « Le Parlement européen souhaite plafonner les paiements en actifs numériques », « Pour restreindre les transactions en espèces et en crypto-actifs, les députés souhaitent plafonner les paiements qui peuvent être acceptés par les personnes fournissant des biens ou des services. Ils fixent des limites allant jusqu'à 7000 euros pour les paiements en espèces et 1000 euros pour les transferts de crypto-actifs pour lesquels le client ne peut pas être identifié. », 2023, disponible sur bitcoin.fr

la reconnaissance monétaire serait une fonction croissante de son adoption[1468]. Il est souligné à ce propos que le bitcoin a déjà cours légal dans deux juridictions (le Salvador[1469] et la République Centre Africaine[1470]), où des biens et services peuvent y être négociés. Bien que la légitimité démocratique de ces pays puisse être remise en question par les puissances occidentales, l'utilisation du bitcoin permet à ces pays de s'ouvrir sur l'univers informatique pour finalement représenter une source de croissance économique et sociale pour ceux-ci. De façon informatiquement et socialement plausible, mais politiquement utopique en l'état des puissances bancaires et gouvernementales mentionnées, le bitcoin pourrait en lieu et place d'une MNBC permettre de réintroduire de la rareté dans le système économique et numérique de la société. Remarquons qu'un euro cryptographique aurait pour vocation première d'être un moyen de paiement, et non pas d'investissement, comme l'amalgame est pourtant souvent réalisé. En partant de ce postulat, un euro 3.0 ne concurrencerait donc bitcoin que sur le segment des paiements et non pas sur celui de l'investissement qui n'entre pas dans son objet. Dès lors, il semble finalement possible et souhaitable de ne plus opposer Bitcoin aux MNBC, au profit de leur complémentarité et en raison de leur coexistence à venir. La résilience informatique et la rareté cryptographique intrinsèque font de Bitcoin un contre-pouvoir monétaire qui libère les personnes sur le plan financier et partiellement social, à la condition que les acteurs du système financier et économique actuel le permettent dans une certaine mesure. En phase de pré-lancement, il semble encore tôt pour affirmer le bienfondé juridique et social du déploiement massif d'un euro cryptographique et de ses futurs liens avec les crypto-actifs. Les crypto-actifs stables déjà en circulation et accessibles au sein de l'UE feront l'objet d'une attention et d'un contrôle particulier de la part du législateur européen, étant donné leur positionnement particulièrement concurrentiel. Finalement, il semble impératif de garantir une stricte protection de l'anonymat lors du déploiement probable d'un euro cryptographique, afin d'assurer la continuité en ligne du modèle physique d'une monnaie sonnante et trébuchante qui a déjà fait ses preuves en termes de consensus social. Au regard de l'adoption progressive du bitcoin, seule son adoption sociale pourrait lui permettre de devenir un bien commun cryptographique et peut être monétaire, c'est-à-dire une monnaie cryptographique universelle, en dépit de son cours instable et de sa reconnaissance légale à ce jour minoritaire à l'international.

[1468] V. Annexe 3, Focus 1, 2, 3 et 6.
[1469] V. Annexe 5.
[1470] Les Echos, « Le bitcoin devient une monnaie officielle en Centrafrique », 2022, disponible à l'adresse suivante

Conclusion de la seconde partie

La seconde partie de cette étude a permis d'introduire et d'approfondir les concepts, le fonctionnement et le potentiel des standards informatiques d'une identité numérique de troisième génération, dont le rôle sera déterminant pour l'avenir 3.0 de l'Internet. L'hypothèse d'une identité juridique et numérique renforcée par la transparence et l'ouverture de ces nouvelles normes cryptographiques se confirme, à la condition qu'elle s'accompagne d'une forme d'intermédiation de l'identité numérique, non pas totalement décentralisée, mais plutôt distribuée sur le plan informatique et social. Une analyse juridique du Règlement eIDAS et de sa proposition d'amendement (eIDAS-2) met en lumière la cohérence entre la garantie des identités juridiques en ligne et celles hors ligne des citoyens européens. Avec l'avènement des technologies convergentes et des règles de droit qui leur sont bientôt applicables, certaines recommandations structurelles et complémentaires sont suggérées pour encadrer et préserver les technologies 3.0, que leur vocation soit financière ou bien identitaire. L'analyse pratique de certains projets hautement décentralisés montre que si l'atteinte d'une identité numérique universelle est désormais informatiquement possible, ce concept demeure pour l'heure utopique en raison de la diversité des systèmes juridiques et politiques, parfois peu ou pas harmonisés dans les pays concernés par cette notion. Il est donc possible d'émettre des preuves d'existence décentralisées sur des blockchains publiques, mais pour qu'elles soient légalement reconnues par un ou plusieurs systèmes juridiques, il est essentiel que soient impliquées les autorités publiques dans les processus de délivrance d'identités numériques. Ainsi, cette délivrance et reconnaissance devient informatiquement distribuée plutôt que décentralisée dès lors qu'une entité est reconnue juridiquement. En France et dans l'Union européenne, les corps politiques et législatifs doivent progressivement distinguer les notions de décentralisation informatique qui concerne l'identité numérique, de celle qui concerne les crypto-actifs. Ces deux cas d'usage sont pour l'instant distincts, et pourtant largement confondus par ces institutions et par voie de conséquence par le grand public. Cela renforce le fait que le temps de la régulation ne doit pas être réduit à celui de l'innovation, souvent plus rapide et immature comme le démontrent la majorité des solutions 3.0, trop souvent supposées décentralisées et fiables. Il s'agit également de ne pas bannir les infrastructures et les technologies les plus ouvertes et décentralisées, car un degré de décentralisation minimum devrait toujours être possible et accessible aux internautes en besoin ou en recherche d'émancipation et/ou de liberté(s) numérique(s).

Conclusion

Le périmètre de la notion d'identité est si vaste qu'il doit être circonscrit afin d'être analysé au regard de la philosophie, des sciences sociales et des règles de droit. À travers l'observation de quelques formes historiques d'expression de l'identité des personnes, il a été démontré que l'identité a toujours été socialement organisée et centralisée auprès de systèmes et d'institutions sociales hiérarchiquement structurés. Chaque être humain produit son identité en même temps qu'il produit l'identité collective de ses semblables, selon un ou plusieurs curseurs spécifiques à chaque culture et société. Aujourd'hui, à mesure que le besoin d'identité croît avec la population mondiale, les frontières de l'identité s'élargissent à l'ère digitale. Alors que de nombreuses solutions numériques 2.0 et désormais 3.0 existent, des millions de personnes peinent toujours à prouver leur identité et ne bénéficient pas de ce droit pourtant fondamental. La présente étude a suggéré que l'identité doit être appréhendée en fonction de ses contextes d'utilisation, soit individuellement, soit collectivement ou les deux selon les cas d'usage. Est introduit le concept d'une identité globale en référence à la fois aux sentiments d'identité subjectifs que peut ressentir chaque personne ainsi qu'à leur identité juridique fixée par l'état civil. Ces notions s'avèrent aussi indispensables que complexes à définir tant elles fluctuent selon les environnements socioculturels. Dès lors trois composantes interdépendantes à toute identité ont été privilégiées comme champs d'étude : l'identité biologique, l'identité juridique et l'identité psychosociale. Pour simplifier, ces composantes ont été regroupées en deux catégories, la première désignant des attributs d'identité primaires (identité biologique et juridique) et la seconde désignant des attributs d'identité secondaires (identité psychosociale).

Il a été démontré que la confiance et l'intermédiation sont intimement liées et jouent un rôle crucial dans le Web 2.0, chaque internaute devant faire confiance à de multiples fournisseurs d'identité et de services en ligne pour leur permettre d'exprimer leur identité numérique et pour interagir avec celles d'autres utilisateurs. L'étude du contexte technologique et du cadre légal de l'identité numérique en Europe a ainsi permis de constater certaines limites spécifiques à l'identité numérique 2.0. Le constat d'une redéfinition du Web 2.0, c'est-à-dire d'un renforcement de l'identité en ligne avec certaines nouvelles technologies du Web 3.0 apparaît comme une nécessité pour les internautes. En effet, les technologies blockchains et l'identité numérique décentralisée (IND) donnent un nouveau sens et renforcent la notion fondatrice de confiance numérique, grâce à de nouveaux mécanismes de transmission de données plus sécurisés. Ces nouvelles technologies façonnent un nouvel environnement informatique inédit pour l'expression et la revendication en ligne des droits des citoyens, notamment au soutien d'une liberté financière sans précédent et d'une confidentialité programmée des données. Les internautes de plus en plus nombreux qui détiennent des crypto-actifs sont par exemple susceptibles de détenir des attestations cryptographiques vérifiables, c'est-à-dire d'adopter une identité primaire distribuée et une identité secondaire - financièrement - décentralisée. Cette étude fait le constat d'un besoin de libérer l'identité

numérique et sociale des personnes tout en renforçant l'exercice de leurs droits lors de leur navigation en ligne. En l'état des technologies et de leurs applications actuelles, il devient urgent pour les cybernautes de passer d'une identité numérique passive à une identité numérique active. Pour cela, il est encouragé que chaque citoyen réalise un examen de son identité numérique, comme le suggérait en 1998 l'académicien français Amin Maalouf à propos de notre identité globale et psychosociale.

Cette étude a proposé de réfléchir au prochain type de société numérique souhaitée avec ses moyens informatiques distribués et décentralisés, de façon équilibrée. Elle introduit et encourage un regard informatique et juridique pragmatique et actualisé sur ces nouvelles technologies 3.0 et leurs applications, loin des idées reçues. Cette étude démontre également qu'une décentralisation informatique n'est pas opportune dans tous les cas. Néanmoins, un haut degré de décentralisation informatique demeure toutefois essentiel pour la confiance accordée par exemple aux monnaies cryptographiques, boucliers numériques et pour certains droits fondamentaux. Ce phénomène de décentralisation informatique n'est ainsi atteint que par une poignée de réseaux informatiques, comme aujourd'hui avec la blockchain Bitcoin. Ce qui paraît le plus opportun est de chercher à décentraliser, et finalement à désintermédier certains domaines d'activités comme celui de l'identité numérique. Il demeure en 2023 un lien indissociable entre les concepts informatiques de blockchains et ceux de crypto-actifs, un constat également valable pour les blockchains privées et hybrides qui se trouveront probablement tokenisées à l'avenir grâce aux monnaies digitales de banques centrales, dont les mécanismes seront légalement reconnus et technologiquement centralisés par la puissance publique. Ainsi, l'opposition entre des briques technologiques 3.0 ouvertes versus fermées risque de s'intensifier au regard des textes et des règles de droit en cours d'adoption, et partiellement alimentés par une volonté politique de contrôle et d'encadrement de ces phénomènes sociaux de décentralisation numérique initialement conçue pour le peuple et au service de son émancipation en ligne.

L'adoption croissante des crypto-actifs par les entreprises, les particuliers et par quelques (quasi)États démontre l'émulation socio-économique qu'entraîne certaines applications distribuées (levées de fonds en crypto-actifs, émission de jetons stables, sociétés décentralisées). Cependant, la facilité avec laquelle un internaute peut créer un jeton ou une application numérique décentralisée est souvent perçue par le législateur comme un risque pour l'investisseur et le citoyen. C'est la raison pour laquelle les premiers textes fondateurs pour l'avenir de ces technologies 3.0 voient le jour en Europe. C'est pour l'instant le cas pour l'identité décentralisée et les crypto-actifs, aux fins d'encadrer ces écosystèmes et leurs acteurs, au point de contraindre directement ou indirectement les écosystèmes des infrastructures les plus décentralisées. Pour les acteurs de l'écosystème des crypto-actifs dont le degré de décentralisation est faible ou moyen, leur mise en conformité règlementaire sera dans les prochaines années leur principale priorité (MiCA, TFR), car leur survie globale en dépend. Ce constat est également partagé pour l'identité numérique décentralisée (RGPD, eIDAS-2, Data Act), tout particulièrement lorsque des attributs d'identité primaire seront impliqués pour identifier des personnes physiques. Cette recherche introduit

une nouvelle grille de lecture concernant les technologies blockchains à l'aune de l'identité numérique et d'une finance 3.0, leur proposant de coexister à divers degrés de décentralisation, des plus conformes aux règles de droit (blockchains fermées) aux plus ambitieuses et parfois non conformes (blockchains ouvertes). Il semble vain de tenter de contrôler toutes ces expressions technologiques, sans cesse en évolution, surtout pour celles dont les protocoles sont pensés avec un haut degré de résilience et de décentralisation informatique. Certains pays comme la France adoptent progressivement un cadre légal qui, certes, est source de sécurité juridique et attire de nouveaux acteurs étrangers, mais qui génère en même temps de nombreuses contraintes pour les acteurs de ces écosystèmes du Web 3.0. Le risque est ainsi de rendre moins compétitifs ces acteurs français au profit d'acteurs étrangers plus solides financièrement et commercialement en raison de systèmes juridiques plus souples et moins contraignants. En théorie, l'enjeu de ce renforcement et durcissement récent du cadre règlementaire applicable aux crypto-actifs[1471] est d'assurer une application effective et équitable à tous les acteurs de cet écosystème, y compris ceux étrangers qui s'adressent au marché français sans enregistrement légal (PSAN) comme cela a été analysé dans cette étude.

Finalement, un équilibre doit être trouvé pour que les crypto-actifs ne forment pas un monde à part de la société, mais plutôt l'une de ses nouvelles dimensions à venir. Il est souhaitable de penser le droit en fonction des cas d'usage des technologies blockchains, c'est-à-dire avec des règles juridiques et des outils cryptographiques adaptés au concept de décentralisation. Une règlementation unique et mondiale applicable aux technologies blockchains a été écartée, car il existe en réalité de multiples variantes pour chaque technologie 3.0, autant que de règles de droit parfois contradictoires. Dès lors, ce ne sont pas les technologies qu'utilisent les blockchains qu'il s'agit d'encadrer, mais surtout leurs usages. Les liens entre le concept de responsabilité personnelle et cryptographique prôné par le Web 3.0 (« *lex cryptographia* »), et l'intervention d'un tiers rend complexe la compréhension des internautes. En effet, plus une solution est décentralisée et moins elle est intuitive pour ses utilisateurs, et ceux qui sont les moins bien formés au numérique préfèreront faire confiance à un tiers compétent en lui déléguant sa responsabilité cryptographique sur ses crypto-actifs et/ou attributs d'identité. La confiance numérique implique ainsi toujours une confiance sociale et il appartient au législateur d'équilibrer l'articulation entre ces deux perceptions possibles tant au niveau de la responsabilité, qu'au cas par cas selon le niveau de décentralisation de la solution 3.0.

Cette étude a conclu à une distinction informatique et conceptuelle entre la notion d'identité numérique décentralisée (IND) et celle d'identité numérique auto-souveraine (INAS). Comprendre l'identité numérique décentralisée implique de bouleverser sa perception actuelle de l'identité numérique. L'utilisateur évolue depuis un schéma où son identité est relativement statique, enfermée et dépendante d'un service en ligne, vers un nouveau schéma dynamique où il devient le propriétaire cryptographique

[1471] ADAN, « Enregistrement renforcé des PSAN : quel bilan après le vote du projet de loi DDADUE ? », 2023, in *adan.eu*, disponible en ligne

de chacune de ses données et traces numériques. Ce passage d'une identité informatique centralisée 1.0 et 2.0, vers une identité décentralisée et 3.0, ouvre de nouvelles perspectives pour chaque relation et interaction en ligne. Elle favorise ainsi l'accès et la communication en ligne, mais aussi hors ligne, tout en réduisant les risques d'usurpation d'identité ou encore de violations de données. L'utilisation d'identifiants cryptographiques pseudo-anonymes, partiellement propriétaires et minimisés par conception en vertu du RGPD, confère aux utilisateurs de ce nouveau concept technologique de sérieux avantages par rapport à l'existant. Couplée à une technologie blockchain légalement reconnue, l'IND augmente et assure la transparence et la qualité des données échangées. En cours de reconnaissance juridique, politique et industrielle à l'échelle de l'UE (eIDAS-2), l'IND représentera d'ici quelques années un nouveau socle de protection cryptographique indispensable aux citoyens européens. Pourtant, la France est en retard concernant cette récente brique technologique qui manque de reconnaissance et de soutien politiques en comparaison à d'autres pays européens comme l'Allemagne et l'Espagne. Pour le moment, il faudra encore du temps pour que l'idée d'une confiance numérique 3.0 soit acceptée par la conscience générale au point de faire l'unanimité. En effet, l'informatique distribuée ou décentralisée attire autant qu'elle éblouit. En attendant son adoption, elle crée une forme de résistance pour ceux qui sont habitués aux systèmes de confiance centralisés et qui peinent à s'y détacher. Le haut degré de décentralisation attaché au concept d'identité numérique auto-souveraine introduit le concept d'une identité numérique universelle. Couplé à une blockchain publique, le concept d'INAS pourrait pour la première fois permettre la naissance d'une identité numérique universellement accessible et ouverte. En d'autres termes, l'utilisation d'IND ou d'INAS permettrait de fournir une preuve d'existence universelle à chaque être humain, leur permettant d'accéder à des droits également décentralisés, tel qu'un revenu universel en crypto-actifs par exemple. Cette preuve d'existence cryptographique doit néanmoins être rattachée à des droits fondamentaux, que seul un État de droit peut garantir.

Dès lors, si atteindre une identité numérique universelle est souhaitable grâce à une blockchain publique qui hébergerait des preuves d'existence numériques infalsifiables, cette possibilité semble pour l'instant utopique en raison du manque de maturité et de reconnaissance du Web 3.0. Par conséquent, seule une preuve d'existence attachée à une identité numérique distribuée et semi-centralisée, permet un lien légalement reconnu avec un tiers de confiance fournisseur d'identité et de facto d'une reconnaissance légale. Cette étude privilégie le recours à des identités distribuées, c'est-à-dire informatiquement hybrides plutôt que complètement décentralisées. Aujourd'hui, une majorité des situations d'identification en ligne requiert pour l'instant des attributs d'identité civile, provenant nécessairement d'un tiers de confiance souvent public et étatique. Sans l'avènement de métavers décentralisés ou de quasi-États autoproclamés, la lex cryptographia chère au Web 3.0 ne peut à elle seule être retenue, car elle ne peut pas couvrir et garantir à elle seule toute la complexité des relations sociales. Pour autant, elle contribue sans doute à les améliorer en offrant de nouvelles alternatives et perspectives numériques, notamment pour les attributs d'identité en ligne des internautes.

Le marché des registres électroniques décentralisés ou distribués est actuellement porté par les blockchains ouvertes qui sont privilégiées par les petites entreprises innovantes pour des raisons économiques (besoin de financement), commerciales (recherche d'un effet de réseau), informatiques (résilience) ou plus marginalement règlementaires (recherche des juridictions les moins contraignantes). À l'heure actuelle, il s'agit de se recentrer depuis une perception occidentale des blockchains publiques, vers une perception plus pragmatique de leur importance et nécessité au sein des pays en voie de développement. Par voie de conséquence, contraindre les blockchains publiques en Occident par le droit revient à empêcher leur adoption légale et sociale dans les pays en voie de développement, qui en ont le plus besoin. Dans ces pays où les États peuvent être instables ou corrompus, une blockchain publique représente un registre électronique ouvert et de confiance, dont les fonctionnalités identitaires et monétaires offrent de nouvelles méthodes de gouvernance. Dès lors, les blockchains publiques représentent une forme de contre-pouvoir et de bien commun numérique universel, dont les pays développés peuvent également bénéficier en cas de dégradation ou de recul de la démocratie.

Pourtant, il est également nécessaire de reconnaître que les blockchains publiques n'ont pas toutes la capacité de répondre à certains enjeux de la société, notamment concernant l'identité numérique primaire et régalienne qui impose pour l'instant le recours à des blockchains privées ou hybrides. Ainsi, aucune infrastructure décentralisée ne peut prétendre répondre à tous les besoins et cas d'usage comme cela est souvent promis par certains acteurs du Web 3.0. Inversement, aucune blockchain privée ou hybride ne peut se prétendre, ni se qualifier d'infrastructure décentralisée, mais tout au plus distribuée. Une perception équilibrée et contextualisée de chaque technologie est donc nécessaire pour qualifier au plus proche de la réalité les enjeux juridiques de ces contextes et de leurs solutions financières et/ou identitaires 3.0. Nous avons également observé que plus une technologie blockchain possède de fonctionnalités, c'est-à-dire héberge un grand nombre de cas d'usages, plus sa surface et sa probabilité d'attaque informatique sont importantes. Si aucune blockchain publique n'est ainsi à l'abri d'une faille ou d'une violation informatique, leur communauté et gouvernance les en éloignent considérablement par rapport aux blockchains privées et hybrides. En parallèle, plus une solution décentralisée est adoptée par un grand nombre d'utilisateurs à travers le monde, plus elle est susceptible d'être strictement encadrée par le législateur. Finalement, toutes les approches réglementaires discutées dans cette étude sont des solutions partielles et imparfaites étant donné l'évolution constante de ces nouvelles technologies. Il s'agit en réalité de ne pas interdire, mais plutôt de préserver certains primitifs de la technologie blockchain afin d'observer si de nouveaux modèles sociaux et numériques peuvent naître, comme cela fut le cas pour le protocole Bitcoin.

Cette recherche suggère que ce protocole représente une révolution copernicienne, car sa création transforme radicalement le système monétaire et financier actuel, tout comme la découverte de Copernic a bouleversé la compréhension de l'univers au XVIè siècle au point d'impacter chacune de ses générations futures. Il a été démontré en Annexes que Bitcoin tend plus à être une infrastructure au

service d'un bien commun universel, qu'une infrastructure pirate destinée à des finalités illicites comme cela est souvent présentée par les médias puis compris par le grand public. La révolution monétaire, financière et probablement identitaire qu'illustre l'infrastructure Bitcoin ne doit ni être favorisée, ni interdite[1472], mais plutôt tolérée et étudiée avec une grande attention par les acteurs publics et privés de la société. L'examen de certains projets inédits, portés par de grandes entreprises technologies comme les sociétés Microsoft (projet ION), Twitter (projet tbDEX) ou encore certaines mises à jour informatiques (Lightning Network, Ordinals), laissent présumer que le potentiel et l'adoption de l'infrastructure Bitcoin n'en sont qu'à leurs débuts. L'étude de l'histoire des technologies démontre effectivement que ce qui semblait inimaginable hier, comme la reconnaissance du bitcoin comme monnaie légale au Salvador, pourrait bien être incontournable demain. Cette recherche estime qu'il serait opportun de ne plus sous-estimer ni discriminer les blockchains publiques. Pour l'instant, le Web 3.0 est d'ailleurs principalement fondé sur ces infrastructures ouvertes, dont seule la blockchain Bitcoin est en réalité stable, fiable, transparente et éprouvée, et susceptible de perdurer contrairement aux nombreuses autres applications et promesses décentralisées du Web 3.0. Le temps est venu d'initier un débat démocratique pragmatique concernant les apports et les enjeux – informatiques, économiques et sociaux – que Bitcoin emporte pour notre société ultra-numérisée, encore fragile. En attendant, les meilleures armes pour que Bitcoin gagne sa place dans la société en luttant contre les attaques politiques et institutionnelles sont l'information et l'éducation des internautes. Pour savoir si les internautes et les citoyens préféreront une infrastructure informatique décentralisée et résiliente, mais peu conforme au droit et monofonctionnelle, ou bien une infrastructure centralisée dotée de multiples fonctionnalités et conforme aux règles de droit, mais peu résiliente, notre étude suggère que les internautes privilégieront une blockchain résiliente pour la monnaie 3.0 (Bitcoin) et moins résiliente pour leur identité numérique 3.0 (blockchains fermées), chacune répondant à des besoins et à des usages différents. Bien que l'internaute ait un besoin naturel de faire confiance à un tiers pour gérer son identité et ses finances à l'ère du Web 2.0, il s'agit également de ne pas négliger sa capacité à (re)prendre le contrôle de ses données numériques, surtout avec l'avènement de nouvelles technologies 3.0 qui lui permet désormais en toute confiance de le faire.

En résumé, la société numérique a besoin d'infrastructures blockchains avec un haut degré de décentralisation (blockchains publiques), et d'infrastructures plus flexibles, moins décentralisées (blockchains privées et hybrides). Il s'agit finalement de ne pas confronter ces variantes technologiques, mais plutôt de chercher à les comprendre aux fins de favoriser leur complémentarité et convergence, car

[1472] La Banque Centrale Européenne (BCE) a publié sur son site internet un article scientifique permettant de prendre l'ampleur de son positionnement politique à l'encontre des mécanismes informatiques de la Preuve de travail (PoW) qu'utilise le protocole Bitcoin « (…) si une approche non interventionniste de la part des pouvoirs publics est possible [concernant le PoW], elle est hautement improbable, et une action politique de la part des autorités (par exemple, des exigences de divulgation, une taxe carbone sur les transactions ou les avoirs en crypto, ou une interdiction pure et simple de l'exploitation minière) est probable. », MITSU Adachi, et al., « Stablecoins' role in crypto and beyond: functions, risks and policy », 2022, in *European Central Bank*, disponible à l'adresse suivante

leurs différents niveaux de décentralisation répondent tout simplement aux différents besoins de décentralisation dont la société a besoin. Si tout ne peut pas être décentralisé, tout peut être plus transparent. Ainsi, cette recherche contribue à mettre fin à l'habillage idéologique que subit chacune de ces variantes technologiques. Pour autant, l'orientation de notre étude démontre que les blockchains privées et hybrides sont plus adéquates que les blockchains publiques pour implémenter à court et moyen termes des solutions d'identité numérique décentralisée. Cela s'explique par un faible coût par transaction, une conformité règlementaire programmée et une interopérabilité plus importante avec des systèmes informatiques et cas d'usage conventionnels (1.0 et 2.0). Ce constat s'observe par le choix de ce type d'infrastructure pour de multiples consortiums européens comme la prochaine blockchain européenne (EBSI), la blockchain espagnole (Alastria), et française (l'Alliance Blockchain France). Il est important de souligner que dans le cas où un État implémenterait sa propre blockchain privée, comme en Estonie, il convient comme pour toute nouvelle technologie, d'adopter une vigilance accrue afin d'écarter toute gouvernance algocratique, c'est-à-dire toute dérive concernant l'utilisation de ces technologies 3.0 (contrôle ou surveillance de masse, dictature par les chiffres[1473])[1474]. En définitive, cette étude souligne qu'il est vraisemblable que les blockchains privées et hybrides soient amenées à cohabiter avec les blockchains publiques, voire à fusionner dans un temps long. Une telle fusion ne serait possible qu'à la condition que les blockchains publiques tiennent leurs promesses de résilience, d'efficience énergétique et d'évolutivité informatique, tout en anticipant l'éventuelle suprématie quantique (4.0) étudiée.

À propos de ces technologies 4.0 et 5.0 évoquées à titre subsidiaire, mais par anticipation technologique, il convient de ne pas sous-évaluer leurs capacités à devenir des sujets fondamentaux à l'avenir, tant elles sont susceptibles d'évoluer dans les années futures. Face à l'avènement de toutes ces nouvelles technologies susceptibles de s'imbriquer, l'adoption continue d'une posture critique, mais objective, s'impose à leur égard. Il s'agit de les défier régulièrement et méthodiquement dans leurs composantes conceptuelles et informatiques afin de comprendre avec précision leurs conséquences et particulièrement les règles de droit les concernant. Cette étude confirme que chaque nouvelle technologie n'est qu'un nouveau support et un outil à la disposition des personnes, dont l'utilisation et les finalités subjectives entraînent des effets duals pour l'ensemble de la société. Le juriste et professeur

[1473] CLAESSENS Michel, « Science et communication, pour le meilleur ou pour le pire ? », chap. La dictature du chiffre, Éd. Quæ, 2009, pp.103-141.

[1474] De FILIPPI Primavera, « Lorsqu'elles sont contrôlées par un gouvernement centralisé et autoritaire, les caractéristiques distinctives d'une blockchain - en termes de résilience, de résistance à la falsification et d'exécution automatique - pourraient conduire à des situations où des acteurs puissants décident d'incorporer leur propre ensemble de règles dans un système basé sur la blockchain, de sorte que toute personne souhaitant interagir avec ce système n'aura d'autre choix que de se conformer à ces règles. Cela pourrait finalement contribuer à étendre le pouvoir des régimes rigides et autoritaires, qui obtiendraient une plus grande capacité à contrôler leurs citoyens par le biais d'une série de règles auto-exécutées basées sur des codes », in *Blockchain and the Law*, *op. cit.*, Ed. Kinde, emplacement 3973 sur 7004.

au Collège de France Alain Supiot estime ainsi que « *le problème est de savoir comment mettre nos outils à notre service au lieu de penser que nous sommes fabriqués sur le modèle de nos outils* »[1475].

Si les nouvelles technologies ne sont effectivement que des outils au service de l'Homme, la responsabilité est autant individuelle que collective pour atteindre une utilisation respectueuse des technologies au respect des droits et libertés individuels, et d'un développement de l'informatique au service du bien commun. À ce titre, le sujet désormais incontournable de l'impact énergétique et de l'utilité sociale attribuée aux technologies 3.0 ne doit pas être laissé pour compte par les acteurs de ces écosystèmes technologiques. Au contraire, il doit être approfondi et examiné avec un pragmatisme scientifique couplé à une diversité des points de vue, pour devenir une priorité. Leur avenir dépend effectivement de l'acceptation sociétale qui sera progressivement ou non attribuée au rapport coût/bénéfice spécifique à chacune des technologies 3.0. Tant concernant l'empreinte énergétique des solutions d'IND, dont les volumes de données traitées sont importants, qu'à propos de l'impact énergétique des blockchains publiques et de leurs crypto-actifs, un temps long sera nécessaire pour obtenir des conclusions fiables et objectives. Pour conclure, il s'agit d'adopter une perspective optimiste et confiante en l'avenir au motif que la question de défense et de revendication de droits numériques n'a jamais autant été traitée qu'aujourd'hui, et que ces nouvelles technologies 3.0 contribuent à renforcer les droits des personnes en ligne. Plus les citoyens seront nombreux à reprendre le contrôle sur leurs données identitaires et financières, c'est-à-dire à comprendre leur importance, plus cet éveil de la société numérique s'imposera aux grandes entreprises technologiques et aux Etats qui devront accepter que ces identités numériques ne leur appartiennent plus. Il est ainsi possible que les choix technologiques s'imposent par les besoins et les usages 3.0 de ces marchés numériques, dictés par les internautes, et non par les pouvoirs institués, de sorte que finalement « o*n résiste à l'invasion des armées, on ne résiste pas à l'invasion des idées* »[1476].

***

[1475] CNNum, « Compte-rendu d'un échange avec Alain Supiot, professeur au Collège de France », publié le 24 septembre 2021, in *cnnumerique.fr*, consulté le 29 mars 2021.

[1476] HUGO Victor, « Histoire d'un crime, déposition d'un témoin », texte établi par J.M. Hovasse et G. Rosa, disponible à l'adresse suivante, p.592.

Bibliographie

I - Lois, actes juridiques, jurisprudence et doctrine

1.1 Lois, articles de lois, ordonnances et autres actes juridiques

Art. L102 du Code des postes et des communications électroniques, Légifrance, disponible en ligne

Déclaration des Droits de l'Homme et du Citoyen de 1789, Conseil constitutionnel, disponible à l'adresse suivante

Code de la consommation, Livre Ier : information des consommateurs et pratiques commerciales, art. L111-1 à L141-2, Légifrance, disponible à l'adresse suivante

Code civil, Art. 1188, Légifrance, disponible à l'adresse suivante

Code civil, Art. 2061, Légifrance, disponible à l'adresse suivante

Code de procédure civile, Chapitre Ier : La compétence d'attribution, art. 33 à 41, Légifrance, disponible à l'adresse suivante

Code pénal, Art. 226-4-1 - Légifrance, disponible à l'adresse suivante

Code monétaire et financier, Art. L54-10-1, Légifrance, disponible à l'adresse suivante

Loi du 8 août 1893 relative au séjour des étrangers en France et à la protection du travail national, disponible à l'adresse suivante

Loi n° 72-3 du 3 janvier 1972 sur la filiation, disponible à l'adresse suivante

Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, disponible à l'adresse suivante

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (1), (LOPPSI), JORF n°0062 du 15 mars 2011, disponible à l'adresse suivante

Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1), (PACTE), JORF n°0119 du 23 mai 2019, disponible à l'adresse suivante

Loi n° 2023-171 du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture, (DDADUE), JORF n°0059 du 10 mars 2023, disponible à l'adresse suivante

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Disponible à l'adresse suivante

Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, disponible à l'adresse suivante

1.2 Décrets

Ministerio del interior, Real Decreto 1553/2005, de 23 de diciembre, por el que se *regula la expedición del documento nacional de identidad y sus certificados de firma electrónica*, 2005, disponible à l'adresse suivante

Décret n° 2022-1212 du 2 septembre 2022 relatif à l'entrée en vigueur de la loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à Internet.

Décret n°2022-1620 du 23 décembre 2022 relatif à la signature des déclarations des formalités des entreprises, à la consultation du Registre national des entreprises et à la radiation de certaines entreprises.

Décret n°2023-63 du 3 février 2023 relatif à la vérification de l'identité de la clientèle pour certains produits et services à faible risque de blanchiment de capitaux et de financement du terrorisme.

1.3 Arrêtés

Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », Légifrance, disponible à l'adresse suivante

1.4 Règlements de l'UE

Règlement (UE) **n°910/2014** du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ou **eIDAS (Electronic IDentification And trust Services)**. Disponible à l'adresse suivante

Règlement d'exécution (UE) **n°2015/1502** de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) no910/2014 du Parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Disponible à l'adresse suivante

Règlement (UE) **n°2016/679** du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ou **RGPD (Règlement Général sur la Protection des Données)**. Disponible à l'adresse suivante

Proposition de Règlement (UE) **n°2020/0265** du Parlement et du Conseil du 24 septembre 2020 sur les marchés de crypto-actifs et modifiant la directive (UE) 2019/1937 ou **MiCA (Market in Crypto-Assets)**. *(Non promulguée à la date du 15/04/2023)*. Disponible à l'adresse suivante.

Proposition de Règlement (UE) **n°2020/0340** du Parlement européen et du Conseil du 25 novembre 2020 sur la gouvernance européenne des données (acte sur la gouvernance des données) ou **DGA (Data Governance Act)**. Disponible à l'adresse suivante

Proposition de Règlement (UE) **n°2020/0374** du Parlement européen et du Conseil du 15 décembre 2020 relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) ou **DMA (Digital Market Act)**. Disponible à l'adresse suivante

Proposition de Règlement (UE) **n° 2021/0136** du Parlement européen et du Conseil du 3 juin 2021 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique ou **eIDAS-2 (Electronic IDentification And trust Services)**. Disponible à l'adresse suivante

Proposition de Règlement (UE) **n°2021/0241** du Parlement européen et du Conseil du 20 juillet 2021 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs (refonte) ou **TFR (Transfer of Funds Regulation)**. *(Non promolguée à la date du 15/04/2023).* Disponible à l'adresse suivante

Proposition de Règlement (UE) **n°2022/0032** du Parlement européen et du Conseil du 8 février 2022 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs (règlement sur les semi-conducteurs). Disponible à l'adresse suivante

Proposition de Règlement (UE) **n°2020/0047** du Parlement européen et du Conseil du 23 février 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) ou **Data Act**. Disponible à l'adresse suivante

Règlements (UE) **no 2022/858** du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) n°600/2014 et (UE) no 909/2014 et la Directive 2014/65/UE (texte présentant de l'intérêt pour l'EEE) ou **Régime Pilote DLT (Distributed Ledger technology)**. Disponible à l'adresse suivante

Règlement (UE) **n°2022/2065** du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) ou **DSA (Digital Service Act)**. Disponible à l'adresse suivante

1.5 Directives

Directive (UE) **95/46/CE** du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible à l'adresse suivante

Directive (UE) **2015/849** du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le Règlement (UE) no 648/2012 du Parlement européen et du Conseil et abrogeant la Directive 2005/60/ce du Parlement européen et du Conseil et la Directive 2006/70/ce de la commission. Disponible à l'adresse suivante

Directive (UE) **n°2015/2366** du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les Directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le Règlement (UE) no 1093/2010, et abrogeant la Directive 2007/64/CE. Disponible à l'adresse suivante

Directive (UE) **2019/1024** du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte). Disponible à l'adresse suivante

1.6 Jurisprudence et doctrine

ACPR (FLICHE olivier, URI Julien, VILEYN Mathieu), *Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire*, document de réflexion, avril 2023. Disponible à l'adresse suivante

CE, *La Commission propose une identité numérique fiable et sécurisée*, Communiqué de presse du 3 juin 2021, disponible à l'adresse suivante

CEF Digital, *eIDAS-Node Demo Tools Installation and Configuration Guide v2.6 (pre-release)*, 2021, disponible à l'adresse suivante

CJUE, *Un contrat de fourniture de services de télécommunication contenant une clause selon laquelle le client a consenti à la collecte et la conservation de son titre d'identité ne peut démontrer qu'il a valablement donné son consentement lorsque la case y afférente a été cochée par le responsable de traitement avant la signature du contrat*, sur *Communiqué de presse n°137/20*, Arrêt dans l'affaire C-61/19 Orange România SA/Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 11 novembre 2020, disponible à l'adresse suivante

CNIL, *Règlement européen sur la protection des données : ce qui change pour les professionnels*, disponible à l'adresse suivante

CNIL, *Sanctions (RGPD)*, disponible à l'adresse suivante. CNIL, *Sanctions (RGPD)*, 2011-2023, disponible à l'adresse suivante

CNIL. *Cookies : la CNIL incite les organismes privés et publics à auditer leurs sites web et applications mobiles*, 2021, disponible en ligne

Commission d'enrichissement de la langue française**,** *Vocabulaire des actifs numériques (liste de termes, expressions et définitions adoptés)*, JORF, no 13, 15 janv. 2021.

Commission staff working document impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council amending regulation (eu) n° 910/2014 as regards establishing a framework for a european digital identity, disponible à l'adresse suivante

CONSEIL DE L'EUROPE (G'SELL Florence, MARTIN-BARITEAU Florian), *L'impact des blockchains sur les droits de l'homme, la démocratie et l'Etat de droit*, 2022, disponible à l'adresse suivante

CONSEIL DE L'EUROPE et CRID (POULLET Yves et DINANT Jean-Marc), *Comite consultatif de la convention pour la protection des personnes a l'égard du traitement automatisé des données à caractère personnel (t-pd) rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications l'autodétermination informationnelle à l'ère de l'internet*, 2004, disponible à l'adresse suivante

CONSEIL D'ÉTAT, *Étude annuelle 2014 - Le numérique et les droits fondamentaux*, disponible à l'adresse suivante

DALLOZ, *Lexique des termes juridiques*, 2017-2018, disponible à l'adresse suivante

European Data Protection Board, Article 29 Working Party, 2018, disponible à l'adresse suivante

Groupe de travail « article 29 » sur la protection des données, *Avis 4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, disponible à l'adresse suivante

HCDH, *Pacte international relatif aux droits civils et politiques*, 1976, disponible à l'adresse suivante

Humanium, *Déclaration de Genève sur les Droits de l'Enfant*, 1924, disponible à l'adresse suivante

IAPP (DESAI Anokhy), *US State Privacy Legislation Tracker*, disponible à l'adresse suivante

Notaires de France. *Le numérique, accompagner et sécuriser L'Homme. La révolution digitale et le droit*, 117ème Congrès des Notaires de France, 2021, Présentation disponible à l'adresse suivante et Rapport (*Chapitre I – Le développement de la cryptoéconomie*) disponible à l'adresse suivante

OMPI, Résumé de la Convention de Berne pour la protection des œuvres littéraires et artistiques (1886), disponible à l'adresse suivante

Parlement européen. *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* Etude du Parlement Européen, Panel for the Future of Science and Technology.Scientific Foresight Unit (STOA). EPRS | European Parliamentary Research Service, 2019, disponible à l'adresse suivante

Règlementation LCB-FT : synthèse des principales mesures devant être mises en œuvre par les prestataires de services sur actifs numériques, disponible à l'adresse suivante

ROLLAND Paul, *Les Modes Alternatifs de Règlement des Différends (MARD) : à chacun sa voie*, sur Village de la Justice. 2020. Disponible à l'adresse suivante

U.S. Government Publishing Office, *Biometric identifiers and the modern face of terror: new technologies in the global war on terrorism, hearing before the subcommittee on technology, terrorism, and government information of the committee on the judiciary united states senate one hundred seventh congress*, first session, november 14, 2001. Disponible à l'adresse suivante

UNICEF, *Convention internationale des droits de l'enfant*, 1990, disponible à l'adresse suivante

Groupe de travail 29, *Avis 3/2012 sur l'évolution des technologies biométriques*. Disponible à l'adresse suivante

Cour de cassation, civile, Chambre civile 1, 3 novembre 2016, 15-22.595, Publié au bulletin | La base Lextenso, disponible en ligne

CNIL, *Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail*, Légifrance, disponible à l'adresse suivante

CA de Montpellier, Civ. 2ème ch., 21 octobre 2021, N°RG 21/00224, in *Actualité Droit Propriété Intellectuelle Technologie de l'information Innovation* - Cabinet Simon et Associés Avocats, disponible à l'adresse suivante

II – Ouvrages et chapitres d'ouvrages

AÏDAN Geraldine, **DEBAETS Emilie**, *L'identité juridique de la personne humaine*, éd. L'Harmattan, coll. Logiques Juridiques, 2013.

ALFORD Richard D, *Naming and identity: a cross-cultural study of personal naming practices*, HRAF Press, 1988.

AMMOUS Saifedean, *L'étalon Bitcoin*, éd. Dicoland (LMD), 2019.

ANTONOPOULOS Andreas, *Mastering Bitcoin 2nd Edition*, éd. O'Reilly Media, 2015.

ANTONOPOULOS Andreas, *The Internet of Money*, éd. Kindle, 2016.

AZAN Wilfrid, CAVALIER Georges, *Des systèmes d'information aux blockchains* : *Convergence en sciences juridiques, fiscales, économiques et de gestion*. Larcier, coll. Droit et économie, 2021.

BELLANGER Pierre, *La souveraineté numérique*, éd. Stock, 2014.

BERGER Peter, **LUCKMANN Thomas**, *La construction sociale de la réalité*, Ed. Armand Colin, coll. Individu et Société, 2018.

BERNARD Alain, *L'identité des personnes physiques en droit privé : Remarques en guise d'introduction*, p. 29.

BERTHOZ Alain, **DEBRU Claude**, *Anticipation et prédiction : du geste au voyage mental*, Odile Jacob, 2015.

BISMUTH Yves, *Le droit de l'informatique*, éd. L'Harmattan, 4e édition, 2017.

BLONDIAUX Loïc, **KANTOROWICZ Ernst**, *Les deux corps du Roi*, éd. Gallimard, 1989, Politix. Revue des sciences sociales du politique, 2, Persée - Portail des revues scientifiques en SHS, 1989, n° 6, p. 84-87, disponible à l'adresse suivante

BOUILLET-CORDONNIER Ghislaine, **MOULIN Jean-Marc**, **QUINIOU Matthieu**, **GASSER Axel et al**. *La finance numérique : aspects juridiques et fiscaux du crowdfunding et des cryptoactifs*, Ed. EFE, 2021.

CATALA Pierre, *Le droit à l'épreuve du numérique : jus ex machina*, 1e édition, PUF, coll. Droit, éthique, société, 1998.

CONSTANT Benjamin, *De la liberté des anciens comparée à celle des modernes*, éd. Mille et une nuits, coll. 1001 Nuits Petite Collection, 2010.

COTIGA-RACCAH Andra, **JACQUEMIN Hervé**, **POULLET Yves**, *Les blockchains et les smart contracts à l'épreuve du droit*, 1éd. Larcier, coll. CRIDS, 2020.

CRETTIEZ Xavier, **PIAZZA Pierre**, *Du papier à la biométrie. Identifier les individus*, Sciences Po Presses, 2006.

CRUET Jean. *La philosophie morale et sociale de Destutt de Tracy (1754-1836) / Jean Cruet*. BNF/Gallica. 1909.

De FILIPPI Primavera, WRIGHT Aaron, *Blockchain and the Law: The Rule of Code*, éd. Harvard University Press, 2018.

DESCOMBES Vincent, *Les embarras de l'identité*, éd. Gallimard, coll. NRF Essais, 2013.

DUBAR Claude, *La crise des identités, l'interprétation d'une mutation*, éd. PUF, coll. Le lien social, 2010.

DUMA Jean, *Norbert Elias et La Société des individus, Histoires de nobles et de bourgeois : individus, groupes, réseaux en France. XVII et XVIII siècles*, Nanterre, Presses universitaires de Paris Nanterre, 2016, p. 17-31. Disponible à l'adresse suivante

DURKHEIM Émile, *Éducation et sociologie*, éd. PUF, coll. Quadrige, 2013.

DURKHEIM Émile, *Leçons de sociologie. Physique des mœurs et du droit*, 157p.

EYNARD Jessica et al. *L'identité numérique ; quelle définition pour quelle protection ?* Ed. Larcier, coll. Création information communication, 2020.

FAVIER Jacques. **LECRIVAIN Jean-Samuel** et **TAKKAL-BATAILLE Adli**, *Bitcoin et protocoles à blockchain. Comprendre l'avènement de la seconde ère numérique*, Mardaga, coll. « Gestion, Entreprise, Finance », 2019.

FRUMKIN Daniel, *Bitcoin Mining Handbook*, éd. Braiins Publishing, 2022.

FUNES (de) Julia, *Quand l'identité devient un piège*, éd. La Montagne, 2023.

GARAPON Antoine et **LASSEGUE Jean**, *Justice digitale : révolution graphique et rupture anthropologique*, PUF, 2018.

GAYON Jean, **NICOGLOU Antoine**, **PONTAROTTI Gaëlle et al**. *L'Identité*. Dictionnaire encyclopédique Gallimard. Folio Essai, 2020.

GUILLAUME Florence, **MAHON Pascal**, *Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ?* Helbing Lichtenhahn Verlag, 2021.

GUILLAUME Florence, **MAHON Pascal**, **ROUSSEL Alexis et al**. *Réelle innovation ou simple évolution du droit ? le droit à l'intégrité numérique*, Université de Neuchâtel, Éd. Helbing, Lichtenhahn, 2020.

ITEANU Olivier, *Quand le digital défie l'Etat de droit*, éd. Eyrolles, 2016.

ITEANU Olivier, **SALVATORY Olivier**, *L'identité numérique en question : 10 scénarios pour une bonne gestion juridique de son identité sur internet*, éd. Eyrolles, 2008.

JEAN Aurélie, *Les algorithmes font-ils la loi ?* Ed. De L'Observatoire, 2021.

KAKU Michio (auteur), **DEPOVERE Paul** (traduction), *L'avenir de l'humanité*, éd. De Boeck Supérieur, coll. Hors collection Sciences, 2019.

KHATCHATOUROV Armen, *Les identités numériques en tension. Entre autonomie et contrôle*, 2019, ISTE Editions.

KLUMOV Gregory, *Digital asset regulation. a cross-country analysis*, 2019.

KUNDERA Milan, *L'identité*, éd. Gallimard, 1998.

LANGLOIS-BERTHELOT Thibault et al. *La Finance Numérique : aspects juridiques et fiscaux du crowfunding et des cryptoactifs*, EFE Edition, pp.147-151, 2021, disponible à l'adresse suivante

LANGLOIS-BERTHELOT Thibault et al. *Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés*. Dans *Blockchain et Cryptos | 60 experts vous expliquent tout*, IS EDITION, pp.516, 2022, Wallcrypt, Chapitre disponible à l'adresse suivante

LASSEGUE Jean, **GARAPON Antoine**, *Justice digitale*, PUF, 2018.

LEGEAIS Dominique, *Blockchain et actifs numériques*, LexisNexis, coll. « Actualité », 2019.

LOCKE John. *Property: John Locke, Second Treatise, Chap. 16 §§ 25--51, 123--26*, 1689.

LOISEAU Grégoire, *Droit des personnes - 2e édition mise à jour et augmentée*, Ed. ELLIPSES, 12 mai 2020.

LOISEAU Grégoire, *Précis de culture juridique* (dir. F.-X. Lucas et T. Revet), 6e éd., 2022, p.135.

LOURIMI Alexandre, BARBET-MASSIN Alice, O'RORKE William, PION Claire, FLEURET Faustine, *Droit des crypto-actifs et de la blockchain*, éd. LexisNexis, 2020.

MAALOUF Amin, *Les identités meurtrières*, éd. Grasset, 1998.

MAUSS Marcel, *La Nation*, éd. Minuit, 1920, disponible à l'adresse suivante

MONEGER Françoise, *Droits de l'enfant*, éd. DALLOZ, 2017.

MOROZOV Evgeny, *Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique*, Fyp éditions, 2014.

MUCCHIELLI Alex, *L'identité*, éd. Presses Universitaires de France, coll. Que sais-je ? 2009.

NISSENBAUM Helen, *Privacy in context: technology, policy, and the integrity of social life*, Stanford University Press, 2009, p. 304

NOIZAT Pierre, *Bitcoin Book*, éd. Kindle, 2012.

NOIZAT Pierre, *Bitcoin, mode d'emploi*, éd. Lulu.com, 2015.

PIKETTY Thomas, *Le capital au XXIe siècle*, Ed. Seuil, coll. les livres du nouveau monde, ISBN : 978.2.02.108228.9, 2013.

PREUKSCHAT Alex, **REED Drummond**, *Self-Sovereign Identity : decentralized digital identity*, début de publication en décembre 2019 et publication finale à l'été 2020, ISBN 9781617296598.

RADLEY-GARDNER Oliver, **BEALE Hugh** et **ZIMMERMANN Reinhard** (dir.), *Fundamental Texts On European Private Law*, Hart Publishing, 2020.

REY Olivier, *Leurre et malheur du transhumanisme*, éd. Les Carnets DDB, 2020.

RICOEUR Paul, *Soi-même comme un autre*, Ed. Seuil, 1990.

SIMMEL Georg, *Philosophie de l'argent*, éd. Quadrige, 2014.

STACHTCHENKO Alexandre, **BALVA Claire**, *Bitcoin & cryptomonnaies faciles - comprendre les monnaies numériques et leurs enjeux économiques*, EAN13 : 9782412081716, Éditeur First, 2022.

STACHTCHENKO Alexandre, BALVA Claire, JEANNEAU Clément, YERETZIAN Antoine, *La blockchain décryptée – les clefs d'une révolution*, éd. Netexplo, 2016.

STIEGLER Bernard, *L'attention, entre économie restreinte et individuation collective*, éd. L'économie de l'attention: Nouvel horizon du capitalisme ?, 2014, pp. 121-135.

SUPIOT Alain, *Homo juridicus : essai sur la fonction anthropologique du droit*, Seuil, 2005.

SUPIOT Alain, *La gouvernance par les nombres*. Cours au Collège de France (2012-2014), Coll. Poids et mesures du monde, Ed. Fayard, 2015.

TAPSCOTT Alex, **TAPSCOTT Don**, *How the technology behind Bitcoin is changing money, business, and the world in Blockchain revolution*, ISBN 9781101980132.

TELLER Marina, *L'avènement de la Deep Law (vers une analyse numérique du droit ?)*, 2020.

TOCQUEVILLE Alexis, *Le despotisme démocratique*, éd. L'HERNE, 2009.

ZUBOFF Shoshana, *The age of surveillance capitalism*, éd. Kindle, 2019.

III - Travaux de mémoires et de thèses

ALSAEDI Musabbeh. *Les émirats arabes unis et la révolution numérique. Nouveaux defis pour le droit public, le droit privé et le droit pénal*. Thèse de doctorat en droit. Université Paris I Panthéon-Sorbonne

BARBET-MASSIN Alice. *Le droit de la preuve à l'aune de la blockchain*. Thèse de doctorat en droit. Université de Lille, 2020, disponible à l'adresse suivante

CONSTANTINO FERREIRA Leonel. *La résolution des litiges blockchain. Vers un arbitrage décentralisé ?* Mémoire de Master, Université de Neuchâtel, 2021, disponible en ligne

DIOP Mame Mariama. *La sécurisation du marché des services de paiement*. Thèse de doctorat en droit. Université de Lille, 2015, disponible en ligne

DOERK, Adrian. *The growth factors of self-sovereign identity solutions in Europe*. Bachelor Thesis. 2020. Disponible à l'adresse suivante

EDDEROUASSI Meryem. *Le contrat électronique International*, Thèse de doctorat en droit. Université Grenoble Alpes, 2017, disponible en ligne

ELIE Pauline, *Analyser l'identité en droit : comment protéger et définir un nouveau territoire à l'ère dématérialisée ?* v. Thèse en cours à l'EHESS, disponible à l'adresse suivante

FOUQUET Kévin, *L'état civil sénégalais aujourd'hui de l'enregistrement à l'archivage*, Mémoire Master 1, 2020, Université d'Angers, disponible à l'adresse suivante

GASSER Axel, *Le financement alternatif de la transition énergétique (aspects juridiques)*, projet de thèse en Droit privé sous la direction de Jean-Marc Moulin, Université de Perpignan.

GUILLEBON Thibaud. *Les monnaies virtuelles : essai sur l'intégration d'une nouvelle classe d'actifs dans les concepts fondamentaux du droit privé*, Université de Bordeaux, 2022, disponible en ligne

HOANG Van-Hoan. *Securing data access and exchanges in a heterogeneous ecosystem: An adaptive and context-sensitive approach*. Cryptography and Security Thesis. Université de La Rochelle, 2022. English. Disponible à l'adresse suivante

JULIEN Marine. *La confiance numérique dans le domaine bancaire*. Thèse de doctorat en droit. Université de La Rochelle, 2022, disponible à l'adresse suivante

LANGLOIS-BERTHELOT Thibault. *Les méthodes de légalisation et de blanchiment des activités mafieuses*, Mémoire Master 2, Université Paris Nanterre & EHESS, disponible à l'adresse suivante

LASSEGUE Jean, *L'intelligence artificielle et la question du continu; Remarques sur le modèle de Turing*, Thèse de philosophie, Université de Nanterre – Paris X, 1994, disponible à l'adresse suivante

LEE David. *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups*, University of California, 1982, disponible à l'adresse suivante

LEHMAN Constance. *Essai sur le prix et la valeur en droit des contrats*. Thèse de doctorat en droit. Université Paris-Saclay, 2022. Français. Disponible en ligne

LEVENEUR Claire. *Les smart contracts : étude de droit des contrats à l'aune de la blockchain.* Thèse en droit. Université Paris 2, 2022, disponible à l'adresse suivante

LOPAMUDRA Mandal, *Ricardian contract : Bridging the Gap Between Smart Contracts and Traditional Contracts*, Master Thesis, International Business Law, juin 2019, p.10, disponible en ligne à l'adresse suivante

SZTULMAN Marc. *Biométrie et libertés : contribution à l'étude de l'identification des personnes*, Thèse de doctorat en droit, Université Toulouse 1, 2015, disponible à l'adresse suivante

IV - Articles de revues et journaux

ALLISON Arthur, **CURRALL James E. P**, **MOSS Michael**, **STUART Susan**. *Digital identity matters*, 2005, Journal of the American society for information science and technology. Disponible à l'adresse suivante

AMR Jacques, PASQUALINI François, De VAUPLANE Hubert et al, *Dettes de l'Etat, dettes des entreprises : quel avenir ?* Ed, Bruylant, coll. Droit & Economie, 2023.

ANCIAUX Arnaud, **FARCHY Joëlle**, *Données personnelles et droit de propriété : quatre chantiers et un enterrement*, Revue internationale de droit économique, novembre 2015, n° 3, p. 307-331, disponible à l'adresse suivante

BARBET-MASSIN Alice, *Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien*, Revue Lamy droit de l'immatériel (WoltersKluwer), n°157, 2019.

BELGA. *Des algorithmes plus transparents : l'UE va les réclamer à Facebook et Google*, sur *RTBF Info*, 2020, disponible à l'adresse suivante

BENOÎT-GUILBOT Odile, **EVERETT Rogers**, *Diffusion of innovations*, Revue française de sociologie, 5, Persée - Portail des revues scientifiques en SHS, 1964, n° 2, p. 216-218. Disponible à l'adresse suivante

BERTRAND-MIRKOVIC Aude, *La notion de personne*, Presses universitaires d'Aix-Marseille, 2003.

BOULLIER Dominique, *Puissance des plateformes numériques, territoires et souverainetés*, Sciences Po, Centre d'Etudes Européennes et de Politique Comparée, 2021, disponible à l'adresse suivante

BOUSQUET Marc, *Tout savoir sur le Bitcoin et les cryptomonnaies*, Dossiers Science Hors-Série, édition du Sens, ISSN : 2802-1843, 2022, 65 pages.

BUTERIN Vitalik, *On Nathan Schneider on the limits of cryptoeconomics*, article en ligne, 2021, disponible à l'adresse suivante

BUTERIN Vitalik, *The Limits to Blockchain Scalability*, article en ligne, 2021, disponible à l'adresse suivante

CARDON Dominique, *L'identité comme stratégie relationnelle*, Hermes, La Revue, n° 53, 2009, n° 1, p. 61-66, disponible à l'adresse suivante

CEYHAN Ayse, *Lutte contre le terrorisme : la technologie n'est pas neutre*, Revue internationale et stratégique, n° 74, juin 2009, n° 2, p. 18-27, disponible à l'adresse suivante

CHAMBARDON Nicolas, *L'identité numérique de la personne humaine. Contribution à l'étude du droit fondamental à la protection des données à caractère personnel*. Thèse de doctorat en droit, Université Lumière-Lyon-2, Revue des droits et libertés fondamentaux, 2019, résumé disponible à l'adresse suivante

CHARDEL Pierre-Antoine, DARTIGUEPEYROU Carine, *Être, temps et différences : pour une approche différencialiste du temps à l'ère numérique*, 2018, Ed. Nicole Aubert, in *la recherche du temps: Individus hyperconnectés, société accélérée : tensions et transformations*, pp. 95-110.

CHARDEL Pierre-Antoine, *L'éthique dans la société technologique : un défi pédagogique majeur*, 2014, Ed. Edwige Rude-Antoine, in *Un état des lieux de la recherche et de l'enseignement en éthique*, l'Harmattan, pp. 131-146.

COROT Léna. *Apple part à l'assaut de Zoom et Teams et dévoile un portefeuille d'identité numérique*, sur *Usine-digitale.fr*. 2021. Disponible à l'adresse suivante

De MOMBYMES Yorick., *Anarchie, cypherpunk et liberté : les racines philosophiques du bitcoin*, in Contrepoints.org, 17 mars 2018. Disponible à l'adresse suivante

De VAUPLANE Hubert, *Quelle régulation pour les offres publiques en cryptomonnaies (ICO) ?* Revue Banque, n°810, 2017.

De VAUPLANE Hubert. *La blockchain défiera-t-elle la règle ?* RDBF, n°6, 2016, p.115.

DEFFAINS Bruno, *Blockchain – Pour un open source responsable !* in *Lexisnexis*, La semaine du droit n° 14, 6 avril 2021, disponible à l'adresse suivante

DOUVILLE Thibault, *Blockchains et preuve*, Ed. Dalloz, 2018.

DUPUY, Caroline. *Cryptomonnaies : comment ça marche ?* Les Nouvelles Publications. 2018. Disponible à l'adresse suivante

EGE Ragip, *À propos de l'ouvrage de Karl Marx : contribution à la critique de l'économie politique. Introduction aux Grundrisse dite « de 1857*, Cahiers d'économie Politique, n° 70, octobre 2016, nº 1, p. 163-166, disponible à l'adresse suivante

FERRIÉ Scarlett-May, *Le droit à l'autodétermination de la personne humaine: essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, IRJS éditions, 2018.

FERRY Luc. *La fin de l'individu, vraiment ?* sur *LEFIGARO*, publié le 23 octobre 2019, disponible à l'adresse suivante

France Culture. *Héraclite, on n'entre jamais deux fois dans le même fleuve - Ép. 1/4 - Du nouveau ?* 2017. Série audio disponible à l'adresse suivante

GEORGES Fanny, *Représentation de soi et identité numérique*, Réseaux, n° 154, avril 2009, nº 2, p. 165-193, disponible à l'adresse suivante

Id., *Le design de la visibilité*, Réseaux, n° 152, 2008, nº 6, p. 93-137, disponible à l'adresse suivante

JEAN Aurélie, *Pourquoi Facebook doit rester en dehors du métavers*, sur *Le Point*, 2021, disponible à l'adresse suivante

KLIPPENSTEIN Ken et **SIROTA Sara**, *The Taliban Have Seized U.S. Military Biometrics Devices*, sur *The Intercept*, 2021, disponible à l'adresse suivante

KOENIG Gaspard, *La propriété de soi*, Revue des juristes de sciences po - n°17 – juin 2019, disponible à l'adresse suivante

KRYPTOSPHERE®. *KryptoPaper : Blockchain & crypto*, 2022, sur LinkedIn, disponible à l'adresse suivante

LARDELLIER Pascal, **BRYON-PORTET Céline**, *Ego 2.0*, Les Cahiers du numérique, Vol. 6, juillet 2010, nº 1, p. 13-34, disponible à l'adresse suivante

LASSEGUE Jean, *Le droit automatisé et le problème de la délibération collective*, Dalloz IP / IT Droit de la propriété intellectuelle et du numérique Numéro 1 - Janvier 2022, Dossier, p. 12. *Justice par la Blockchain*, disponible à l'adresse suivante

LE HEN Solène. *Trois questions sur la nouvelle carte d'identité qui entre en vigueur lundi 2 août*, sur *Franceinfo*, publié le 2 août 2021, disponible à l'adresse suivante

LEGEAIS Dominique. « L'apport de la Blockchain au droit bancaire », RDBF, janv. 2017, p. 5.

LOW Kelvin F.K., **MIK Eliza**, *Pause the Blockchain Legal Revolution*, 22 août 2019, revu 6 avril 2020, in International & Comparative Law Quarterly 135-175, disponible à l'adresse suivante

MAUGER Gérard. *A. Strauss, Miroirs et masques. Une introduction à l'interactionnisme*, in Politix, vol. 6, n°21, 1er trimestre 1993. Représentations de Paris. pp. 142-146, disponible à l'adresse suivante

MESURE Sylvie, *Le lien social à l'épreuve de l'individualisme le « culte de l'individu chez Durkheim »*, Revue internationale de philosophie, n° 280, avril 2017, no 2, p. 157-180, disponible à l'adresse suivante

MIRHADY David C., *Aristotle and the Law Courts*, in Polis: The Journal for Ancient Greek Political Thought, 23, 2006, no 2, p. 1/17, disponible à l'adresse suivante

MOEREL Lokke et **TIMMERS Paul**, *Reflections on Digital Sovereignty*, sur EU Cyber Direct, 2021, disponible à l'adresse suivante

NAKAMOTO Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 oct. 2008, disponible à l'adresse suivante

NEWTON Casey, *Mark Zuckerberg is betting Facebook's future on the metaverse*, sur *The Verge*, 22 juillet 2021, disponible à l'adresse suivante

NOUR Soraya et **LAZZERI Christian**, *L'intégration parreconnaissance del'identité : l'héritage freudien*, sur Presses universitaires de Paris Nanterre, 2009, disponible à l'adresse suivante

PARGAMIN David, *Les réseaux sociaux font payer la fin de l'anonymat*, Revue Challenges n° 776, 2 mars 2023, p. 34 et 35.

PARGAMIN David, *Sur la piste des voleurs de cryptomonnaies*, Revue Challenges n°779, 23 mars 2023, p. 46 et 47.

PARK Sunoo, **SPECTER Michael**, **NARULA Neha**, **RIVEST Ronald L**. *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, MIT, 2020, disponible à l'adresse suivante

PELLEGRINI François, **VITALIS André**, *La création du fichier biométrique TES : la convergence de logiques au service du contrôle*, Sociologie, PUF, décembre 2017, no N° 4, vol. 8, disponible à l'adresse suivante

PERRET Virgile, *Monnaie et citoyenneté : une relation complexe en voie de transformation*, sur Etudes internationales, 2011, disponible à l'adresse suivante

SPIVAC Simon, *Claude Lévy-Strauss, La pensée sauvage*, Revue Tiers Monde, 5, Persée - Portail des revues scientifiques en SHS, 1964, no 19, p. 596-597, disponible à l'adresse suivante

SUBTIL Romain. *Protection des données personnelles : la Californie s'inspire de l'Europe*, sur *La Croix*, 2018, disponible à l'adresse suivante

VERBIEST Thibault, *Technologies de registre distribué (blockchain) : premières pistes de régulation*, RLDI, no 129, 2016, p. 52.

WOITIER Chloé. *Facebook et Ray-Ban dévoilent leur paire de lunettes connectée, les Ray-Ban Stories*, sur *LEFIGARO*, publié le 8 septembre 2021, disponible à l'adresse suivante

World Bank Group. *Cross-practice initiative: Identification for Development*. Flyer, 2015, disponible à l'adresse suivante

WRIGHT Aaron, **De FILIPPI Primavera**, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015.

ZOLYNSKI Célia, *La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne*, Dalloz IP/IT, 2020.

V – Articles, études, rapports, vidéos et pages en ligne

ABRAMOV Oleg, **BEBELL Kirstin L**. et **MOJZSIS Stephen J**. *Emergent Bioanalogous Properties of Blockchain-based Distributed Systems, in Origins of Life and Evolution of Biospheres*, 51, juin 2021, nº 2, p. 131-165, disponible à l'adresse suivante

Académie Française. *Identité*, Dictionnaire de l'Académie française, disponible à l'adresse suivante

ADAN et **KPMG**, *La crypto en France : structuration du secteur et adoption par le grand public*, 2022, disponible à l'adresse suivante

AFLALO Jérémie, **MILLERAND Arthur**, **LECLERC Michel**. *Le numérique peut-il sauver la démocratie ?* sur *Third* et *PARALLEL AVOCATS*, 2021, disponible à l'adresse suivante

Alliance pour la Confiance Numérique, *Collectif pour la Feuille de route Nationale sur l'identité numérique*, 2014, disponible à l'adresse suivante

ANDERBERG, A. ANDONOVA, E. BELLIA, et al. Publications Office of the European Union, Luxembourg, 2019, disponible à l'adresse suivante

ANGELI Guillaume, **SFEZ Betty**, **CHOUTEAU Vincent**, **Broustail Alain** pour SOLEGAL et Blockchain EZ Livre blanc *L'utilité de la signature électronique sur blockchain publique pour les grands comptes : intérêt, faisabilité et valeur juridique*. 2020. Disponible à l'adresse suivante

ANSSI. *Publication du référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID),* sur *ANSSI*, disponible à l'adresse suivante

AUDRAND Stéphane. *« Conquérir ou soumettre » - réflexion autour des contraintes d'une réunification "forcée" de Taïwan à la République Populaire de Chine*, sur *Theatrum Belli*. 2021, disponible à l'adresse suivante

BALL Matthew. *Framework for the Metaverse*, sur *MatthewBall.vc*, 2021, disponible à l'adresse suivante

BAMDÉ Aurélien. *Autodétermination informationnelle*, sur *A. Bamdé & J. Bourdoiseau*, disponible à l'adresse suivante

BAMDÉ Aurélien. *Les attributs du droit de propriété : l'usus, le fructus et l'abusus*, sur *A. Bamdé & J. Bourdoiseau*, 2020, disponible à l'adresse suivante

BBC. *Apple digital IDs come with conditions and costs*, sur *BBC News*. Disponible à l'adresse suivante

BECKER Katrin. *Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*. Law and Critique. 2022. Disponible à l'adresse suivante

BECKER Katrin. *La technologie blockchain et la promesse crypto-divine d'en finir avec les tiers*. Sur Etudes digitales, 2019. Disponible à l'adresse suivante

BECKER Katrin. *Lex cryptographica, smart contracts et gouvernements personnalisés : Les implications juridico-culturelles de la technologie blockchain*. Sur Grief, disponible à l'adresse suivante

BLANDIN Apolline, **PIETERS Gina**, **WU Yue**, **et al**. *3rd Global Cryptoasset Benchmarking Study*, Cambridge Center for Alternative Finance, University of Cambridge Judge Business School, 2020.

BONAZZI Hervé, **HEUDEBERT Paola**, **DROUOT Quentin et al**. *Le futur de l'identité numérique est décentralisé*, 2021, disponible à l'adresse suivante

BOTHOREL Eric, **COMBES Stéphanie**, **VEDEL Ranaud et al**. *Mission Bothorel – Pour une politique publique de la donnée*, SIRCOM, Mission confiée par le Premier ministre, 2020.

BOUFFARTIGUE Jean, *Les animaux techniciens, Rursus. Poiétique, réception et réécriture des textes antiques*, Université Nice-Sophia Antipolis, juillet 2006, nº 1, disponible à l'adresse suivante

BOUILLET-CORDONNIER Ghislaine, LANGLOIS-BERTHELOT Thibault, *Tour d'horizon du droit financier Suisse : Crowdfunding - ICO - STO, Albatross Legal*, 2021, disponible à l'adresse suivante

CAMERON Kim, *The Laws of Identity*, 2005, article disponible à l'adresse suivante

CAMPESE Sandrine. *Voltaire, le jongleur de lettres (1/2)*, sur *Le Projet Voltaire*, 2015, disponible à l'adresse suivante

CARRICK, Jon. *Bitcoin as a Complement to Emerging Market Currencies*. Emerging Markets Finance and Trade, 2016. Disponible à l'adresse suivante

CARSON Brant, **ROMANELLI Giulio**, **WALSH Patricia**, **ZHUMAEV Askhat** pour MCKINSEY. *The strategic business value of the blockchain market*, 2018, disponible à l'adresse suivante

CARUGATI Christophe, *Building an efficient regulation in the digital economy*, sur CRED, working paper n°2020-10.

Cercle du Coin. *Table Ronde du Cercle du Coin : Preuve de travail et écologie*, disponible à l'adresse suivante

CHAROLLES Valérie. *Distinguer libéralisme et capitalisme au 21ème siècle* - S&O Center HEC Paris. 2020. YouTube. Disponible à l'adresse suivante

CHM. *Internet History of 1980s | Internet History | Computer History Museum*, disponible à l'adresse suivante

CNIL. *Premiers éléments d'analyse de la CNIL - Blockchain*, 2018, disponible à l'adresse suivante

CNIL. *Quand la confiance paie : les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données*, 2021, disponible à l'adresse suivante

COURBE Thomas et al. *Les verrous technologiques des blockchains*, Rapport pour le Gouvernement de l'INRIA, CEA et l'IMT, 2021.

CROUSILLAC Jean, *Le Combat des Enfants Fantômes*, Backpack Productions, 2021, reportage disponible à l'adresse suivante.

De COETLOGUON Perrine, **DURAND Marc**, **GENIN Claire**, **BOULET Pierre**, **LANGLOIS-BERTHELOT Thibault et al**. *Les technologies blockchain au service du secteur public*, 2021, Rapport disponible à l'adresse suivante

De LA BOÉTIE Étienne, *Discours de la servitude volontaire*, disponible à l'adresse suivante

De LA RAUDIERE Laure et **MIS Jean-Michel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur les chaînes de blocs (blockchains)*, Assemblée nationale, 2018, disponible à l'adresse suivante

De MOMBYNES Yorick. *Dépolitiser la monnaie*. YouTube Conférence à Surfin' Bitcoin. 2022, disponible à l'adresse suivante

Découvre Bitcoin. Chaîne Youtube disponible à l'adresse suivante

DHAPTE Aarti, *Blockchain Identity Management Market Research Report Information by Component Type (Software, and Solution), by Provider (Application, Middleware, and Infrastructure), by Organization Size (Large Enterprises, and SMEs), by Vertical (BFSI, Telecom & IT, and Government), By Region (Asia-Pacific, North America, Europe, and Rest of the World) - Forecast till 2030*, 2023, analyse disponible à l'adresse suivante

DOMINGO Agnacio Alamillo, *SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*, European Commission & CEF Digital Connecting Europe, 2020, disponible à l'adresse suivante

Europe Finances Régulation. *La confidentialité des paiements : du xviiie siècle à l'euro numérique*, Revue d'èconomie Financière, n.°149

European Union Blockchain Observatory & Forum, *EU Blockchain Ecosystem Developments*, 2020, disponible à l'adresse suivante

EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM *Legal and Regulatory Framework of Blockchains and Smart Contracts*, 2019.

EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. *Blockchain and Digital Identity*, 2019.

EUROSMART. *Eurosmart positionpaper post quantum cryptography*, 2021, disonible à l'adresse suivante

EY-Parthenon. *Modèles économiques de l'identité numérique*, in acteurspublics.fr, 2019, disponible à l'adresse suivante

FAURE-MUNTIAN Valeria et **FASQUELLE Daniel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur les plateformes numériques*, Assemblée nationale, 2020, disponible à l'adresse suivante

GAUDIAUT Tristan. *Infographie : L'informatique entre dans l'ère quantique*, sur *Statista Infographies*, 2021, disponible à l'adresse suivante

GEORGAKOPOULOS Takis pour JP MORGAN, *Payments are eating the world*, 2021, disponible à l'adresse suivante

GHOSH Devarsi. *Meet 'Elliot Alderson' – the vigilante hacker taking down UIDAI, one tweet at a time*, sur *Scroll.in*. 2018. Disponible à l'adresse suivante

GODEFROY Lemy D., **LEBARON Frédéric**, **LEVY-VEHEL Jacques**. *Comment le numérique transforme le droit et la justice vers de nouveaux usages et un bouleversement de la prise de décision*. Rapport de recherche. Mission de recherche. Droit et Justice. 2019. Disponible à l'adresse suivante

Gouvernement. L'Agenda 2030 en FRANCE, *ODD16 - Promouvoir l'avènement de sociétés pacifiques et ouvertes aux fins du développement durable*, disponible à l'adresse suivante

GRAMLICH John. *10 facts about Americans and Facebook*, sur *Pew Research Center*, disponible à l'adresse suivante

Grand Angle Crypto. Chaîne Youtube disponible à l'adresse suivante

GREGOIRE Paul et **HILLS Adam**. *Digital Identity Theft and Online Fraud in NSW*. NSW Courts. 2020. New South Wales Courts. Disponible à l'adresse suivante

GRIGG Ian. *Financial Cryptography in 7 Layers*, disponible à l'adresse suivante

GRIGG Ian. *The Ricardian Contract*, disponible à l'adresse suivante

HAMILTON DUFFY Kim et al. *Building the digital credential infrastructure for the future,* A White Paper by the Digital Credentials Consortium, 2020, disponible à l'adresse suivante

HAO Karen. *How Facebook and Google fund global misinformation,* sur *MIT Technology Review,* 2021, disponible à l'adresse suivante

HENNEBERT Christine, **Coutor Sophie, FAHER Mourad**. *Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité'*, Rapport du Ministère de l'intérieur, 2020, disponible à l'adresse suivante

HENNION Christine et **MIS Jean-Michel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur l'identité numérique*, Assemblée nationale, 2020, disponible à l'adresse suivante

HEUDEBERT Paola, DROUOT Quentin, et al. *Le future de l'identité numérique sera décentralisé*. Livre Blanc de la société Archipels, 2021, disponible à l'adresse suivante

HUBBARD Bryan, *Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities,* sur Office of the comptroller of the Currency, 2021, disponible à l'adresse suivante

HUGUES Eric. *A Cypherpunk's Manifesto*, sur *Adam.nz*, 1993, disponible à l'adresse suivante

KRYPTOSPHERE®, *Les Ricardian contracts, l'avenir des smart contracts ?* sur *Cryptoast*, publié le 5 septembre 2020, article disponible à l'adresse suivante

KRYPTOSPHERE®, *Milton Friedman avait prédit l'air des crypto-monnaies en 1999 !* 2019. Vidéo Youtube, disponible à l'adresse suivante

KRYPTOSPHERE®. *À la découverte du mouvement cypherpunk à l'origine du Bitcoin*, sur *Cryptoast*, 2020, disponible à l'adresse suivante

L'HERMITE Marie et **STENNE Paul**, *La preuve, la blockchain et les professions réglementées*, Nuäg, 2019, disponible à l'adresse suivante

LAHER Rudy, *La numérisation des activités de l'huissier de justice*, *Cahiers Droit, Sciences & Technologies*, PUP, mai 2020, nº 10, p. 129-145, disponible à l'adresse suivante

LANDAU Jean-Pierre et **GENAIS Alban**, *Les crypto-monnaies*, Rapport au ministre de l'Économie et des Finances, 2018, disponible à l'adresse suivante

LANGLOIS-BERTHELOT Thibault et al. Partie : *Vers une identité numérique décentralisée*. Rapport 2021 de l'Observatoire de la Sécurité des Moyens de Paiement (OSMP) de la Banque de France, disponible à l'adresse suivante

LANGLOIS-BERTHELOT Thibault. *La blockchain, un nouveau fondement pour la confiance numérique ?* Observatoire d'IN Groupe, 2021, article disponible à l'adresse suivante

LANGLOIS-BERTHELOT Thibault. *Proposition d'une taxonomie française pour l'identité décentralisée*. 2021. Disponible à l'adresse suivante

LAROUSSE. *Identité bas latin identitas -atis du latin classique idem le même* - LAROUSSE, disponible à l'adresse suivante

LAW COMMISSION (UK), *Smart legal contracts: advice to government*, 2021.

LEQUESNE-ROTH Caroline. *Fiscalité des NFTs et du Metaverse - Une introduction*. Revue de droit fiscal, 2022, disponible à l'adresse suivante

LEQUESNE-ROTH Caroline. *Metavers, Web3 : la révolution juridique en trompe-l'oeil*. Receuil Dalloz, 2022. Disponible à l'adresse suivante

LITAN Avivah. *Hype Cycle for Blockchain 2021 ; More Action than Hype*, 2021, article disponible à l'adresse suivante

LOCKWOOD Mick. *An Accessible Interface Layer for Self-Sovereign Identity*, *Frontiers in Blockchain*, 2021, disponible à l'adresse suivante

MARTINSON Priit pour PWC. *Estonia –the Digital Republic Secured by Blockchain*, 2019. Disponible à l'adresse suivante

MICROSOFT. *Microsoft HoloLens | Mixed Reality Technology for Business*, 2022, disponible à l'adresse suivante

MRASILEVICI Christian. *Valérie Charolles, Se libérer de la domination des chiffres*. 2022. YouTube. Disponible à l'adresse suivante

NAKAMOTO Satoshi. V. *Profile of satoshi*, sur bitcointalk, disponible à l'adresse suivante

National Science & Technology Council. *NSTC National Strategic Overview for QUANTUM INFORMATION SCIENCE*, 2018, disponible à l'adresse suivante

Nations Unies, *Enregistrement des naissances et droit de chacun à la reconnaissance en tout lieu de sa personnalité juridique*, Assemblée générale du 19 mars 2013, Conseil des droits de l'homme : Vingt-deuxième session, disponible à l'adresse suivante

Nations Unies, *L'Assemblée générale adopte un Programme de développement durable ambitieux pour « transformer notre monde » d'ici à 15 ans* | UN Press. (2015, 25 septembre). Disponible en ligne

NETTER Emmanuel. *Blockchain et professions réglementées. Quelle place pour les professions réglementées dans la révolution numérique ?* Colloque organisé par M. Blanchard et S. Moreil, 2018, disponible à l'adresse suivante

El MADHOUN Nour, HATIN Julien, BERTIN Emmanuel, *A Decision Tree for Building IT Applications What to choose: Blockchain or Classical Systems ?* Annals of Telecommunications - annales des télécommunications, in Springer, 2021, accessible en ligne

El MADHOUN Nour, MALDONADO-RUIZ Daniel, et al., *An Innovative and Decentralized Identity Framework Based on Blockchain Technology*, The 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), in *IEEE*, 2021, disponible en ligne

OMAAR Jamila. *Forever Isn't Free: The Cost of Storage on a Blockchain Database*, sur *IPDB Blog*. 2017. Disponible à l'adresse suivante

PATEL Nilay, *Meta's Andrew Bosworth on moving Facebook to the metaverse*, sur *The Verge*, 2021, disponible à l'adresse suivante

PETROC Taylor. *Total data volume worldwide 2010-2025*, sur *Statista*, disponible à l'adresse suivante

PETROSYAN Ani. *Internet users in the world 2021*, sur *Statista*, disponible à l'adresse suivante

PIAZZA Manon. *L'élaboration de représentations collectives en faveur de blockchains au sein d'espaces de la finance : Mythe et prophéties d'un futur possible investi*. Sur *ESSACHESS Journal for Communication Studies*. 2022. Disponible à l'adresse suivante

QUITTEM Brandon. *Bitcoin is a Decentralized Organism (Mycelium) — Part 1 / 4*, sur Medium, 2018, disponible à l'adresse suivante

REED Drummond. *Does the W3C Still Believe in Tim Berners-Lee's Vision of Decentralization?* Sur *Evernym*, publié le 12 octobre 2021, disponible à l'adresse suivante

ROACH John. *Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun*, sur *Innovation Stories*. 2021. Disponible à l'adresse suivante

ROSS Don, *Game Theory*, *The Stanford Encyclopedia of Philosophy*, Metaphysics Research Lab, Stanford University, 2019, disponible à l'adresse suivante

SCHMITT Carl, trad. **KIESOW Rainer Maria**, *Loi et jugement. Une enquête sur le problème de la pratique du droit.* EHESS. 2019.

SCHNEIDER Nathan. *Cryptoeconomics as a Limitation on Governance*, University of Colorado Boulder, 2022, disponible à l'adresse suivante

SCHREPPEL Thibault, *Smart contracts and the digital single market through the lens of a "law + technology" approach*, Direction générale des réseaux de communication, du contenu et des technologies, 2021.

SCHWAB Pierre-Nicolas. *Statistiques RGPD Europe : évolution du nombre de plaintes par pays*, sur *Conseils en marketing*, 2019, disponible à l'adresse suivante

Secure Identity Alliance, *On the road to User-Centricity: Digital Identity in the Electronic Wallet era, An SIA guide exploring usages, policies, models and best practices*, 2022, disponible à l'adresse suivante

SEDLMEIR Johannes, **SMETHURST Reilly**, **RIEGER Alexander, FRIDGEN Gilbert**. *Digital Identities and Verifiable Credentials*. Sur Business & Information Systems Engineering. 2021. Disponible à l'adresse suivante

SIFFREIN-BLANC Caroline. *L'identité des personnes : une identité pour soi ou pour autrui ?* Personnes et Familles - Hommage à Jacqueline Pousson-Petit, Presses de l'Université Toulouse 1 Capitole, 2016, disponible à l'adresse suivante

Smart Contract Academy (collectif), *Smart contracts - Etudes de cas et réflexions juridiques*, 2018, ecan.fr

Sovrin Foundation. *Self-Sovereign Identity and IoT*. 2020. Disponible à l'adresse suivante

STALLMAN Richard. *En quoi l'open source perd de vue l'éthique du logiciel libre - Projet GNU - Free Software Foundation*, disponible à l'adresse suivante

Statistica. *Global identity verification market size 2017-2027*, sur *Statista*. Disponible à l'adresse suivante

SUROWIECKI James. *The wisdom of crowds*, 2005, disponible à l'adresse suivante

SZABO Nick. *A Formal Language for Analyzing Contracts*, sur Nakamoto Institute, 2002. Disponible à l'adresse suivante

SZABO Nick. *Formalizing and Securing Relationships on Public Networks*, sur First Monday, 1997, disponible à l'adresse suivante

Tech London Advocates. *Blockchain: Legal & Regulatory Guidance*, sur *The Law Society*, 2020.

TEMOSHOK David, **ABRUZZI Christine**. *Developing Trust Frameworks to Support Identity Federations*, sur National Institute of Standards and Technology (NIST n°8149), 2018.

TREILLES Clarisse. *Le Conseil d'Etat valide l'amende de 100 millions d'euros prononcée par la CNIL contre Google*, sur *ZDNet France*. Disponible à l'adresse suivante

VERBIEST Thibault, **ATTIA Jonathan J**., *Internet of Universal Resources*, IOUR Foundation, 2020.

VIAL Claude, *Lexique de la Grèce ancienne, Armand Colin, 2008*, disponible à l'adresse suivante

Vie Publique. *Enfants sans identité : un pays sur trois concerné dans le monde*, sur *Vie publique.fr*, 2020, disponible à l'adresse suivante

Wikipedia contributors. *George Sand*, The Free Encyclopedia., disponible à l'adresse suivante

Wikipedia contributors. *Mosaic (web browser)*. In Wikipedia, The Free Encyclopedia, 2021, disponible à l'adresse suivante

Wikipedia contributors. *Public key infrastructure*. The Free Encyclopedia. 2022. Disponible à l'adresse suivante

WOERTH Éric, Rapport d'information déposé en application de l'article 145 du Règlement en conclusion des travaux d'une *mission d'information relative aux monnaies virtuelles*, Assemblée nationale, 2019, disponible à l'adresse suivante

World Economic Forum, *Bridging the Governance Gap: Interoperability for blockchain and legacy systems*, sur *Centre for the Fourth Industrial Revolution (C4IR)*, 2020, disponible à l'adresse suivante

X. CHEN Biran et **ROOSE Kevin**. *Are Telegram and Signal the Next Misinformation Hot Spots? Sur The New York Times*, 2021, disponible à l'adresse suivante

YOUSSR Youssef, *René Carmille, un hacker sous l'Occupation*, documentaire sur Public Sénat, Production TSVP, 2021, disponible sur Youtube à l'adresse suivante

VI – Colloques, évènements et autres contributions

APP et **Legal Brain Avocat**, *Constituez-vous des preuves infalsifiables avec l'horodatage certifié et l'horodatage par blockchain*, Webinar, 2020.

BECKER Katrin et **KIESOW Rainer Maria**, *La promesse du droit*, séminaire et intervention sur les technologies blockchains, le 27/02/2020 à l'EHESS, Paris.

BECKER Katrin, **LASSEGUE Jean**, **KIESOW Rainer Maria**. *Ateliers sur la Justice décentralisée*, série de six ateliers de quatre heures avec un groupe de travail composé de chercheurs, EHESS, Paris.

Centre de Recherches sur le Droit Public (**CRDP**). Colloque sur *La transformation numérique du service public : Une nouvelle crise ?* 14 et 15 janvier 2021, disponible à l'adresse suivante

CLUZEL-MÉTAYER Lucie, **PREBISSY-SCHNALL Catherine**, **SEE Arnaud**, **LEQUESNE-ROTH Caroline**, **HOURSON Sébastien**, et al, 2021, *La transformation du service public : une nouvelle crise ?* Ed. Mare & Martin, coll Droit & gestions publiques, 2022.

COURTIER Avocats et **AFDIT**, *Journée de l'AFDIT. Tiers de confiance, blockchains : stratégies et régulation - Cédric DUBUCQ - Avocat a. BRUZZO DUBUCQ*. 2023. YouTube. Disponible en ligne

ELIE Pauline, **SEGHIER Neil**, **LANGLOIS-BERTHELOT Thibault**. *Blockchain et Digital ID Wallet : vers une identité européenne décentralisée ?* Les Temps Numériques, atelier en mai 2022 à l'EHESS, Paris, France. pp.14. Compte rendu disponible à l'adresse suivante

FORUM DE L'AIT, Participation au « Hackathon » (« marathon de conception ») organisé le 7 et 8 février 2023 - *Accélérer les transitions pour les mobilités*. Disponible à l'adresse suivante

Forum International sur la Cybersécurité (**FIC**), *Quels models alternatifs pour l'identité*, table ronde du 09/09/2021 à Lille, en présence de Jean-Jacques Quisquater et Olivier Dussutour.

HIMMER Vincent et **PIAZZA Manon**, séminaire en ligne sur *L'entrepreneuriat au prisme des sciences sociales*, 14 février 2023 de 16h30 à 18h30. Présentations n°1 : *Faire la morale par le marché. Une étude de cas des entrepreneurs à impact*. Présentations n°1 : *Quels modes d'accumulation dans l'espace des cryptomonnaies ?* Disponible à l'adresse suivante

INSEAD, *CEPR and INSEAD webinars on Fintech and Digital Currencies*, Webinars du 2-15-30 septembre 2020, disponible à l'adresse suivante

Kramer Levin, *Webinars Legal Crypto dédié aux fintech, à la blockchain et aux crypto-monnaies*, lundi 18 mai 2020, 17h30 19h00

KRYPTOSPHERE® Blockchain Summit, *A day of exchanges and meetings with the biggest players in the blockchain ecosystem*, disponible à l'adresse suivante

LASSEGUE Jean, **GARAPON Antoine**, *Concluding Remarks of the Seminar on Blockchain and Procedural Law: Blockchain and the Problem of Injustice*. Sur *Stanford Journal of Blockchain Law & Policy*. Max Planck Institute Luxembourg, 2021, disponible à l'adresse suivante

Paris Blockchain Society, *L'identité décentralisée : vers un monde d'utilisateurs souverains ?* Table ronde du 24 janvier 2023 à Paris. En présence de Frédéric Martin, Nicolas Caille et Thibault Langlois-Berthelot. Résumé disponible à l'adresse suivante

PISTOR Katharina, *La loi du capital ; Comment la loi crée la richesse capitaliste et les inégalités*, présentation du libre à l'EHESS, le 02/05/2023

BLANC Nathalie, HAFTEL Bernard, MEKKI Mustapha et al. *Blockchain et métiers du droit : la fin des tiers de confiance ? Cycle « Entre mystères et fantasmes : quel avenir pour les blockchains ? »*, Colloque à la Cour de cassation, 2019, rediffusion disponible à l'adresse suivante

Science Po Crypto & KRYPTOSPHERE®, *Le Bitcoin va-t-il rôtir la planète ?* Conférence avec Sébastien Gouspillou, spécialiste du minage de bitcoins, 4 avril 2023 de 15h30 à 17h00, disponible à l'adresse suivante

Glossaire

- A -

Actifs numériques : actifs cryptographiques conçus pour fonctionner comme un moyen d'échange, une réserve de valeur, une unité de compte.

Administration : l'ensemble des services publics chargés d'assurer la gestion et l'exécution des politiques publiques.

Amendement : proposition de modification ou d'ajout d'informations à un texte juridique (loi, constitution, etc.).

Anonymat : l'état d'une personne ou d'une entité qui n'est pas identifiable dans une situation donnée.

Anonymat résiduel : possibilité pour un internaute de cacher son identité numérique pour accéder à certains services en ligne.

Application décentralisée : application logicielle décentralisée fonctionnant au-dessus d'un protocole quasi décentralisé et intégrant généralement un ou plusieurs contrats intelligents.

Application sectorielle : v. cas d'usage.

Application-Specific Integrated Circuit : ordinateur spécialement conçu pour faire fonctionner la fonction de minage du Bitcoin.

Arbitrage : une procédure de résolution de conflits impliquant un tiers neutre qui prend une décision arbitrale contraignante pour les parties en conflit.

ASIC : circuit spécialisé et intégré à une machine conçu pour effectuer efficacement les calculs nécessaires à la validation des transactions et à la création de nouveaux blocs sur le réseau Bitcoin.

Attestation(s) vérifiable(s) : un document électronique contenant des informations permettant de vérifier son authenticité et son intégrité grâce à de nouveaux mécanismes cryptographiques.

Attribut(s) d'identité : tous types d'informations en ligne ou hors ligne désignant l'identité d'une personne physique.

Authentification : processus de vérification de l'identité d'un utilisateur en utilisant des informations d'identification préalablement enregistrées (identifiants de connexion, empreintes digitales, etc.).

Auto-détermination informationnelle : référence au droit des individus à contrôler et à protéger leurs données personnelles.

Autonomie juridique : capacité d'une personne à déterminer ses propres droits et obligations, sans influence extérieure.

- B -

Biométrie : utilisation de caractéristiques biologiques uniques d'une personne, comme les empreintes digitales, la reconnaissance faciale ou l'iris de l'œil, à des fins d'identification et de vérification d'identité.

Bitcoin : premier crypto-actif né en 2009 et à l'origine de la première blockchain publique. Cette dernière est connue pour son fonctionnement fiable et résilient.

Bits : la plus petite unité de mesure de toute information numérique, représentée par un chiffre binaire 0 ou 1 ensuite interprété par des ordinateurs.

Bloc : groupe de transactions diffusé dans un réseau blockchain puis inscrit en son sein.

Blockchain : registre numérique décentralisé des transactions d'actifs numériques conservés sur un réseau d'ordinateurs.

Blockchain d'entreprises : v. blockchain consortium.

Blockchain européenne : référence au cadre et aux infrastructures 3.0 développés par la Commission européenne depuis 2018.

Blockchain fermée : v. blockchain privée.

Blockchain hybride : système qui combine les caractéristiques de la blockchain publique et privée, permettant une utilisation flexible pour différents cas d'utilisation.

Blockchain ouverte : v. blockchain publique.

Blockchain privée : version restreinte de la blockchain publique, utilisée par un groupe spécifique d'acteurs pour enregistrer et vérifier des transactions.

Blockchain publique : registre décentralisé et transparent, accessible à tous, où les transactions sont enregistrées de manière sécurisée et immuable.

Bluetooth : technologie de communication sans fil à courte portée, utilisée pour connecter des appareils électroniques tels que des téléphones portables, des ordinateurs et des enceintes.

Boîte à outil règlementaire : v. sandbox règlementaire.

Branches du droit : se réfère à une catégorie spécifique de lois, par exemple, le droit civil, le droit des affaires, etc.

Brique(s) technologique(s) : module logiciel ou matériel réutilisable qui peut être intégré à différents systèmes pour fournir une fonctionnalité spécifique.

- C -

Cas d'application : v. cas d'usage.

Cas d'usage : situations, contextes et possibilités de développement et d'utilisation commerciale d'un produit, d'un service ou d'une technologie.

Censure : pratique de supprimer ou de restreindre l'accès à l'information, aux idées ou aux innovations qui sont considérées comme offensantes, dangereuses ou inappropriées par une autorité gouvernementale, une entreprise ou une autre organisation.

Centralisé : système ou organisation contrôlé par une personne, un groupe, une société ou un gouvernement.

Chaîne de bloc : (blockchain en anglais) une base de données distribuée ou décentralisée qui contient une liste de transactions sécurisées et vérifiables de façon plus ou moins ouverte.

Chaîne de valeur : ensemble des activités d'un concept, système ou d'une organisation depuis la conception jusqu'à la production, commercialisation puis distribution à des utilisateurs finaux.

Chemin d'éligibilité : grandes orientations et questions qu'une organisation peut étudier pour savoir si l'utilisation d'une blockchain est nécessaire.

Clause léonine : disposition abusive ou injuste dans un contrat qui donne un avantage excessif à une partie au détriment de l'autre partie.

Clé privée : utilisée pour déchiffrer des messages ou des transactions destinées à un destinataire spécifique

Clé publique : utilisée pour chiffrer des messages ou des transactions destinées à un destinataire spécifique

Code QR : version numérique d'une donnée qui peut être scannée par un lecteur QR.

Code source : texte écrit par un programmeur dans un langage de programmation, qui est ensuite converti en code exécutable par l'ordinateur.

Concurrence déloyale : pratique commerciale qui consiste à nuire à un concurrent en utilisant des moyens illégaux ou trompeurs pour obtenir un avantage sur le marché.

Concurrence des citoyennetés : concurrence entre des citoyennetés et revendications identitaires spécifiques à des communautés en ligne, par rapport au concept de citoyenneté territoriale généralement et adopté dans la société.

Conditions générales d'utilisation : règles d'utilisation d'un service ou d'un site web, ainsi que les droits et les obligations des utilisateurs et du propriétaire du service ou du site web.

Confiance numérique 2.0 : utilisation des briques technologiques du Web 2.0 pour bâtir des systèmes et des services en ligne de confiance.

Confiance numérique 3.0 : utilisation des briques technologiques du Web 3.0 pour bâtir des systèmes et des services en ligne de confiance.

Confirmation : l'inclusion réussie d'une transaction d'informations au sein d'un bloc d'une blockchain

Conformité : ensemble des règles, normes et lois auxquelles une organisation doit se conformer dans ses activités et opérations.

Consensus blockchain : mécanisme par lequel les participants d'une blockchain parviennent à un accord sur l'état actuel de la blockchain et sur les transactions qui y sont enregistrées.

Consortium : regroupement et association d'entreprises, d'organisations ou de gouvernements qui travaillent ensemble sur un projet commun, tout en conservant leur autonomie et leur indépendance.

Contrat intelligent : ensemble d'instructions écrites en code sur une blockchain qui s'exécutent automatiquement dès lors que des conditions spécifiques sont remplies

Contrat Ricardien : brique technologique permettant de réaliser des contrats légalement formés et valables également disponibles ou exécutables sous la forme numérique.

Contrôleur d'identité : v. vérificateur d'identité

Corruption : utilisation abusive du pouvoir public et/ou privé à des fins personnelles, telles que l'enrichissement personnel, l'obtention de privilèges ou l'avancement de sa propre cause au détriment de l'intérêt public.

Couche informatique : niveau d'abstraction dans un système informatique qui permet la communication entre différents composants.

Crypto-actifs stables : actifs numériques adossés à une monnaie ou un actif sous-jacent pour maintenir une stabilité de leur valeur.

Crypto-actifs : v. actifs numériques

Cryptographiquement : référence à l'utilisation de solutions 3.0.

Crypto-monnaies : v. actifs numériques

Cyberespace : environnement virtuel créé par l'interconnexion de réseaux informatiques, comme Internet, à travers le monde.

Cybernaute : v. internaute.

Cypherpunks : communauté d'internautes qui défendent certaines valeurs pionnières d'internet des nouvelles technologies numériques, comme la protection des données personnelles, de la vie privée et plus largement la souveraineté individuelle et le droit à l'anonymat.

- D -

DAO : organisation autonome décentralisée basée sur les contrats intelligents d'une ou plusieurs blockchains.

Décentralisation informatique : processus matériel et/ou logiciel de transfert de la gestion et de la responsabilité de systèmes informatiques centralisés par quelques entités vers des utilisateurs finaux et multiples unités opérationnelles.

Decentralized Finance : services financiers basés sur une ou plusieurs blockchains et souvent utilisés sans avoir recours à un intermédiaire.

Decentralized identifiers : identifiants numériques uniques et permanents (3.0) qui permettent à une personne ou à une organisation de contrôler de manière indépendante ses informations d'identité et de vérifier leur authenticité sans avoir recours à un tiers de confiance centralisé (1.0 ou 2.0).

Degrés de décentralisation : le spectre, c'est-à-dire les niveaux de décentralisation informatique possible pour un système numérique comme une blockchain.

Dérive(s) technologique(s) : phénomène par lequel une technologie évolue de manière imprévue ou incontrôlée du fait de l'Homme, souvent vers des applications imprévues ou des conséquences négatives.

Désintermédiation : référence à une recherche de réduction des dépendances et/ou de la confiance envers un ou plusieurs tiers en ligne. La désintermédiation est également évoquée en contraste à la décentralisation, en tant que degré inférieur (décentralisation partielle).

Détournement de finalité : v. dérive technologique.

Développeur(s) : personne physique qui conçoit, crée et programme des logiciels et des applications en utilisant des langages de programmation et des outils de développement appropriés.

Directive : acte juridique de l'Union européenne qui fixe des objectifs à atteindre par les États membres, tout en leur laissant une marge de manœuvre concernant des moyens pour les atteindre.

Données numériques : données représentées sous forme de chiffres binaires, stockées et traitées par des ordinateurs et des dispositifs électroniques.

Droit à l'identité : droit de chaque individu d'être reconnu et traité en tant que personne distincte et unique.

Droit communautaire : ensemble des règles de droit applicables au sein de l'Union européenne et qui ont une primauté sur le droit national des États membres.

Droit cryptographique : v. Lex cryptographia.

Droit de propriété : droit pour une personne d'avoir la maîtrise exclusive et la disposition d'un bien matériel ou immatériel.

Droit interne : ensemble des règles juridiques en vigueur dans un pays ou un territoire spécifique.

Droit naturel : théorie juridique qui postule que certaines lois et droits sont inhérents à la nature humaine, indépendamment de la loi humaine et de la culture.

Droit positif : ensemble des règles de droit en vigueur dans un pays ou une juridiction à un moment donné.

Droits numériques (augmentés) : désigne l'exercice en ligne de certains droits des personnes.

- E -

Education (informatique) : enseignement de la compréhension, de l'utilisation et de la programmation des ordinateurs et des technologies associées.

Empreinte numérique : v. hash.

En ligne : connecté à Internet et à ses services en ligne.

Epistémologie : branche de la philosophie qui étudie la connaissance et la recherche scientifique.

Etat de droit : principe selon lequel l'État et toutes les institutions et personnes agissant au nom de l'État sont soumis aux lois, qui sont appliquées de manière juste et équitable pour protéger les droits fondamentaux des citoyens.

Etat de l'art : l'ensemble des connaissances et des avancées les plus récentes dans un domaine particulier.

Etat de non-droit : caractérisé par l'absence ou l'effondrement de l'autorité de l'État et de ses institutions légales, où les droits des citoyens ne sont pas protégés, c'est-à-dire où la violence, la corruption et l'arbitraire sont courants.

Etat-blockchain : utilisation par un Etat de technologies blockchains pour ses services administrations et services publiques.

Ethereum : deuxième crypto-actifs en importance qui se concentre principalement sur l'activation de services basés sur une blockchain grâce à l'utilisation de contrats intelligents, *et*

Ethereum : blockchain publique partiellement décentralisée et open source qui permet l'exécution de contrats intelligents et d'applications décentralisées directement sur son registre électronique.

Ethique numérique : moralité et responsabilité individuelle et collective dans le contexte de l'utilisation des technologies numériques 2.0 et 3.0.

Euro cryptographique : monnaie numérique légalement établie dans la zone euro et dont la sécurité et la confidentialité sont garanties par des techniques cryptographiques 3.0 garanties par la BCE.

Euro numérique : v. euro cryptographique.

- F -

Fiat : monnaie fiduciaire moderne comme l'euro, le dollar, souvent sous la forme électronique et non pas cryptographique.

Fongible : qualité selon laquelle deux ou plusieurs exemplaires d'une même chose, comme des bitcoins, ont une valeur identique et se substituent parfaitement les uns aux autres

Fork : changement radical du protocole logiciel d'une blockchain qui rend invalides les blocs et les transactions précédemment valides

Fournisseur(s) d'identité(s) : entité ou organisation délivrant des attributs d'identité numérique.

Fournisseur(s) de service(s) en ligne : entité ou organisation fournissant l'accès à un ou plusieurs services en ligne.

Frais de transaction : coût payé pour inciter les utilisateurs d'une blockchain à confirmer une transaction sur cette même blockchain.

- G -

Genesis bloc : désigne le tout premier bloc miné sur la blockchain du Bitcoin.

- H -

Hachage : action d'utiliser un programme informatique pour transformer des informations en une chaîne de lettres et de chiffres d'une longueur prédéterminée.

Hachage cryptographique : fonction mathématique qui prend en entrée des données de taille variable et génère en sortie une empreinte numérique de taille fixe qui est unique et difficile à falsifier.

Halving : réduction périodique de moitié du taux d'émission du Bitcoin, ou le taux auquel les nouveaux bitcoins sont mis en circulation par l'exploitation minière[1477].

Horodatage : processus de certification de la date, de l'heure, de l'origine et de l'intégrité d'une transaction d'informations numériques au moyen de techniques cryptographiques.

Hors ligne : une communication numérique sans connexion à internet grâce à d'autres standards et technologies informatiques.

- I -

Identifiant(s) décentralisé(s) : v. decentralized identifiers.

Identification : processus de reconnaissance et de vérification de l'identité d'un individu.

Identité (numérique) auto-souveraine (INAS) : ensemble de mécanismes cryptographiques avancés permettant à un internaute de contrôler et de gérer ses propres attributs d'identité, sans recourir à aucune autorité centrale pour les vérifier ou les valider.

Identité (numérique) centralisée : système où les informations d'identification d'un individu sont stockées sur un serveur centralisé et contrôlé par une autorité centrale.

Identité (numérique) décentralisée : une solution informatique permettant l'usage d'identifiants décentralisés, d'attestations vérifiables et/ou d'une blockchain pour partager son identité numérique de façon particulièrement indépendante (moins que l'INAS).

Identité (numérique) décentralisée/distribuée (IND) : l'identité numérique de troisième génération.

Identité (numérique) distribuée : solution informatique permettant l'usage d'identifiants décentralisés, d'attestations vérifiables et/ou d'une blockchain pour partager son identité numérique fournie par quelques tiers de confiance.

Identité de troisième génération : v. identité décentralisée.

Identité des machines : caractéristiques qui permettent d'identifier et de distinguer les différentes machines dans un réseau ou un système informatique.

Identité en iceberg : concept simplifié pour décomposer l'identité en couche sémantique tout en gardant à l'esprit son aspect ductile.

Identité juridique : caractéristiques qui concourent à définir une personne ou une entité juridique au regard de la loi.

Identité numérique génétique (4.0) : représentation numérique des informations génétiques d'un individu, souvent stockées dans des bases de données génétiques et utilisées à des fins de recherche et d'identification.

[1477] Consultez le site internet suivant pour suivre ces évènements en temps réel

Identité numérique : informations et traces personnelles qui identifient un individu auprès de services en ligne, notamment les noms d'utilisateur, les adresses e-mail, les numéros de téléphone et les informations de carte de crédit.

Identité philosophique : manière subjective dont une personne comprend et interprète les grandes questions de la vie, telles que la vérité, l'éthique, l'existence et la connaissance.

Identité primaire : attributs de l'identité civile, légale, racine d'une personne physique.

Identité psychosociale : perception psychologique et sociale que les individus ont d'eux-mêmes en tant que membres de groupes culturels, qui influencent leur comportement, leur personnalité et leur estime de soi.

Identité régalienne : v. identité primaire.

Identité secondaire : attributs de l'identité qui reposent, complètent ou s'émancipent de l'identité primaire d'une personne physique.

Identité sociale : caractéristiques personnelles et sociales qui définissent une personne en tant que membre d'un groupe ou d'une communauté, influençant ainsi sa perception de soi et sa relation aux autres.

Identité universelle : une identité numérique unique pour chaque individu, éventuellement indépende de leur nationalité, de leur religion, de leur race ou de leur culture.

Information immuable : information invariable, immuable et qui ne peut pas être modifiée ou altérée.

Informations : données et faits collectés, stockés et communiqués en ligne pour fournir des connaissances et des éclairages sur des sujets spécifiques.

Informatique : traitement de l'information à travers des algorithmes et des systèmes informatiques.

Infrastructure numérique : v. réseau.

Initial Coin Offering : méthode de financement alternatif basé sur les crypto-actifs, utilisée par des entreprises et des protocoles, et dans laquelle un jeton natif est échangé contre des devises fiduciaires ou d'autres crypto-actifs.

Innovation numérique : utilisation de technologies et de méthodes avancées pour créer de nouveaux produits, services et processus qui améliorent la réponse à des besoins, l'efficacité, la productivité et l'expérience d'utilisateurs.

Institutions publiques : organisations officielles établies par l'État pour remplir des fonctions et des services spécifiques au service du bien commun.

Intelligence artificielle : domaine de l'informatique qui se concentre sur la création de machines et de logiciels capables de simuler l'intelligence humaine et de réaliser des tâches qui nécessitent normalement l'intelligence humaine.

Internaute : personne physique qui utilise Internet pour accéder à des ressources et services en ligne, pour communiquer avec d'autres utilisateurs et pour effectuer des activités virtuelles.

Internet : réseau mondial de communication qui permet à des ordinateurs et à d'autres appareils de se connecter et de communiquer entre eux.

Interopérabilité informatique : capacité entre différents systèmes informatiques d'échanger des informations et de communiquer ensemble de manière transparente et efficace.

- J -

Juristes : professionnels du droit qui étudient, appliquent et interprètent les lois et règlements, et fournissent des conseils juridiques à des particuliers, des entreprises et des organisations.

Justice (numérique) alternative : utilisation de la technologie et des moyens numériques pour fournir des solutions de règlement des différends en dehors du système judiciaire traditionnel, tel que la médiation et l'arbitrage en ligne.

Justice décentralisée (3.0) : utilisation de la technologie de la blockchain pour créer des systèmes de résolution des conflits qui sont autonomes, transparents, sécurisés et opérés par des pairs, sans la nécessité d'une autorité centrale. V. Kleros.

- K -

Kleros : plateforme de justice décentralisée basée sur la blockchain, qui utilise des jurés en ligne pour résoudre les litiges de manière rapide, transparente et équitable.

Know your business : exigences imposées par les fournisseurs de services centralisés, souvent à la demande des gouvernements, qui collectent des informations personnelles de personnes physiques représentantes de personnes morales.

Know your customer : exigences imposées par les fournisseurs de services centralisés, souvent à la demande des gouvernements, qui collectent des informations personnelles d'utilisateurs et de personnes physiques.

- L -

Layer 1 & 2 : protocoles ou plateformes construites (L2) à côté d'une blockchain existante et qui ajoutent généralement des fonctionnalités ou une efficacité supplémentaire au réseau principal (L1).

Lex cryptographia : expression latine qui signifie que la loi cryptographique supplante la loi des textes de droit, en se référant aux principes et règles qui régissent l'utilisation de la programmation informatique, de la cryptographie, confidentialité et sécurité des données.

Libertarien : personne qui croit en la primauté de la liberté individuelle, la non-ingérence de l'État dans les affaires personnelles et économiques et le strict respect du droit de propriété, y compris cryptographique.

Liberté d'expression : droit fondamental qui garantit la liberté de tout individu de communiquer en ligne ou hors ligne ses opinions, ses idées et ses croyances sans crainte de représailles ou de censure.

Lightning Network : protocole et seconde couche de la blockchain Bitcoin, conçue pour des paiements économiques, rapides et privés entre ses utilisateurs.

Livre Blanc : document de recherche technique et/ou commercial décrivant les finalités et/ou fonctionnalités d'un crypto-actif, d'une blockchain et plus largement d'une solution 3.0.

Logiciels libres : programmes informatiques distribués sous une licence permettant à l'utilisateur d'exécuter, copier, modifier et distribuer librement le code source du logiciel.

Logiciels : programmes informatiques conçus pour exécuter des tâches spécifiques sur des ordinateurs ou d'autres appareils électroniques.

Loi naturelle : théorie morale et philosophique qui soutient que certaines lois et principes moraux sont universellement vrais et évidents par la raison et la nature humaine.

- M -

Mémoire numérique : stockage immuable de l'histoire de l'humanité sur des supports informatiques pérennes que représentent a priori la blockchain publique Bitcoin ou éventuellement d'autres blockchains.

Métavers : réseau d'univers virtuels en 3D axés sur l'immersion et la connexion sociale en ligne, souvent croisés avec des crypto-actifs.

Minage : processus consistant à deviner informatiquement un nombre aléatoire avant tous les autres participants de la blockchain Bitcoin afin d'émettre de nouveaux bitcoins en circulation.

Mineur(s) ou miners : personne physique ou morale en possession d'une machine ASIC dont la puissance de calcul vise à extraire des bitcoins de ce protocole à des fins économiques.

Modèle d'affaire en losange : proposition d'un concept simplifié illustrant les principales attentes des sociétés concernant le déploiement ou l'utilisation d'une blockchain pour leurs activités.

Monnaie cryptographique : v. monnaie d'internet.

Monnaie d'Internet : monnaie cryptographique utilisée par les internautes pour leurs transactions en ligne, souvent indépendante (pair à pair) des institutions financières traditionnelles.

Monnaie légale : monnaie émise et garantie par un État et reconnue internationalement comme moyen de paiement légal dans un pays donné.

- N -

Niveaux de décentralisation : v. degrés de décentralisation.

Nœud : ordinateur qui participe à la vérification des transactions valides sur le réseau Bitcoin.

Non Fungible Token (NFT) : jeton non fongible qui est une représentation cryptographiquement unique d'un actif numérique ou physique sur une blockchain.

Normalisation : v. interopérabilité.

Normes : règles établies par des organismes officiels ou des industries pour garantir des pratiques cohérentes et des niveaux de qualité ou de performance spécifiques.

- O -

Objet connecté : objet doté de capteurs et de la connectivité Internet, permettant la collecte et l'échange de données pour améliorer ou automatiser des tâches.

Ordinateur conventionnel : ordinateur basé sur la technologie de traitement de l'information classique qui utilise des bits binaires pour stocker et manipuler des données.

Ordinateur quantique : type d'ordinateur qui utilise les lois de la physique quantique pour effectuer des calculs incroyablement rapides et complexes.

Outils numériques : v. solutions numériques.

- P -

Pair à pair : modèle de communication informatique dans lequel chaque ordinateur ou nœud sur le réseau peut agir en tant que client ou serveur pour les autres, permettant un partage direct de fichiers ou de ressources sans passer par un serveur centralisé.

Patrimonialisation des données : volonté et processus de monétisation des données personnelles primaires et/ou secondaires en vertu de l'extension du droit de propriété.

Pays développés : nations qui ont un niveau de vie élevé, une économie industrialisée, un système de santé et d'éducation avancé, ainsi qu'une monnaie forte et stable.

Pays en voie de développement : nations qui ont un niveau de vie relativement bas, une économie peu diversifiée et plutôt dépendante d'autres pays, un accès limité à l'éducation, aux infrastructures ainsi qu'une monnaie instable.

Peer-to-Peer (P2P) : *v*. pair à pair.

Personne morale : entité juridique, telle qu'une société, une organisation ou une association, qui a une existence distincte de ses membres et peut agir en tant que sujet de droits et d'obligations juridiques.

Personne physique : individu sujet de droits et d'obligations juridiques distinct de toute entreprise ou organisation.

Phygital : terme utilisé pour décrire une expérience qui combine à la fois des éléments physiques et numériques, souvent utilisé pour décrire les interactions entre le monde physique et le monde virtuel.

Plateforme d'échange : plateforme qui permet aux utilisateurs d'échanger des crypto-monnaies et des monnaies fiduciaires.

Portefeuille d'identité numérique décentralisé : programme informatique conçu pour sécuriser la clé privée utilisée pour accéder à ses attestations vérifiables (VC) et identifiants décentralisés (DID) dispositif spécialement conçu pour verrouiller la clé privée utilisée pour accéder à ses bitcoins

Portefeuille de crypto-actifs : dispositif et/ou programme qui stocke les clés privées et publiques qui permettent ensemble l'accès aux crypto-actifs de l'utilisateur qui sont stockées sur ce support.

Preuve à divulgation nulle de connaissance (ZKP) : protocole cryptographique qui permet à une partie de prouver la validité d'une information sans révéler l'information elle-même, ni aucune information associée à cette information.

Preuve d'existence : ensemble d'outils 3.0 permettant à une personne de générer et d'affirmer en ligne de façon basique son existence physique, sans pour autant que cette preuve d'existence numérique représente une identité légalement formée et juridiquement valable.

Preuve d'existence légale : ensemble d'outils 3.0 permettant à une personne de générer et d'affirmer en ligne de façon basique son existence physique, tout en bénéficiant d'une reconnaissance légale grâce à des tiers de confiance étatiques.

Preuve légale : preuve admissible en justice pour prouver ou réfuter un fait ou une allégation, qui est obtenue de manière légale et présentée conformément aux règles de preuve applicables.

Programmation : processus de création d'un ensemble d'instructions informatiques qui sont exécutées par un ordinateur ou une autre machine pour effectuer une tâche spécifique.

Proof-of-Authority (PoA) : algorithme de consensus d'une blockchain où les validateurs sont des entités approuvées qui prouvent leur identité et leur autorité pour valider les transactions, plutôt que de résoudre des problèmes mathématiques comme dans d'autres algorithmes de consensus.

Proof-of-Stake (PoS) : algorithme de blockchain dans lequel la probabilité qu'un participant soit sélectionné pour confirmer un bloc sur une blockchain est liée de manière probabiliste au pourcentage de l'approvisionnement en jetons de la blockchain que le participant contrôle.

Proof-of-Work (PoW) : l'algorithme sur lequel fonctionne la blockchain Bitcoin. La Preuve de travail est définie par la conversion de l'électricité en puissance de traitement.

Propriété cryptographique : v. Lex cryptographia.

Propriété intellectuelle : désigne les droits légaux accordés aux créateurs et propriétaires d'œuvres de l'esprit, tels que les inventions, les œuvres littéraires et artistiques, les marques et les brevets.

Protection des données personnelles : processus de préservation de la vie privée et des droits des individus en encadrant par exemple la collecte, l'utilisation, le stockage et la divulgation de leurs informations personnelles par des tiers.

Protection des libertés personnelles : préservation des droits individuels et fondamentaux tels que la liberté d'expression, la liberté de pensée, la vie privée, l'égalité devant la loi et la protection contre la discrimination et l'oppression.

Protocole : ensemble établi de règles dictant la manière dont les nœuds d'une blockchain interagissent entre eux et avec la base de code

Protocole (informatique) : ensemble de règles, de normes et de procédures standardisées qui permettent à différents systèmes informatiques de communiquer et d'échanger des informations de manière cohérente et fiable.

Pseudo-anonymat : méthode de protection de la vie privée dans laquelle l'identité d'un individu est masquée derrière un pseudonyme ou un identifiant, offrant une relative protection contre la divulgation de son identité réelle, mais pas une protection totale.

Pseudo-anonymat contextuel : nécessité d'adapter par conception le niveau du pseudo-anonymat de chaque internaute en fonction des services en ligne sur lesquels il évolue.

Puissance publique : ensemble des pouvoirs exécutif, législatif et judiciaire détenus par l'État pour gouverner et administrer un pays.

- R -

Recherche d'anonymat : la volonté et le droit de chaque internaute de pouvoir naviguer anonymement sur des services en ligne légaux.

Recherche de décentralisation (informatique) : la volonté et le droit de chaque internaute de pouvoir participer et utiliser des infrastructures numériques décentralisées sans enfreindre de lois.

Régime juridique : l'ensemble des règles et des principes juridiques qui régissent une question ou un domaine spécifique, tel que le droit du travail, le droit fiscal ou le droit de la propriété intellectuelle.

Registre électronique : v. blockchain.

Règlement (communautaire) : règle juridique émise par les institutions de l'Union européenne qui est applicable directement à tous les États membres sans nécessiter de mesures nationales pour sa mise en œuvre.

Réseau (informatique) : ensemble de dispositifs interconnectés, tels que des ordinateurs et des serveurs, qui permettent le partage des ressources et des informations entre les utilisateurs du réseau.

Réseaux sociaux (numériques) : plateformes en ligne qui permettent aux utilisateurs de créer des profils, de se connecter avec d'autres utilisateurs et de partager des informations, des photos, des vidéos et d'autres contenus avec leur réseau d'amis et de contacts.

Responsabilité informatique : obligation de respecter les lois, les règlementations et les normes en matière de sécurité, de protection des données et de respect de la vie privée dans l'utilisation des technologies de l'information.

Responsabilité juridique : obligation légale et/ou contractuelle de répondre des actes ou des comportements considérés comme illégaux ou dommageables envers une personne ou une entité.

Revendications identitaires : demandes de reconnaissance et de respect d'une identité individuelle ou collective, qui peuvent être basées sur des caractéristiques telles que l'origine ethnique, la religion, la sexualité, le genre ou la nationalité.

Révocation d'attributs (d'identité) : processus qui permet à un utilisateur ou à un fournisseur d'identité de retirer ou de révoquer certains attributs associés à son identité numérique, tels que des autorisations ou des droits d'accès.

- S -

Sandbox règlementaire : environnement réglementé dans lequel les entreprises peuvent tester de nouveaux produits, services ou modèles économiques sans risquer de violer les lois en vigueur.

Satoshi Nakamoto : la ou les personnes responsables du code logiciel original de Bitcoin et de la publication du livre blanc dédié.

Satoshis - Sats : la plus petite unité de Bitcoin sur la chaîne, égale à 0,00000001 BTC.

Sécurité informatique : ensemble de mesures techniques, organisationnelles et juridiques visant à garantir la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Sécurité juridique : principe de droit selon lequel les règles juridiques doivent être claires, accessibles et prévisibles pour garantir la stabilité des relations juridiques et le respect des règles de droit.

Segwit : *(Segregated Witness)*, modification du protocole de Bitcoin qui permet d'augmenter la capacité de la blockchain tout en améliorant la sécurité et la flexibilité des transactions.

Service en ligne : service fourni via Internet, généralement accessible via un navigateur Web et qui permet aux utilisateurs d'effectuer diverses tâches, interactions ou d'obtenir des informations.

SHA-256 : fonction de hachage cryptographique utilisée pour sécuriser les transactions et les informations sur la blockchain Bitcoin.

Sidechain : une blockchain parallèle développée à côté d'une blockchain principale. V. Layer 1 & 2

Signature électronique / cryptographique : mécanisme mathématique qui permet de prouver la propriété d'une clé cryptographique par la personne qui la détient.

Société numérique : société dans laquelle les technologies numériques jouent un rôle central dans les interactions sociales, les échanges économiques et les activités culturelles.

Solution 2.0 : solutions informatiques utilisant les normes et standards développés à l'ère du Web 2.0.

Solution 3.0 : solutions informatiques utilisant les normes et standards développés à l'ère du Web 3.0.

Source de confiance : système, entité ou personne considérée comme fiable pour fournir des informations précises.

Souveraineté numérique : capacité d'une entité à protéger ses intérêts dans le monde numérique en contrôlant sa propre infrastructure et en garantissant la confidentialité et la sécurité de ses données.

Sphère numérique : v. société numérique.

Stablecoin : jeton cryptographique conçu pour maintenir une parité de prix avec un autre actif financier du monde réel.

Staking : processus spécifiques aux blockchains en Proof of Stake (PoS) qui consiste à séquestrer ses avoirs en crypto-actifs sûr pour gagner des unités supplémentaires en crypto-actifs similaires.

Standards informatiques : normes établies pour garantir l'interopérabilité et l'efficacité des systèmes informatiques.

Stockage décentralisé : méthode de stockage de données où les informations sont réparties sur différents nœuds d'un réseau décentralisé, plutôt que d'être stockées sur un serveur centralisé.

Stockage distribué : méthode de stockage de données où les informations sont réparties sur différents nœuds d'un réseau distribué, plutôt que d'être stockées sur un serveur centralisé.

Supranationalité : caractéristique des institutions et des décisions qui sont prises au-delà du cadre national, impliquant des actions concertées entre plusieurs États.

Suprématie quantique : désigne le moment où un ordinateur quantique parvient à résoudre un problème que les ordinateurs classiques ne peuvent pas résoudre en un temps raisonnable.

- T -

Taproot : mise à niveau de Bitcoin qui vise à améliorer la confidentialité, la sécurité et l'efficacité des transactions.

Taro : mise à niveau de Bitcoin qui vise à permettre de nouvelles fonctionnalités et de nouveaux cas d'usage sur cette blockchain publique.

Taux de hachage : l'unité de mesure de la puissance de calcul et de traitement de la blockchain du Bitcoin.

tBDEX : plateforme d'échange décentralisée basée sur la technologie blockchain pour les actifs numériques.

Technologie(s) 2.0 : *v*. solutions 2.0.

Technologie(s) 3.0 : *v.* solutions 3.0.

Territorialité du droit : principe selon lequel les règles juridiques sont applicables uniquement sur le territoire géographique où elles ont été édictées.

Tiers de confiance : entité indépendante qui assure la gestion et la vérification de transactions électroniques entre deux parties. Il peut s'agir d'une personne morale du secteur public et/ou privé qui garantit la confiance de certaines informations et interactions en ligne pour le compte d'utilisateurs.

Token : unité de valeur sur une blockchain qui peut intégrer une variété de cas d'utilisation, comme la gouvernance ou un programme de récompenses.

Transaction : entrée d'une blockchain qui enregistre le transfert de valeur ou d'informations d'un utilisateur à un autre.

Triangle d'incompatibilité : concept et illustration informatique spécifique à la technologie blockchain démontrant certaines de ses limites conceptuelles et matérielles.

Triangle de confiance : concept et illustration informatique spécifique à l'identité numérique décentralisée.

- U -

Universel : quelque chose qui est valable, applicable ou s'applique, à tous les cas ou toutes les personnes, sans exception ni distinction.

Usurpation d'identité : se faire passer pour une autre personne en utilisant ses données personnelles sans son consentement.

Utilisateurs : *v*. internautes.

- V -

Vérificateur d'identité : personne ou organisation responsable de la vérification de l'identité des individus, souvent dans le cadre de processus d'authentification ou de contrôle d'accès.

Vitalik Buterin : programmeur et entrepreneur russo-canadien, connu en tant que co-fondateur et inventeur de la plateforme de contrats intelligents et de blockchain, Ethereum.

Vote décentralisé : processus de vote où les décisions sont prises par des internautes via l'utilisation de solutions 2.0 et/ou 3.0.

- W -

Web 1.0 : première version statique et unidirectionnelle du World Wide Web, où les utilisateurs ne pouvaient que consulter des pages Web mais n'avaient pas la possibilité de contribuer à leur contenu.

Web 2.0 : évolution du Web 1.0, caractérisé par des sites web interactifs et des réseaux sociaux qui permettent la participation active des utilisateurs à la création de contenu en ligne.

Web 3.0 : une nouvelle version de l'Internet basée sur les technologies blockchains et l'identité décentralisée.

Dictionnaire des acronymes

- A -

ABE	autorité bancaire européenne *(EBA en anglais)*
ABF	alliance blockchain France
ACPR	autorité de contrôle prudentiel et de résolution
ADAN	association pour le développement des actifs numériques
ADN	acide désoxyribonucléique
AEC	automate exécuteur de clauses *(smart contract)*
AEFR	association europe finances regulations
AEMF	autorité européenne des marchés financiers *(ESMA en anglais)*
AEPD	agencia española de protección de datos
AES	advanced encryption standard
AFADPP	association francophone des autorités de protection des donnée personnelles
AFDI	annuaire français de droit international
AFNOR	association française de normalisation
AGRASC	organe de gestion et de recouvrement des avoirs saisis et confisqués
ALICEM	authentification en ligne certifiée sur mobile
AMF	autorité des marchés financiers
ANSSI	agence nationale de la sécurité des systèmes d'informations
AP-HP	assistance publique hôpitaux de Paris
API	application programming interface *(interface de programmation d'application)*
AR	augmented reality *(réalité augmentée)*
ARCEP	autorité de régulation des communications électroniques, des postes et de la distribution de la presse
ARPANET	advanced research projects agency network
Art.	article
ASIC	application specific integrated circuit

- B -

B2G	business-to-government
BaaS	blockchain as a service
BaFin	bundesanstalt für finanzdienstleistungsaufsicht *(autorité fédérale de supervision financière allemande, créée en 2002)*
BAHTX	Baidu, Alibaba, Huawei, Tencent, Xiaomi *(les 5 géants du Web chinois)*
BCC	banque centrale chinoise
BCE	banque centrale européenne
BCG	boston consulting group
BCID	blockchain et identité numérique
BCN	blockchain notariale
BFDI	der bundesbeauftragte für den datenschutz und die informationsfreiheit
BIC	business indentifier code
BIP	bitcoin improvement proposal
BIS	bank for international settlement *(BRI en français)*
BMC	bitcoin mining council
BRI	banque des règlements internationaux *(BIS an aglais)*
BTC	blockchain bitcoin
BtoB	business-to-business
BtoC	business-to-consumer *(partage de données entre entreprises et consommateurs)*

- C -

CA	cour d'appel
CASP	crypto-asset service provider *(PSAN (ou) PSCA en français)*
Cass.	cassation
CBDC	central bank digital currencies *(MNBC en français)*
CCP	cadre de confiance pan canadien
CCPA	california consumer privacy act *(Etats-Unis)*
CCPA	california consumer privacy act *(Etats-Unis)*
CCT	clause contractuelle type
CDH	conseil des droits de l'homme
CE	commission européenne
CEDH	convention européenne des droits de l'homme
CEPD	comité européen de la protection des données *(EDPB en anglais)*
CERN	conseil européen pour la recherche nucléaire
cf.	confer *(latin)*
CICE	crédit d'impôts pour la compétitivité et l'emploi
CIDE	convention internationale des droits de l'enfant
CIR	crédit impôt recherche
Civ.	civile
CJUE	cour de justice de l'union européenne
CMF	code monétaire et financier
CNCJ	chambre nationale des commissaires de justice
CNI	carte nationale d'identité
CNIe	carte nationale d'identité numérique
CNIL	commission nationale de l'informatique et des libertés
CNNum	conseil national du numérique
CNRS	centre national de la recherche scientifique
CNUD	commission des Etats-Unis pour le droit commercial international
CNUDCI	commission des nations unies pour le développement du commerce international
Cold Wallet	portefeuille de stockage à froid *(génération et stockage hors ligne des clés)*
CSDHLF	convention de sauvegarde des droits de l'homme et des libertés fondamentales
CSP	catégories sociaux professionnelles
CtoB	consumer-to-business *(partage de données entre consommateurs et entreprises)*

- D –

DADDUE	dispositions d'adaptation au droit de l'UE *(loi n°2023-171 du 9.03.2023 qui transpose en droit français la Directive 2019/882 du 17.04.2019)*
DAM	digital asset management *(GAN en français, gestion des actifs numériques)*
DAO	decentralized autonomous organisation *(OAD en français, organisation automne décentralisée)*
DApps	applications décentralisées de nouvelles générations
DataAct (Règlement)	règlement européen sur les données
DCP	donnée à caractère personnel
DDHC	déclaration des droits de l'homme et du citoyen
DEEP	dispositif d'enregistrement électronique partagé *(DLT en anglais : distributed ledger technology)*
DeFi	decentralized finance *(finance décentralisée)*
DeSoc	decentralised society
DGA (Règlement)	data governance act *(Règlement européen sur les données)*
DGE	direction générale des entreprises

DID	decentralized identity *(identité décentralisée)*
DID4ALL	decentralized identifiers for all
DIF	decentralized identity foundation
DINUM	direction interministériel du numérique
dir.	sous la direction de
DLC	district log contract
DLT	distributed ledger technology *(DEEP en français : dispositif d'enregistrement électronique distribué)*
DMA	digital markets act
DNIe	documento nacional de identidad electronica *(Espagne)*
DPKI	decentralized public key infrastructure *(infrastructure à clé publique décentralisée)*
DPO	data protection officer (*délégué à la protection des données*)
DSA	digital services act *(Etats-Unis)*
DUDH	déclaration universelle des droits de l'homme

- E -

EBA	european banking authority *(autorité bancaire européenne)*
EBSI	european blockchain service infrastructure
e-CNY	e-yuan numérique chinois *(ou renminbi numérique)*
Ed.	édition
EDI	electronic date interchange *(échange de données informatiques)*
EDIC	european digital infrastructure consortium
EDIW	european digital identity wallets *(portefeuille européen d'identité numérique)*
EDPB	european data protection board *(CEPD en français : conseil européen de la protection des données)*
EDRI	european digital rights
EEA	entreprise euthereum alliance
EEE	espace économique européen
EHESS	école des hautes études en sciences sociales
eID	electronic identification numérique
eIDAS 1 (Règlement)	electronic identification authentication and trust services *(identification, authentification électronique et services de confiance)*
eIDAS 2 (Règlement)	electronic identification authentication and trust services *(identification, authentification électronique et services de confiance)*
EME	établissement de monnaie électronique
ENISA	agence de l'union européenne pour la cybersécurité
ESMA	European securities and markets authority *(AEMF en français)*
ESSIF	european self-sovereign identity framework
etc.	etcetera
ETH	euthereum
ETSI	european telecommunication standard institute
EUROC	euro coin

- F –

FATF	financial authority tasks force *(GAFI en français)*
FCS	facteurs clés de succès
FED	federal reserve system
FIC	forum international sur la cybersécurité
FINMA	swiss financial market supervisory authority
FMI	fond monétaire international

FNTC	fédération des tiers de confiance du numérique

- G -

G20	group of twenty
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
GAFI	groupement d'action financière *(FAFT en anglais)*
GAN	gestion des actifs numériques *(DAM en anglais : digital asset management)*

- H -

HCDH	haut-commissariat des Nations Unies aux droits de l'homme
HCR	haut-commissariat des Nations Unies pour les réfugiés

- I -

IA	intelligence artificielle
IAM	identity and access management
IBAN	international bank account number
Ibid.	ibidem *(du latin, signifie du même auteur, même ouvrage que la référence précédente)*
ICO	initial coin offering *(offre au public de jeton)*
Id.	idem
IdO	internet des objets
IDP	identity provider
IEO	initial exchange offering
In	dans
INAS	identité numérique auto-souveraine
IND	identité numérique décentralisée/distribuée
Infra	en-dessous de *(latin)*
ION	identity overlay network
IoT	internet of things *(IdO en français : internet des objets)*
IP	internet protocol
IPFS	internet protocol files system
ISO	organisation internationale de normalisation *(créée à Genève en 1949)*
ISP	international organisation for standardisation
ITV	international communication union

- J -

JNF	jeton non fongible
JOEA	journal officiel électronique authentifié
JORF	journal officiel de la république française
JOUE	journal officiel de l'union européenne

- K -

KPI	key performance indicatror
KYB	know your business
KYC	know your costumer

- L -

L1	layer 1
L2	layer 2
LBCA	legal blockchain and crypto association *(association des juristes de la Blockchain et des cryptos-actifs)*

LCB-FT	lutte contre le blanchiment et le financement du terrorisme
LGDJ	librairie générale de droit et de jurisprudence
LLM	liberland merit
LN	lightning network
LoA	level of assurance
LIL	loi informatique et libertés *(n° 78-17 du 6 janvier 1978)*
LOPPSI (loi)	loi d'orientation et de programmation pour la performance de la sécurité intérieure *(n° 2011-267 du 14 mars 2011)*
LSC	liberland smart chain

- M -

MC&M	mobile connect & moi
MiCA (loi)	markets in crypto-assets *(marchés de crypto-actifs, loi n°2020/0265 du 24 septembre 2020)*
MiFID 2	market in financial instrument directive
MNBC	monnaie numérique de banques centrales *(CBDC en anglais)*
MR	mixt reality

- N -

NFC	near-field communication *(espagne)*
NFT	non fungible token *(jeton non fongible)*

- O -

OACI	organisation de l'aviation civile internationale
ODD	objectif de développement durable
ODR	online dispute resolution *(système de résolution de litige en ligne)*
OFAC	office of foreign assets control
OMPI	organisation mondiale de la propriété intellectuelle
ONU	organisation des nations unies
Op. cit.	opus citatum *(ouvrage cité, latin)*
OPOCE	office des publications officielles des communautés européennes

- P -

p.	page(s)
P2P	peer to peer
P2P	peer to peer *(pair à pair)*
PACTE (loi)	plan d'action pour la croissance et la transformation des entreprises *(loi n°2019-486 du 22 mai 2019)*
PBoC	public bank of china *(banque populaire de chine)*
PCB	pre-commercial procurement
PDF	portable document format *(document PDF)*
PED	pays en voie de développement
PFI	participating financial institution
PIDCP	pacte international relatif aux droits civils et politiques
PIND	portefeuille d'identité numérique décentralisée
PIPL	personnal information protection law
PKI	public key infrastructure
PNK	pinakion *(jeton numérique d'utilité)*
PoA	proof of authority
PoH	proof of humanity
PoS	proof of stake

PoW	proof of work
PSAN	prestataire de services sur actifs numériques *(CASP en anglais)*
PSCA	prestataire de services sur crypto-actifs *(CASP en anglais)*
PUF	presse universitaire de France
PVID	prestataire de vérification d'identité à distance

- Q -

QR code	quick response code

- R -

RCS	registre du commerce et des sociétés
REF	revue d'économie financière
RGPD	règlement général sur la protection des données à caractère personnel
RNIPP	répertoire national d'identification des personnes physiques

- S -

s. d.	sans date
SaaS	software as a service
SAML	security assertion markup language
SBT	soul bound token
SCIC	société coopérative d'intérêt collectif
SDN	société des nations
SEC	securities and exchange commission *(Etats-Unis)*
SGIN	service de garantie de l'identité numérique
SIM	subscriber identity module
SMSI	système de management de la sécurité de l'information
SSI	self-sovereign identity *(identitée auto-souveraine)*
SSO	single sign on
STO	security token
supra	ci-dessus *(latin)*
SWIFT	society for worldwide interbank financial telecommunication

- T -

TCP	transmission control protocol
TCR	token curated registries
TES	titres électroniques sécurisés
TFR	transfer of fund regulation
TFUE	traité de fonctionnement de l'UE
Th.	thèse
TRACFIN	traitement du renseignement et action contre les circuits financiers clandestins
TRO	temporary restrictif order *(ordonnance restrictive temporaire)*

- U -

UBI	universal basic income *(token)*
UE	union européenne
UETA	uniform electronic transactions act *(Etats-Unis)*
UIT	union internationale des télécommunications
UNHCR	agence des nations unies pour les réfugiés
UNICEF	united nations international children's emergency fund *(Fonds des Nations unies pour l'enfance)*
URL	uniform resource locator

USDC	USD coin

- V -

V.	voir
VC	verified credentials *(attestation verifiable)*
VP	verifiable presentation
VR	virtual reality *(réalité virtuelle)*

- W -

W3C	world wide web consortium
Wallet	portefeuille numérique de crypto-monnaies
WEF	world economic forum
WiPO	world international property office

- Y -

YCC	eYuan numérique

- Z -

ZKP	zero knowledge proof

Annexes

Annexe 1 : Vingt-et-une questions pour appréhender l'identité au 21ème siècle

1	*Pourquoi définir l'identité ?*
2	*Faut-il définir l'identité ?*
3	*Qu'est-ce que l'identité ?*
4	*Qu'est-ce que l'identité numérique ?*
5	*Comment définir l'identité juridique ?*
6	*Comment définir l'identité sociale ?*
7	*Comment définir l'identité philosophique ?*
8	*Comment segmenter l'identité numérique ?*
9	*L'identité est-elle un fait social, juridique ou numérique ?*
10	*Une identité universelle est-elle possible ?*
11	*Une identité universelle est-elle souhaitable ?*
12	*Quelle est la différence entre le droit à une identité et le droit à une identité universelle ?*
13	*Quelles évolutions technologiques pour l'identité ?*
14	*Les nouvelles technologies sont-elles au service de l'identité ?*
15	*Les données sont-elles et (dé)font-elles notre identité ?*
16	*La technologie blockchain contribue-t-elle à libérer l'identité numérique des personnes ?*
17	*Qu'est-ce que l'identité numérique décentralisée ?*
18	*L'identité décentralisée est-elle l'avenir de l'identité numérique sur Internet ?*
19	*Dans quelles mesures l'identité financière est-elle si importante à l'ère numérique ?*
20	*Quels sont les impacts juridiques et sociaux de l'identité décentralisée ?*
21	*L'avenir de l'identité sera-t-il génétique ?*

Annexe 2 : Tableau résumé des problématiques et des hypothèses par niveau d'abstraction

Niveau d'abstraction (A - C)	**Problématiques traitées**	**Hypothèses**
Niveau A *(Questions structurelles)*	• Les technologies 3.0 impactent-elles l'identité juridique et primaire des personnes ? Leur identité secondaire ?	• Oui. Oui.
	• La blockchain est-elle une révolution pour l'identité numérique ? Pour la société ?	• Oui. Oui.
	• Le Métavers impacterait-il l'identité numérique des internautes ?	• Oui.
	• Faut-il distinguer la technologie blockchain de Bitcoin ?	• Non, excepté pour l'identité numérique.
	• Décentraliser toute la société serait-il bénéfique ?	
	• Décentraliser tout l'Internet serait-il bénéfique ?	• Non.
	• L'identité numérique décentralisée est-elle une révolution complémentaire et dans la continuité de l'identité numérique 2.0 ?	• Oui
	• La blockchain et l'IND possèdent-elles des variantes technologiques ?	• Oui
	• Existe-t-il un lien indissociable entre l'identité numérique 3.0 et les crypto-actifs ? Entre le Web 3.0 et les crypto-actifs ?	• Oui
	• Les blockchains, les crytoactifs et l'IND convergent-ils au regard de l'histoire des sciences informatiques pour répondre au besoin de nouveaux contre-pouvoirs numériques ?	• Oui. Oui. • Oui.
Niveau B *(Questions connexes)*	• La blockchain menace-t-elle la souveraineté étatique et le monopole monétaire ?	• Oui et non.
	• L'IND menace-t-elle la souveraineté et le monopole identitaire ?	• Oui et non.
	• La décentralisation informatique est-elle au service des droits et libertés en ligne des internautes ?	• Oui et non.
	• Un nouveau droit cryptographique est-il nécessaire et envisageable ?	• Oui

	• Faut-il reconnaitre un droit de propriété cryptographique en ligne ? • Un droit au pseudo-anonymat en ligne est-il nécessaire ? L'anonymat également ? • Le droit doit-il s'emparer de nouvelles méthodes cryptographiques par conception respectueuses des données des internautes ? • Les blockchains publiques souffrent-elles de leur manque de conformité juridique ? • L'IND renforce-t-elle l'exercice des droits des personnes en ligne ? • Le succès des technologies 3.0 réside-t-il en partie dans leur résilience et interopérabilité informatique globale ? • La justice décentralisée peut-elle se substituer à la justice traditionnelle ? Peut-elle la rendre plus transparente et efficiente ?	• Oui et non. • Oui. Oui. • Oui. • Non et oui. • Oui. • Oui. • Non. Oui.
Niveau C *(Questions subsidiaires)*	• Les titres d'identité officiels disparaitront-ils ? Seront-ils tous dématérialisés ? • Une identité numérique universelle est-elle souhaitable ? Viable ? • Bitcoin et son mécanisme de consensus informatique doivent-ils être restreints ou interdits ? • La puissance publique peut-elle construire des infrastructures de confiance 3.0 pour l'identité numérique de ses citoyens ? Doit-elle les financiariser ? • La blockchain et l'IND peuvent-elles permettre de fournir des preuves d'existence numérique fiable comme fondement pour une identité juridique ? • La suprématie quantique pourrait-elle bouleverser le Web 1.0, 2.0 et 3.0 ? • Une identité numérique et génétique est-elle possible ?	• Non. Oui. • Oui. Non. • Non. • Oui. Non. • Oui. • Oui et non. • Oui.

Annexe 3 : Focus sur Bitcoin

Focus 1 : Qu'est-ce que Bitcoin ?

Aujourd'hui, une pratique acceptée par la communauté d'internautes et d'utilisateur de bitcoins est d'utiliser le terme Bitcoin (au singulier avec la lettre **B** majuscule) pour désigner ce réseau informatique, ce protocole et/ou cette communauté. Le terme bitcoin (avec un **b** minuscule) désigne quant à lui les unités ou jetons cryptographiques à vocation monétaire (dont l'acronyme est « BTC ») qui circulent sur cette infrastructure informatique. Ces unités de compte cryptographiques permettent d'effectuer des paiements quasi-instantanés à toute personne et dans le monde entier, grâce à une simple connexion Internet (parfois sans). Accessible ouvertement aux internautes depuis 2009, Bitcoin utilise une suite de technologies complémentaires pour fonctionner sans autorité(s) centrale(s) et de façon hautement décentralisée, et notamment inspiré de plus de 40 ans de recherches et de développement des technologies de l'informatique[1478]. La gestion des transactions et l'émission de son crypto-actif natif (les bitcoins - BTC) sont effectuées collectivement par un réseau d'ordinateurs nommés des « nœuds »[1479]. Ces machines sont (pseudo)anonymes et géographiquement réparties à travers le monde. Plutôt que de s'appuyer sur des autorités centrales pour fonctionner, le protocole Bitcoin repose sur des mécanismes mathématiques et cryptographiques afin de contrôler la création et le transfert de jetons. Depuis environ une décennie, les bitcoins sont progressivement considérés par une partie des internautes comme étant la monnaie d'Internet, dont la rareté est mathématiquement vérifiable et graduellement démontrée depuis sa création. Étant donné l'histoire et le positionnement de cette monnaie expérimentale pour certains, ou quasi-monnaie pour d'autres, le bitcoin représente aujourd'hui un étalon pour le marché des technologies blockchains et des crypto-actifs qu'il a vu naître. Sa conception et son code ont inspiré la majorité des crypto-actifs qui tentent de s'émanciper sur le plan informatique, mais force est de constater qu'il demeure à date la première et principale application financière pérenne d'une blockchain ouverte. Cette infrastructure informatique représente en quelque sorte un système monétaire et communautaire alternatif, dématérialisée et décentralisée. Sa communauté fait généralement référence aux interactions entre des machines (des « nœuds » et des « mineurs »)[1480], des développeurs et des utilisateurs/investisseurs. En d'autres termes, il est possible de résumer ses principales caractéristiques ainsi :

[1478] HELD Dan, « Planting bitcoin — soil (3/4) », in *danheld.com*, 2018, disponible en ligne
[1479] Pour quelques centaines d'euros il est possible de mettre en place son propre *nœud bitcoin,* c'est-à-dire un système de gestion et de stockage physique et numérique pour ses bitcoins, directement chez soi. De cette façon chaque internaute gère en quelque sorte sa propre banque en ligne 3.0. V. ci-après.
[1480] V. Annexe 6, Focus 1.

Résumé des principales caractéristiques de Bitcoin
Paiements mobiles et Web en toute simplicité (via des QR codes, des liens, etc.)
Sécurité (mathématique) et contrôle (cryptographique) des jetons par les utilisateurs
Fonctionne en toute circonstance depuis 2009 avec Internet et quelquefois sans Internet (transferts de bitcoins possibles par SMS[1481] voire par ondes radio[1482])
Paiements internationaux rapides ou instantanés
Frais faibles (réseau principal) voire nuls (réseau secondaire « Lightning Network »)
Préservation par conception de l'identité des utilisateurs (pseudo-anonymat)

A quoi sert-il ?

Il permet simplement d'envoyer et de recevoir de la valeur en tant que « système de cash électronique pair à pair »[1483], sans discrimination géographique et grâce à l'utilisation d'un ordinateur, d'un téléphone ou d'une simple connexion Internet. Dans un avenir relativement proche, Bitcoin pourrait accueillir de nouveaux cas d'usage (NFT[1484], stablecoins, réseaux sociaux P2P) grâce à des protocoles adjacents en cours de développement, détaillés ci-après.

Pourquoi est-il révolutionnaire ?

Bitcoin étant à la fois une monnaie cryptographique et l'agrégat de protocoles informatiques ouverts sur Internet, son appréhension informatique, économique, sociale et juridique recquiert quelques années d'apprentissage et d'observation continue pour le comprendre de façon relativement objective. Contrairement aux autres méthodes de transfert de valeurs et de monnaies sur Internet, les échanges de bitcoins fonctionnent en principe sans avoir besoin de faire confiance à un intermédiaire[1485]. Le simple fait que ce système puisse fonctionner et être utilisé sans tiers de confiance signifie qu'il représente la première infrastructure de paiements publiques et cryptographiques – distribuée ou décentralisée - au

[1481] HALL Joe, « Bitcoin without Internet : SMS service allows sending BTC with a text », in *Cointelegraph*, 2022, disponible à l'adresse suivante
[1482] Ledger, « School of Block Episode 4 – Bitcoin by Radio, This can't be possible ! », in *ledger.com*, 2022, disponible à l'adresse suivante
[1483] NAKAMOTO Satoshi, « Bitcoin: a Peer-to-Peer electronic cash system », accessible en ligne à l'adresse suivante
[1484] V. par exemple le protocole « *Ordinals* » ci-après dans le Focus 3.
[1485] *Op. cit.* Dans les faits, selon une étude du 24 mars 2023, 80% des détenteurs de crypto-actifs (bitcoins y compris) les hébergent et les stockent au sein d'une plateforme et un tiers de confiance et seulement 30% les détiennent cryptographiquement sur un ou plusieurs portefeuilles non hébergés. Pour plus d'informations, consultez les informations suivantes, Coingecko, « Where People Store Their Crypto, Post-FTX Collapse », 24 mars 2023, disponible à l'adresse suivante

monde. Ce réseau ouvert est en effet accessible à tous et n'appartient pas à date à un ou plusieurs acteurs qui pourraient en prendre le contrôle de façon significative. Avant Bitcoin il n'existait que quelques infrastructures publiques permettant de s'échanger de l'information librement, comme Internet qui demeure - difficilement à ce jour[1486] - l'infrastructure ouverte la plus importante en taille et en enjeux. Dans le secteur monétaire, la principale infrastructure de paiement publique accessible à tous est la monnaie fiduciaire (billets en papier et pièces en métal), qui fonctionne pourtant aujourd'hui seulement pour des transactions en face à face, ce qui est une forme de limitation en comparaison à Bitcoin dont la vocation est relativement similaire (possibilité d'un pseudo-anonymat et d'une propriété exclusive lors des paiements), mais dont la nature et la forme exclusivement numériques renforcent sa pertinence en termes d'usage et de portée à l'ère digitale. En d'autres termes, avant Bitcoin, si une personne souhaitait payer à distance une autre en utilisant un téléphone ou un ordinateur, il était compliqué voire impossible d'utiliser une infrastructure numérique publique et in fine nécessaire de se tourner vers des acteurs privés (banques, sociétés mobiles, grandes entreprises technologiques), c'est-à-dire de faire confiance à leurs systèmes et registres comptables et financiers. Concrètement, cela implique pour les internautes d'utiliser de multiples services en ligne en se soumettant de facto à une validation récurrente de leurs demandes de transactions auprès de ces tiers (dépendance informatique), auxquelles ils doivent également faire confiance dans un temps long (dépendance sociale). Avec la blockchain Bitcoin[1487], chacun peut désormais ajouter une transaction à ce registre public en transférant des fractions de bitcoins à d'autres utilisateurs, un bitcoin pouvant être fractionné jusqu'à huit décimales, permettant par exemple d'envoyer l'équivalent de quelques centimes d'euros en bitcoins à ses utilisateurs[1488]. Tout internaute peut ainsi pour la première fois, sans distinction de frontière, de solvabilité, de nationalité, de genre ou de religion, accéder gratuitement à une adresse bitcoin pour en recevoir ou en transmettre grâce à cette infrastructure publique. Par conséquent, Bitcoin symbolise et représente une forme de liberté informatique et individuelle à l'état pur. Il est informatiquement immuable, car sa blockchain est théoriquement impossible à corrompre, c'est-à-dire à pirater, contrairement à son écosystème social composé d'applications qui demeure faillible comme le souligne l'Annexe 7. Ce réseau quasi-monétaire et financier ouvert est socialement résilient grâce aux milliers d'individus qui enregistrent et stockent chacun de ses blocs de transactions sur leurs ordinateurs personnels (nœuds)[1489], ce qui signifie qu'ils

[1486] Gouvernement, « Câbles sous-marins de communication », in *L'économie bleue en France*, Ed. 2022, « L'essor d'internet et de la mondialisation financière a considérablement accentué la dépendance des États face aux câbles sous-marins de communication. Il a été estimé que 10 000 milliards de dollars de transactions financières transiteraient chaque jour par le réseau des câbles sous-marins de communication. Le dysfonctionnement d'un câble peut générer d'importantes conséquences pour un État. […] De nouveaux enjeux comme l'émergence de grands groupes privés — essentiellement les GAFAM — dans l'activité câblière mondiale et les risques d'une potentielle remise en cause du principe de la neutralité du net doivent également être particulièrement surveillés », p. 4, consulté le 08/01/2023 à l'adresse suivante

[1487] V. Annexe 6, Focus 1.

[1488] A titre d'illustration, le réseau social Twitter permet une nouvelle fonctionnalité depuis 2021 pour effectuer des donations en bitcoins entre utilisateurs. Cela signifie que tout internaute peut en théorie, recevoir quasi-gratuitement des fonds avec pour seule condition d'avoir accès à Internet (l'ouverture d'un compte Twitter étant gratuite). V. exemple de Tweet dédié.

[1489] Consultez la page suivante pour observer le nombre estimé de *nœuds* répartis en temps réel dans le monde. Pour quelques centaines d'euros au total, il est possible de mettre en place son propre *nœud bitcoin,* c'est-à-dire un système de gestion et de

peuvent fournir à la communauté l'historique complet de ces blocs - enregistrés automatiquement sur leurs ordinateurs – en cas de besoin (mise à jour communautaire, piratage, bogue).

Peut-il être considéré comme une monnaie ?

En 2009, le lancement du bitcoin était en partie motivée par le besoin d'éviter les abus du secteur financier qui ont entraîné la crise financière de 2008[1490]. Bien qu'il n'ait pas été directement largement reconnu comme un système viable de cash électronique mondial à l'époque, sa popularité et confiance croissante lui permettent en 2023 de se rapprocher de la célèbre définition d'une monnaie que proposait Aristote. D'après lui, une monnaie doit remplir trois fonctions clés et cumulatives, c'est-à-dire être à la fois une unité de compte, un moyen d'échange ainsi qu'une réserve de valeur. En équilibrant les échanges, elle facilite par conséquent les échanges et développe les relations sociales[1491]. Actuellement, le bitcoin semble remplir les deux premières fonctions clés d'une monnaie et il est probable qu'il remplisse la troisième à l'avenir[1492]. En outre, la définition de la monnaie au sens du philosophe français Joseph Moreau[1493] semble correspondre au fait que le bitcoin puisse devenir une monnaie à part entière, comme cela est déjà le cas au Salvador (v. Annexe 5), à la condition qu'il atteigne un consensus social et politique suffisamment important à l'avenir. En somme, le bitcoin a connu une progression significative depuis sa création en 2009 et continue d'évoluer vers une définition de monnaie plus complète. Cependant, le statut ultime de monnaie légale dépend *in fine* d'une acceptation sociale et politique majoritaire, qui pourrait être possible à long terme bien qu'utopique en l'état actuel des textes qui encadre progressivement son écosystème[1494]. En mars 2023, le bitcoin peut toutefois déjà être considéré comme étant la monnaie d'Internet dans la mesure où plus d'un milliard d'adresses bitcoins ont déjà été impliquées dans une transaction[1495], et que plus de 300 000 transactions sont effectuées chaque jour sur ce réseau[1496]. Il peut ainsi être affirmé que le bitcoin est utilisé quotidiennement par un nombre relativement important d'individus, notamment dans des pays en voie de développement.

---

stockage de ses bitcoins, directement chez soi. De cette façon chaque internaute devient en quelque sorte sa propre banque. Pour plus d'informations, consultez les solutions et périphériques informatiques (*nœuds*) proposés par les sociétés *Umbrel* ou encore *Nodl*

[1490] NAKAMOTO Satoshi, traduction libre de l'anglais, « Le problème avec cette solution est que le sort de l'ensemble du système monétaire dépend de l'entreprise qui gère la frappe de la monnaie, avec chaque transaction devant passer par elle, comme une banque », 2008, accessible en ligne à l'adresse suivante, p.2.

[1491] Aristote théorise le principe d'échanges équilibrés et les trois grandes fonctions de la monnaie, 2022, in *citeco.fr*. Disponible en ligne, « La monnaie sert à la fois d'unité de compte, d'intermédiaire dans les échanges et de réserve de valeur. En équilibrant les échanges, elle les facilite, ce qui permet à chacun de mieux satisfaire ses besoins et développe les relations sociales ».

[1492] En 2029, le bitcoin aura 20 ans d'existence, ce qui permettra probablement d'apprécier avec un meilleur discernement à quel point il aura rempli cette fonction de réserve de valeur.

[1493] MOREAU Joseph, « Aristote et la monnaie », in *Revue des Études Grecques*, tome 82, fascicule 391-393, 1969, pp. 349-364, « La monnaie est alors une institution, non seulement en ce sens qu'elle a été instituée, établie par une convention […], mais parce qu'elle est devenue un usage courant (currency), qui s'impose en vertu de la coutume, des idées reçues, à peu près comme l'usage de la langue. Le nom même qui la désigne […] indique qu'elle ne tient pas sa valeur de la nature, mais de l'opinion commune, de la loi », disponible à l'adresse suivante

[1494] V. Annexes 7 et 14

[1495] Pour plus d'informations, consultez en temps réel ce nombre à l'adresse suivante, Glassnode Studio, « On-Chain Market Intelligence ». Cependant, les utilisateurs peuvent avoir plus d'une adresse de portefeuille bitcoins ou conserver leurs bitcoins sur des plateformes d'échanges centralisés (tiers de confiance), ce qui rend difficile d'estimer le nombre exact de personnes qui utilisent le bitcoin dans le monde.

[1496] Pour plus d'informations, consultez en temps réel ce nombre à l'adresse suivante, in *BitInfoCharts*.

Est-il parfait ?

Si Bitcoin semble initialement s'aligner avec le courant de pensée du « *solutionnisme technologique* »[1497], il semble que le mouvement du « Web 3.0 » lui corresponde plutôt. L'amalgame est toutefois courant, car Bitcoin s'inscrit certes dans le mouvement du Web 3.0, mais avec un positionnement bien particulier qui implique qu'il ne prétend pas être à l'origine une solution technologique ultime à tous les maux numériques mentionnés dans cette recherche. En effet, parce que les promesses du Web 3.0 ne sont pas encore concrètes (Defi, NFT), Bitcoin, lui, a fait ses preuves depuis plus de 14 ans sur le plan informatique et social mais quasi-exclusivement dans le domaine monétaire et peut-être bientôt financier (*v.* Focus 4 suivant). Néanmoins, en tant que monnaie cryptographique distribuée donc supposé indépendante, son cours n'est pas aussi stable qu'une monnaie officielle émise par un gouvernement et il sert principalement comme alternative de paiement ou comme réserve de valeur (sa rareté cryptographique lui valant la juste appellation « d'or numérique »)[1498]. Bien qu'il ait d'un côté acquis une notoriété en tant que valeur refuge auprès d'une communauté d'internautes grandissante, il n'est pas encore largement accepté comme moyen de paiement dans le monde entier en comparaison aux monnaies légalement encadrées[1499]. Il reste probablement un long chemin à parcourir pour que le bitcoin devienne une solution monétaire universelle. En attendant, force est de constater qu'il représente un nouvel actif inédit au sein de l'univers des paiements et plus largement de la finance numérique. Il est ainsi probable que la révolution monétaire initiée par le bitcoin ne soit encore qu'à ses prémices. Dans certains cas, les systèmes de paiement privés actuels peuvent être améliorés voire remplacés par ce réseau de paiement public 3.0, cela étayant la probabilité que d'autres systèmes numériques privés se tournent progressivement vers cette infrastructure publique de confiance et pourtant sans tiers de confiance significatifs susceptible de censurer ce réseau. D'ici quelques années, Bitcoin ne se limitera peut-être plus au domaine monétaire mais pourrait également être utilisée pour d'autres usages et contextes comme la gestion d'identités numériques (IND/INAS), d'écritures comptables, de plateformes de réseaux sociaux ou même de jeux vidéo (métavers). Si le protocole Bitcoin et d'autres systèmes similaires ne sont pas encore matures pour relever certains défis sociétaux, informatiques, politiques et économiques, ils représentent depuis leur lancement une alternative sérieuse et un espoir pour y répondre au moins partiellement à l'avenir. Il est ainsi important pour l'UE de promouvoir et de mettre en place des politiques plus accomodantes pour encourager l'émergence d'autres systèmes informatiques publics qui bénéficieront au bien commun, à la sécurité juridique européenne ainsi qu'à la liberté financière et numérique des citoyens européens.

[1497] MOROZOV Evgeny, « Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique », 2014, Ed. Fyp. Le solutionnisme technologique fait référence à la croyance que tous les problèmes sociaux et politiques peuvent être résolus par la technologie.
[1498] V. Annexe 6, Focus 1.
[1499] Il est possible de consultez sur la carte interactive suivante plus de 8000 commerces qui acceptent en 2023 le bitcoin comme moyen de paiement.

Faut-il le prohiber ?

Parce que la notion de décentralisation informatique, sociale et économique n'est qu'un spectre comme le constate la présente recherche, cette difficile 'confiscabilité' des bitcoins dérange fondamentalement l'ordre établi. Pourtant, cette décentralisation globale semble limitée à long terme, en raison d'une recentralisation sociale et économique progressive de bitcoins, ce que la décentralisation informatique du protocole ne peut probablement pas empêcher elle seule (elle doit également s'accompagner d'une volonté et recherche de décentralisation globale par les internautes de leurs avoirs en bitcoins). Pour autant, il semble complexe et inefficace d'interdire Bitcoin, bien qu'essentiel de mettre en place des règlementations et des lois pour encadrer ses usages et assurer la sécurité juridique des utilisateurs et des entreprises qui s'impliquent au sein de cette infrastructure prometteuse pour un Internet 3.0. De nombreux pays ont déjà adopté des règles spécifiques pour régir l'achat et la vente de crypto-actifs[1500] (bitcoins y compris) en essayant de prendre en compte chacune des caractéristiques informatiques et des finalités de ces actifs, qui sont en réalité pour la plupart informatiquement centralisés (aux antipodes de la recherche de décentralisation continue spécifique à Bitcoin). Ces règles peuvent inclure des exigences de conformité et de transparence pour les entreprises qui utilisent ou proposent ces actifs ou encore des obligations de déclarations comptables et fiscales pour les individus qui les possèdent et les utilisent. En établissant des règlementations appropriées, mais proportionnées, il serait possible de protéger les consommateurs des activités illégales qui ont effectivement été facilitées par bitcoin par le passé[1501]. Toutefois, en fonction des parties prenantes techniques d'une technologie blockchain, comme ses utilisateurs, ses investisseurs, ses opérateurs de nœuds ainsi que les sociétés françaises et étrangères opérant dans son écosystème, la règlementation est souvent perçue comme une tentative d'ingérence, c'est-à-dire de centralisation et de contrôle, sur ce protocole informatique pourtant décentralisé (*v.* Annexe 7). En réponse à ces exigences règlementaires pour certaines peu proportionnées et dont les motivations politiques ne semblent plus cachées comme cela a été démontré, un mouvement social porté par des individus « *maximalistes de la décentralisation* »[1502] et en faveur de la protection du protocole Bitcoin, se fait entendre sur Internet. A la date d'écriture de cette thèse, il est peu probable qu'une interdiction partielle ou totale de Bitcoin entraîne sa disparition, comme le suggèrent pourtant certains chercheurs[1503]. En effet, ce réseau existe depuis plus de 14 ans en vertu de « l'effet Lindy », déjà mentionné, et ce dernier n'a encore jamais été attaqué informatiquement par un consortium d'États ou d'entreprises. Des attaques existent plutôt sur le plan politique comme le rappel cette recherche. Au lieu

[1500] V. Annexe 14

[1501] Après son lancement, le bitcoin a été rapidement adopté comme une forme de monnaie numérique sur des plateformes illégales en ligne, qu'elles soient visibles ou cachées sur l'internet. Bien que la majorité des transactions Bitcoin soient désormais légales, cette histoire tumultueuse a laissé des stigmates qui continuent de susciter une confusion entre ces utilisations licites et illicites de cette monnaie numérique. Cette étude démontre également que cette image passée est devenue un argument politique plus que pragmatique.

[1502] V. *supra*, I, Titre 2, 2.1.3

[1503] DUFRENE Nicolas, DELAHAYE Jean-Paul, et al., « Il est urgent d'agir face au développement du marché des cryptoactifs et de séparer le bon grain de l'ivraie », Tribune de l'Institut Rousseau du 8 février 2022, consulté le 18 octobre 2022 à l'adresse suivante

de l'interdire[1504], il semblerait préférable de composer avec ce protocole informatique innovant voire de l'encourager pour ses différents cas d'utilisation, notamment au regard de ses bénéfices sociaux et numériques (*v.* Focus 3 à 6). Ainsi, plutôt que de considérer Bitcoin comme une menace sociétale nécessitant une interdiction légale directe ou bien détournée (plus probable), il semble plus judicieux de l'aborder comme une opportunité pour les entreprises et les organisations qui peuvent d'ores et déjà explorer de nouvelles formes de transactions numériques plus vérifiables, résilientes et sécurisées.

Focus 2 : La résilience informatique du protocole Bitcoin face à la fragilité de son écosystème

Pour que la blockchain Bitcoin garantisse son fonctionnement et sa sécurité informatique, elle se doit d'attirer de nouveaux utilisateurs, d'une part pour atteindre un effet de réseau suffisant pour assurer sa décentralisation et sa résilience informatique, et d'autre part pour affirmer son utilité sociale sur le plan énergétique comme cela est étudié dans l'Annexe suivante. Parmi ces utilisateurs et investisseurs, certains deviennent des validateurs du réseau (« miners ») moyennant une rétribution automatique et variable en bitcoins pour leur contribution matériel et électrique à la sécurisation de ce protocole. A cet égard, la création de bitcoins doit suivre des règles d'émission strictes[1505], comme une quantité limitée ainsi qu'une émission restreinte de nouveaux jetons, des règles communément définies et modifiés par sa communauté d'internautes (développeurs, mineurs). Ce fonctionnement transparent, lisible et accessible par tout autre internaute permet ainsi à Bitcoin - aux yeux de son nombre croissant d'utilisateurs - de se voir conférer une valeur d'usage et de réserve progressivement croissante, car résultantes de l'offre et de la demande de bitcoins sur Internet. Pour approfondir ce processus, un utilisateur – ajourd'hui souvent un professionnel - extrait des bitcoins en exécutant un logiciel qui cherche la solution à un problème mathématique long à résoudre[1506] et dont le degré de difficulté est connu avec précision. Cette difficulté de résolution (*v.* Annexe 6, Focus 1) est ainsi automatiquement ajustée selon un calendrier informatiquement prévisible, de sorte que le nombre de solutions trouvées pour une unité de temps donnée soit constant. Ainsi, le réseau Bitcoin vise environ six solutions par heure soit une toutes les dix minutes[1507]. Lorsqu'une solution est trouvée, la machine de l'utilisateur

[1504] Pour observer en temps réel les pays ayant interdits ou autorisé Bitcoin, consultez la carte interactive suivante, in *Bitrawr,* « Bitcoin Legality by Country Map ».

[1505] NAKAMOTO Satoshi, traduction libre de l'anglais, « La nature du Bitcoin est telle que, dès la sortie de la version 0.1, la conception fondamentale a été figée pour le reste de sa durée de vie. C'est pourquoi j'ai voulu la concevoir pour prendre en charge tous les types de transactions possibles auxquels j'ai pu penser. […] Si le Bitcoin connaît un grand succès, ce sont des choses que nous voudrons explorer à l'avenir, mais elles devaient toutes être conçues dès le début pour s'assurer qu'elles seraient possibles plus tard. Je ne pense pas qu'une deuxième implémentation compatible du Bitcoin sera jamais une bonne idée. », in « *Transactions and Scripts* », 17 juin 2010, accessible en ligne à l'adresse suivante

[1506] En réalité, les mineurs ne produisent pas directement des bitcoins, ils produisent des blocs. S'ils sont valides, les mineurs sont automatiquement récompensés en bitcoins par le protocole. Le calendrier d'émission de bitcoins étant fixé et stable dans le temps, plus d'énergie utilisée pour le minage ne signifie pas que plus de bitcoins seront minés. Dès lors, ce que beaucoup appellent aujourd'hui le « *minage* » se poursuivra après le *minage* du dernier bitcoin. Par conséquent, le terme de « *minage* » ou « *d'extraction* » est sémantiquement trompeur et inapproprié et il pourrait être désigné par le concept de « *production de blocs* ». Toutefois, par soucis d'intelligibilité, il est communément admis dans l'écosystème Bitcoin de conserver le terme de *minage*, ici privilégié.

[1507] NAKAMOTO Satoshi, traduction libre de l'anglais, « Il s'agit d'une base de données distribuée à l'échelle mondiale, avec des ajouts à la base de données consentis par la majorité, en fonction d'un ensemble de règles qu'ils suivent : - Chaque fois que quelqu'un trouve une preuve de travail pour générer un bloc, ce dernier reçoit de nouvelles pièces [bitcoins]. - La difficulté de

informe automatiquement le reste du réseau de l'existence de cette solution nouvellement trouvée ainsi que d'autres informations regroupées dans ce qu'on appelle un « bloc (de transactions) ». Notons que si chaque solution est volontairement longue à trouver pour des « miners » (ordinateurs validateurs), elles sont faciles à vérifier par les autres nœuds du réseau (des ordinateurs vérificateurs moins spécifiques et puissants), étant donné que le chemin de cette solution a déjà été tracé par un validateur puis très rapidement propagée, vérifié et approuvé par les autres nœuds vérificateurs du réseau qui stockent l'historique desdits blocs.

Le processus et mécanisme de validation informatique mentionné, celui qui consomme aujourd'hui une importante quanité d'électricité, est nommé la Preuve de travail (« Proof of Work – PoW »), détaillée au début de l'Annexe 6. Grâce à ce mécanisme, tout bloc créé par un utilisateur malveillant qui ne respecterait pas les règles communes à ce protocole sera rejeté par les autres participants du réseau (mineurs et/ou nœuds). Concrètement, lors de chaque transaction en bitcoin, chaque information est envoyée et transmise au plus grand nombre possible d'ordinateurs et nœuds du réseau. De cette façon, s'illustre un registre prenant la forme – imagée - d'une chaîne de blocs en croissance constante, maintenu collectivement par un nombre très important de machines et d'ordinateurs (chacun en possède une copie complète ce qui évite toute perte des données et assure une résilience optimale et durable des transactions de cette chaîne cryptographique). En effet, tous les blocs sont automatiquement enchaînés cryptographiquement de telle manière que, si l'un d'entre eux venait à être modifié, tous les blocs précédents et suivants devraient être recalculés, ce qui est informatiquement impossible en l'état des connaissances informatiques actuelles.

Cependant, si Bitcoin est théoriquement immune aux attaques informatiques comme en témoigne son fonctionnement sans incident majeur depuis plus d'une décennie[1508], son écosystème ne l'est pas pour autant comme en témoigne les récurrentes et multiples affaires d'escroqueries, de vols[1509] ou de gel, de saisie et confiscation par voie légale de bitcoins mal acquis. Cela s'explique par l'importante décentralisation informatique qui protège son protocole et non pas son écosystème d'acteurs qui demeure le plus souvent centralisé sur le plan informatique et social comme l'illustre l'Annexe 7. Il peut également être souligné plusieurs sources de dépendance dont Bitcoin fait l'objet, notamment à la

---

la preuve de travail est ajustée toutes les deux semaines pour viser une moyenne de 6 blocs par heure (pour l'ensemble du réseau). - Le nombre de pièces données par bloc est divisé par deux tous les 4 ans. On pourrait dire que les pièces sont émises par la majorité. Elles sont émises en quantité limitée et prédéterminée », 18 février 2009, accessible en ligne à l'adresse suivante

[1508] Il est fait référence à un cas de piratage survenu sur la blockchain Bitcoin en août 2010. Contrairement à la pensée commune, Bitcoin a en effet déjà subis une attaque informatique avec succès : un pirate informatique a exploité une faille dans son code pour générer 184 milliards de bitcoins (alors que le total de bitcoins en circulation est limité à 21 millions de bitcoins comme évoqué plus loin). Le bogue a été corrigé en quelques heures par Satoshi Nakamoto en personne. La personne à l'origine de cet évènement nommé « The value overflow incident » reste à ce jour inconnue. V. « Strange block 74638 », in *bitcointalk.org* le 15 août 2010, consulté le 2022 à l'adresse suivante

[1509] Le Monde avec AFP, « Sam Bankman-Fried, ancien PDG de la plate-forme de cryptomonnaies FTX, plaide non coupable à New York », 2023, Le Monde.fr, V. également Wikipedia contributors, « *Mt. Gox* », disponible à l'adresse suivante

production de puces informatiques[1510] ou à certaines normes informatiquement et socialement centralisées d'Internet, que Bitcoin exploite et dont il peut dépendre[1511]. Cela signifie qu'en théorie ces leviers de dépendances latents pourraient un jour être activés et articulés par certains acteurs (entreprises, institutions, gouvernements) afin de déstabiliser ce réseau. En pratique, il serait assez complexe pour des acteurs de réussir à coordonner l'activation de tels leviers afin de décrédibiliser la confiance accordée dans tout ou partie de ce réseau et de son écosystème d'acteurs. Conscients de ces dépendances et menaces pour l'instant inexploitées, certains acteurs de la communauté Bitcoin innovent continuellement aux fins de réduire ces liens de dépendance informatique et sociaux, notamment aux infrastructures d'Internet toujours centrales (TCP/IP, plateformes internet, etc.). Par exemple, il est possible depuis août 2017 de faire fonctionner un nœud Bitcoin satellitaire via l'acquisition d'une parabole directement reliée au satellite de la société Canadienne Blockstream[1512]. Ce dernier synchronise en temps réel les blocs valides de la blockchain Bitcoin puis transmet ces données à chaque parabole de ce réseau parallèle, désormais indépendant d'Internet, car satellitaire. Plus récemment, depuis juillet 2022, il est possible d'envoyer des fractions de bitcoins (« satoshis ») via le Lightning Network[1513] directement depuis tous les types de téléphones mobiles, une solution actuellement déployée en Afrique[1514]. Ainsi, Bitcoin semble progressivement moins dépendant d'Internet, une tendance qui devra se confirmer à l'avenir pour assurer sa résilience informatique dans un temps long.

Focus 3 : Un nouveau système d'incitation et de valorisation économique et comptable

Une fois validés, les blocs créent et libèrent actuellement 6,25 nouveaux bitcoins toutes les dix minutes[1515]. Ce montant, appelé récompense de bloc (« *genesis bloc compensation* »), incite les utilisateurs à réaliser le travail de calcul mentionné – et approfondie en Annexe 6 - afin de générer de nouveaux blocs conformes. A noter que tous les quatre ans environ, le nombre de bitcoins qui peuvent être minés, c'est-à-dire émis par bloc, est réduit de moitié (un phénomène nommé « *halving* »). Cette raréfaction cryptographique programmée explique ainsi une hausse a priori durable de la valorisation d'un bitcoin à travers le temps[1516], car l'offre devient théoriquement inférieure à la demande grâce à ce

[1510] Pour toute l'industrie informatique et y compris pour l'infrastructure Bitcoin, le déclenchement d'un conflit à Tawaïn pourrait entraîner une rupture probable de l'approvisionnement en puces informatiques, notamment pour certains *circuits intégrés* (*ASIC*). Les sociétés de minage reposent en effet sur la société TSMC (en *oligopole* avec plus de 50% de parts de marché) qui produit à ce jour une importante quantité de ces composants donc nécessaire à l'infrastructure Bitcoin). Une telle dépendance matérielle de Bitcoin à ces puces et leurs fournisseurs est un point de dépendance sujet aux aléas de sa géopolitique et géographie proche. V. Wikipédia contributors, « Taiwan Semiconductor Manufacturing Company », 2022, disponible à l'adresse suivante

[1511] De FILIPPI Primavera, « Blockchain and the Law », 2017, *op. cit.*, « *Les protocoles comme le Bitcoin s'appuient finalement sur TCP/IP pour fonctionner.* », emplacement 968 sur 7004.

[1512] Consultez les « *Satellite Kits* » sur le Blockstream Store à l'adresse suivante ainsi que la carte interactive dédiée

[1513] V. Annexe 6, Focus 1.

[1514] MAIRE Vincent, « Bitcoin (BTC) : Machankura permet de recevoir des satoshis sans connexion Internet », 2022, disponible à l'adresse suivante

[1515] Pour rappel, pour être acceptés dans la chaîne des blocs précédents, les nouveaux blocs doivent inclure une *Preuve de travail* valide.

[1516] En 2008, la récompense pour chaque bloc de bitcoin était de 50 unités, émises toutes les dix minutes. Cette récompense a été réduite de moitié automatiquement le 28 novembre 2012, passant à 25 bitcoins émis toutes les dix minutes, puis encore réduite de moitié le 9 juillet 2016, pour atteindre 12,5 bitcoins, et de nouveau le 11 mai 2020 pour atteindre 6,25 bitcoins. En

mécanisme initialement artificiel adopté il y a 14 ans[1517], et désormais supposé immuable par sa communauté. En 2140 environ, cette diminution programmée de la récompense par bloc prendra fin et les validateurs (« miners ») seront donc exclusivement rémunérés en percevant des frais sur la validation des transactions des utilisateurs[1518]. A cet égard, l'utilisateur qui envoie une transaction en bitcoin paie ainsi une commission sur la transaction qui sera conservée par celui qui trouvera le prochain bloc. Le paiement de ces frais par les utilisateurs encourage ainsi les miners à inclure plus rapidement la transaction dans un nouveau bloc (plus les frais son important plus la transaction sera rapidement traitée dans la limite de 10 minutes entre chaque bloc). Notons par ailleurs que la dépense électrique des miners nécessaire pour trouver la solution mathématique susvisées (qui est un *hash gagnant* parmi tous les autres *hash calculés*), est intuitivement perçu comme un gaspillage énergétique[1519]. En réalité, ces calculs supposés informatiquement inutiles représentent un coût électrique sur lequel repose le statut et la valeur sociale et monétaire accordés à Bitcoin en comparaison aux monnaies fiduciaires actuelles (qui ne reposent pas sur un modèle de coût énergétique unifié et transparent). Parallèlement à ce processus d'émission monétaire programmée et stable dans le temps grâce à la protection de sa communauté de développeurs, il est essentiel de rappeler qu'il n'y aura jamais plus de 21 millions de bitcoins émis, ce qui signifie que sa quantité totale émissible est limité en nombre et dans le temps, au même titre que la quantité théorique d'or disponible dans le monde[1520].

Sur un plan comptable, l'augmentation progressive du nombre de transactions en bitcoins[1521], y compris pour des transactions économiques, pourrait enrichir la comptabilité à double entrée[1522] qui est

---

mai 2024, cette même récompense sera de 3,12 bitcoins émis toutes les dix minutes. Cette rareté planifiée, constante et automatique dans la production de nouveaux bitcoins conduit à une augmentation théorique et progressive de sa valeur tous les quatre ans, comme pour l'or dont la quantité disponible et en circulation est limitée, ce qui explique le surnom « *d'or numérique* » attribué aux bitcoins.

[1517] Il est souligné que ces mécanismes algorithmiques et physiques (machines) qui ont pour objet et effet de générer une raréfaction numérique sont initialement 'artificiels' dans le sens où ils sont socialement programmés et souhaités par sa communauté (contrairement à l'or par exemple). Toutefois, cette raréfaction devient progressivement 'pure' et non plus 'artificielle', car les personnes à l'origine de ces mécanismes n'en possèdent plus le contrôle et ne peuvent plus exercer d'influence sur ces concepts qui fonctionnent finalement au service de tout ce réseau ouvert qui devient par conséquent un bien commun numérique.

[1518] Si ce système de raréfaction cryptographique programmée tient sa promesse d'ici 2140, chaque fraction de bitcoin émis deviendra très rare et par effet de conséquence un prix élevé, ce qui garantira aux validateurs/mineurs un revenu économique fiable et durable grâce aux frais de transactions entre les utilisateurs comme unique source de rémunération (car après 2140 il n'y aurait plus de « *genesis bloc compensation* »).

[1519] V. Annexe 6, Focus 1.

[1520] Cette quantité est estimée à l'équivalent d'un stade de football seulement, ce qui explique la rareté de l'or et donc son prix élevé. Toutefois, il semble important de distinguer deux notions, la *rareté relative* de la *rareté absolue*. L'or est d'une *rareté relative*, car sa quantité totale est limitée et soumise aux moyens d'extraction (mines, machines), tandis que le bitcoin est d'une *rareté absolue*, puisque sa quantité est mathématiquement limitée et informatiquement scellée, ce qui signifie que tenter d'utiliser plus d'ordinateurs pour extraire plus que 21 millions de bitcoins est théoriquement impossible. Le choix de ce montant de 21 millions de bitcoins s'explique en ces termes par Satoshi Nakamoto (librement traduit de l'anglais) « Mon choix pour le nombre de pièces [bitcoins] et le programme de distribution était une supposition éclairée. C'était un choix difficile, car une fois que le réseau est lancé, il est verrouillé et nous sommes coincés avec lui. Je voulais choisir quelque chose qui rendrait les prix similaires aux monnaies existantes, mais sans connaître l'avenir, c'est très difficile. J'ai fini par choisir une solution intermédiaire. Si le bitcoin reste une petite niche, il vaudra moins par unité que les monnaies existantes. Si vous imaginez qu'il soit utilisé pour une fraction du commerce mondial, il n'y aura que 21 millions de pièces pour le monde entier, et sa valeur unitaire sera donc beaucoup plus élevée. », in *Gmail - Questions about Bitcoin*, consulté le 27 octobre 2022, à l'adresse suivante

[1521] Il est possible d'observer en temps réel depuis 2010 jusqu'à aujourd'hui la croissance indéniable des transactions réalisées sur la blockchain bitcoin. Consultez le lien suivant, Blockchain.com | « Charts - Total Number of Transactions. ».

[1522] Wikipédia contributors, « Comptabilité en partie double », 2022, disponible à l'adresse suivante

aujourd'hui comptablement normalisée pour toute personne morale. En effet, les registres comptables, qu'ils soient papiers ou digitaux, peuvent être facilement manipulés et modifiés par des tiers, ce qui peut engendrer des erreurs qui peuvent compromettre l'équilibre d'une comptabilité. L'utilisation de la blockchain Bitcoin et des bitcoins pourraient contribuer à réduire l'impact des erreurs humaines en automatisant certains types de transactions et en fournissant des données plus précises et plus facilement vérifiables. Par conséquent, l'incorporation des bitcoins dans une « *comptabilité à double entrée* » pourrait améliorer l'exactitude, la transparence et l'efficacité de certains processus comptables. Ce concept de « *comptabilité à triple entrée* »[1523] est un concept principalement rendu possible par la blockchain publique Bitcoin. Ce nouveau principe comptable propose ainsi une troisième composante 3.0 : une blockchain publique. Parce que seule la blockchain publique Bitcoin semble incorruptible, c'est-à-dire probablement présente dans quelques décennies, sa transparence informatique permettrait de l'utiliser en tant que système d'audit comptable et financier. En effet, chaque débit en bitcoins pourrait servir à horodater, suivre, voire émettre des crédits liés à d'autres actifs (euro, autres crypto-actifs stables ou non) qui seraient ancrés sur cette chaîne de données cryptographiques afin de laisser une trace comptable et numérique inaltérable. Cela permettrait supposément de réduire considérablement certaines erreurs et fraudes comptables, tout en assurant une accessibilité en temps réel à chaque entrée comptable (débit, crédit). Au-delà des preuves d'identités numériques mentionnées dans cette recherche, une utilisation pertinente de la comptabilité à triple partie consisterait à certifier des informations comptables professionnelles et commerciales (non pas personnelles), telles que des comptes annuels ou des réserves obligatoires spécifiques aux banques commerciales[1524]. Cela permettrait de prouver de manière fiable et plus transparente l'approbation de ces informations, renforçant ainsi la responsabilité, la confiance et la crédibilité liées aux transactions financières, cela dans un contexte – de crise de la confiance - numérique. Bien que la comptabilité à triple partie soit principalement applicable à la blockchain Bitcoin qui possède seule un degré de décentralisation pure au sens de cette étude[1525], son émergence sera probablement confrontée à de nombreuses barrières sociales, politiques et juridiques mentionnées tout au long de cette étude. Pour faire adopter ce principe de comptabilité à triple entrée, l'utilisation de certaines couches et protocoles complémentaires à celui de Bitcoin, comme le « Lightning Network », « Taro » ou plus récemment « Ordinal »[1526] et « Bitcoin Stamps »[1527] étudiés plus loin, pourrait permettre de surmonter une partie de ces freins aujourd'hui omniprésents. Concrètement, la récente mise à jour Taro et les développements qui s'en suivront permettraient d'ancrer des documents administratifs et comptables directement sur la blockchain Bitcoin, tout en permettant la réalisation d'opérations de prêts et de crédits directement sur cette même blockchain (toujours avec l'intervention d'institutions financières 2.0 et 3.0 légalement encadrées). Cela

[1523] Bitcoin.fr, « Une application de Bitcoin : la comptabilité à triple entrée », 2015, disponible sur bitcoin.fr
[1524] Banque de France, « Les réserves obligatoires », 2022, disponible à l'adresse suivante
[1525] V. *supra*, I, Titre 2, 2.1.3
[1526] V. ci-après.
[1527] V. ci-après.

pourrait ouvrir la voie à l'avènement de la comptabilité à triple partie, en redéfinissant les contours de nos principes comptables actuels. Finalement, il est souligné que l'augmentation progressive du prix du bitcoin depuis son lancement incite les acteurs économiques à rejoindre ce réseau pour le sécuriser, tout en finançant ses améliorations algorithmiques et infrastructurelles. Il s'agit donc d'un cercle de financement vertueux qui contribue à créer un bien commun cryptographique rare plutôt bénéfique pour l'humanité.

Focus 4 : Vers un réseau monétaire (Lightning Network), financier (Taproot & Taro) et de stockage (Ordinals/Bitcoin Stamps), multimodal et en devenir

Pour garantir qu'un tiers et un utilisateur malicieux ne puisse pas dépenser les bitcoins d'autres utilisateurs en créant des transactions non conformes, le protocole Bitcoin utilise la cryptographie à clé publique afin d'assurer une vérification des signatures numériques. Dans ce système, chaque utilisateur possède une adresse unique associée à une paire de clés publiques et privées qui sont conservés dans un portefeuille bitcoin dédié (généralement via une application mobile, un logiciel sur un ordinateur ou encore clé USB spécifique, tous dédiés à cet effet). Seul l'utilisateur possédant une clé privée peut signer une transaction pour envoyer tout ou partie de ses bitcoins à l'adresse bitcoin – clé publique - d'un autre internaute et utilisateur. Grâce à ce fonctionnement, chaque utilisateur est en mesure d'échanger des bitcoins avec d'autres utilisateurs moyennant un coût et un temps de validation relativement faibles à date en comparaison au secteur bancaire[1528]. De cette façon, le protocole Bitcoin fournit d'ores et déjà un système de paiement efficace pour les transactions de montants importants. Si un utilisateur peut en théorie également réaliser des transactions de faibles montants (« microtransactions »), les frais de transaction applicables dissuadent en pratique souvent les utilisateurs à réaliser de telles opérations, car les frais sont supérieurs au montant desdites transactions. Cette impossibilité de réaliser des transactions de quelques centimes - en fractions de bitcoins (microtransactions en « satoshis ») - constituait dès 2015 une problématique pour certains utilisateurs. En effet, cela empêchait le bitcoin d'être considéré comme une monnaie. La possibilité de réaliser des microtransactions est donc essentielle pour de nombreux échanges comme l'achat de produits de première nécessité (alimentaires, logement). Sans une solution adéquate pour le réseau Bitcoin, les utilisateurs doivent concrètement attendre des dizaines de minutes, parfois plusieurs heures, avant d'être certains que leurs transactions sont inscrites dans un bloc valide. Dès lors, ces paiements inférieurs à quelques euros d'équivalent en satoshis n'étant que peu adapté sur le réseau principal de Bitcoin (« *Layer 1 - L1* ») en raison des frais trop importants, un réseau informatique secondaire (« *Layer 2 - L2* ») est imaginé en 2015 puis implémenté à partir de 2017 pour

[1528] En réalité, il est souligné que les frais fluctuent automatiquement selon certains paramètres du réseau Bitcoin. Toutefois, l'utilisateur peut toujours décider des frais qu'il souhaite verser aux mineurs pour que sa transaction soit validée dans le bloc le plus proche (au mieux en dix minutes et autrement après plusieurs blocs, par exemple 6 blocs, soit 60 minutes d'attente).

répondre à cette problématique : le « *Lightning Network - LN* »[1529]. Le LN[1530] est simplement un protocole P2P dont la particularité est d'être cryptographiquement attaché à la blockchain Bitcoin (L1). De cette façon, le LN peut être considéré comme un protocole informatique d'externalisation (L2)[1531] dédié à la réalisation de microtransactions en fractions de bitcoins, dont la sous-unité de compte se nomme pour rappel un « *satoshi* »[1532]. A ce jour fonctionnel et en cours d'adoption continue par des dizaines de milliers de personnes dans le monde, le LN permet donc non seulement à ses utilisateurs d'effectuer des transactions de tous les montants, au même titre qu'une monnaie (ici indépendante et automatisée), mais également de dépenser une fraction de ces actifs comme étant une réserve de valeur, ce qui est par exemple impossible pour l'or qui ne peut pas être aisément fractionné puis dépensé. En d'autres termes, cela signifie qu'il est désormais possible grâce au LN de dépenser des fractions de son or numérique (en satoshis), une action impossible avec un lingot d'or. Dès lors, Bitcoin et ses protocoles (L1 et L2) permettent à la fois de conserver de la valeur dans le temps, tout en permettant de dépenser des fractions de bitcoins instantanément, quasi-gratuitement et sans tiers de confiance. Ainsi, la blockchain Bitcoin (LN y compris) constitue une (r)évolution pour le secteur des paiements en ligne. Toutefois, le Lightning Network demeure un protocole en phase d'expérimentation (« *beta* »)[1533] avec certaines failles de sécurité théoriques déjà identifiées[1534], bien que non exploitées à ce jour. Le LN est également partiellement centralisé d'un point de vue informatique et social (v. Annexe 7), tout simplement car son lancement est relativement récent. Si son fonctionnement est fait pour être progressivement décentralisé comme la blockchain Bitcoin (L1), cela nécessite du temps ainsi qu'un certain effet réseau, incompressibles, entrainant en attendant un besoin et degré de confiance initial (des tiers offrant des accès simplifiés donc plutôt centralisés à ce L2). Si ce réseau est en phase de croissance depuis son lancement, il faut rappeler qu'il ne peut pas en l'état actuel (2023) être implémenté et utilisé par tous. D'une part il ne convient pas à toutes les situations, c'est-à-dire qu'il ne répond pas à tous les besoins de paiements, et d'autre part, une adoption trop soudaine entraînerait probablement certains des

[1529] MICHALAKIS Fanis, chaîne Youtube, disponible à l'adresse suivante
[1530] Pour comprendre les rudiments de ce protocole adjacent à la blockchain Bitcoin consultez la traduction suivante, libre de l'anglais, « Le Lightning Network est un système décentralisé de micropaiements instantanés à haut volume qui élimine le risque de déléguer la garde des fonds à des tiers de confiance. Par exemple, Bitcoin, la monnaie numérique la plus largement utilisée et la plus précieuse au monde, permet à quiconque d'envoyer de la valeur sans intermédiaire ou dépositaire de confiance. Bitcoin contient un système de script avancé qui permet aux utilisateurs de programmer des instructions pour les fonds. Cependant, il y a des inconvénients au design décentralisé de Bitcoin. Les utilisateurs doivent attendre des dizaines de minutes voire une heure pour avoir confiance que leurs transactions ne seront pas annulées. Les micropaiements, ou les paiements inférieurs à quelques centimes, sont confirmés de manière inconsistante, et les frais rendent de telles transactions inviables sur le réseau aujourd'hui. Le Lightning Network résout ces problèmes. Il est l'une des premières mises en œuvre d'un contrat intelligent multi-parties (argent programmable) utilisant le script intégré de Bitcoin. », « Layer 2 | Lightning Network. » (2022), in *MIT Digital Currency Initiative*, disponible à l'adresse suivante
[1531] Les transactions de montants élevés (par exemple supérieures à 100€ d'équivalent en bitcoins) sont réalisées sur le *Layer 1* et les transactions de faibles montants sur le *Layer 2* (Lightning Network).
[1532] Les *satoshis* sont des fractions de bitcoins, il s'agit du même actif mais simplement d'une unité de compte plus précise. A date du 14/08/2022, 1 *satoshi* équivaut à 0.00000001 bitcoin ou encore 0,00024 centime de dollars, v. le site de conversion en ligne à l'adresse suivante
[1533] Lightning Labs, « Announcing lnd 0.15 beta: To Taproot and Beyond! », 2022, disponible à l'adresse suivante
[1534] SGUANCI Cosimo, « Mass Exit Attacks on the Lightning Network », 2022, University of Illinois at Chicago Chicago, disponible à l'adresse suivante

défis informatiques mentionnés dans cette recherche (centralisation et/ou congestion du réseau, augmentation des frais, attaques informatiques, etc.)[1535].

En 2021, une nouvelle mise à jour du protocole Bitcoin propose l'implémentation de « *Taproot* », une amélioration de son système qui combine plusieurs propositions d'optimisation du protocole Bitcoin (« *Bitcoin Improvement Proposal - BIP* »)[1536]. Ces propositions de mises à jour ont été implémentées en novembre 2021 puis progressivement déployées au sein des logiciels et des applications de l'écosystème Bitcoin, c'est-à-dire rejoins par les logiciels de portefeuilles numériques ainsi que par les plateformes d'échange, qui permettent pour rappel la conversion et/ou l'échange de bitcoins. Concrètement, l'implémentation de Taproot a permis de renforcer l'évolutivité de Bitcoin, c'est-à-dire sa mise à l'échelle, mais contribue également à sa sécurité, à sa confidentialité (pseudo-anonymat) et à la flexibilité de ses transactions. D'ici quelques mois ou années, Taproot ouvre la voie au déploiement des concepts de contrats intelligents, de DAO, de NFT ou de stablecoins directement sur la blockchain Bitcoin (voir la complémentarité avec le protocole « *Taro* » ci-dessous). Ainsi, de nombreuses briques technologies pourront à terme être rattachées à Bitcoin pour construire des services associés de tout ordre, tels que des réseaux sociaux décentralisés, des navigateurs en ligne distribués (P2P)[1537], etc.

Fort de multiples mises à jour consécutives, notamment « *Segwit* » opérée en 2017[1538], savamment orchestrée par sa communauté puisque compatibles et imbriquées chronologiquement les unes aux autres, le lancement d'un nouveau protocole en cours de conception a été annoncé le 5 avril 2022 : « *Taro* ». Annoncée en avril 2022[1539], ce nouveau protocole permettrait, pour simplifier, de diversifier Bitcoin en rendant ses L1 et L2 compatibles avec de multiples cas d'usages pour l'instant inaccessibles à ses utilisateurs. Pour certains, Taro représenterait un sérieux aboutissement pour le projet et l'écosystème de Bitcoin : son protocole deviendrait multifonctions, multimodal, et non plus monofonctionnel comme à présent. Il évoluerait ainsi depuis une infrastructure numérique exclusivement monétaire vers une infrastructure numérique éclectique[1540]. Pour les institutions financières, l'implémentation puis l'adoption de Taro représenterait probablement, si elles tiennent leurs promesses, un immense défi au regard de certains de leurs modèles d'affaires actuels. Concrètement,

---

[1535] V, *supra*, I, Titre 1, 2.3.2

[1536] Lorsque des développeurs souhaitent faire une mise à jour concernant le protocole Bitcoin, ces derniers soumettent des *BIP* sur le compte Github dédié

[1537] En novembre 2022, le navigateur *Impervious* a fait son apparition. Il s'agit d'une suite d'outils P2P pour les communications et les paiements, intégrée directement dans le navigateur Web des internautes. Ce navigateur intègre d'ores-et-déjà nativement le Lightning Network, les standards de l'identité décentralisée (did) ainsi que le protocole ION que nous avons évoqué. En bref, ce navigateur nous conforte dans notre hypothèse qu'il s'agit d'une nouvelle étape vers une identité numérique native et sophistiqué bâti directement sur la blockchain Bitcoin (INAS). Pour plus d'informations, consultez l'adresse suivante

[1538] Investopedia, « What Is Segregated Witness (SegWit)? », 2022, disponible à l'adresse suivante

[1539] « Nous considérons Taro comme une étape importante dans la 'bitcoinisation' du dollar, en obtenant le meilleur des deux mondes : 1) en émettant des actifs comme les stablecoins sur la blockchain la plus décentralisée et la plus sûre, le bitcoin, et 2) en permettant aux utilisateurs d'effectuer des transactions sur le réseau de paiement mondial le plus rapide et aux frais les plus bas, le Lightning », « Announcing Taro : A New Protocol for Multi-Asset Bitcoin and Lightning », 5 avril 2022, in *Lightning Labs*. Disponible à l'adresse suivante

[1540] « Qui rassemble une grande variété de tendances, qui choisit dans des catégories très diverses », in *Larousse 2022*. Définitions : éclectique - Dictionnaire de français www.larousse.fr

Taro permettrait à tout internaute, organisation et utilisateur de bitcoins, d'émettre leurs propres actifs directement sur la blockchain Bitcoin, avec une efficacité quasi-instantanée, une importante capacité de volume et moyennant des frais de transactions relativement faibles. Dans l'hypothèse où Bitcoin atteindrait grâce à Taro ce Graal numérique décentralisé d'abord monétaire, puis éventuellement financier et industriel, les banques centrales et plus généralement les institutions du monde entier subiraient une certaine remise en question de leur utilité et rôle respectifs. Ce passage numérique vers un univers monétaire et financier 3.0 commun permettrait de renégocier certains rapports de force souvent défavorables qu'entretiennent certains pays en voie de développement et leurs monnaies instables (Bolivar vénézuélien, Livre turque, Livre libanaise), face aux monnaies plus fortes des pays développés. A ce titre, la reconnaissance du bitcoin en tant que monnaie légale au Salvador constitue une première étape vers cet avenir utopique (*v.* Annexe 5). S'il est difficile de soutenir que Bitcoin puisse accueillir toutes les transactions digitales dans un avenir proche, en raison de son incapacité à répondre à tous les besoins complexes de la société, il semble pour autant fournir un socle pertinent pour toutes les transactions à forte valeur ajoutée sociale, identitaire, financière, monétaire ou comptable. Pour l'instant, Taro est aux prémices de son développement, le Lightning Network lui fournissant un socle plus avancé, mais également toujours en construction. Pour l'heure, il n'y a aucune garantie que Taro soit mis en œuvre et déployé avec succès dans un avenir proche, car les difficultés et les imprévus sont des risques constants et récurrents lors des processus de développement de logiciels complexes, car ici imbriqués et ouverts.

Début 2023, une nouvelle fonctionnalité - involontairement permise par la mise à jour Taproot mentionnée - a émergé : le protocole « *Ordinals* »[1541]. Ce concept propose la création de ce qui s'apparente à des NFT directement stockés au sein des blocs Bitcoin. Pour rappel chaque bitcoin est composé de petites unités, des satoshis, et ces derniers peuvent désormais – grâce au protocole *Ordinals* - être individuellement 'gravé' avec du contenu tels que des images, des vidéos ou du texte, afin de créer des artefacts numériques uniques qui circulent sur la blockchain Bitcoin. Ils peuvent ainsi être conservés dans des portefeuilles Bitcoin spécifiques et transférés à l'aide de transactions classiques en bitcoins. Ces gravures (« *inscriptions* »)[1542] ou NFT spécifiques à la blockchain Bitcoin, sont donc supposées aussi durables, immuables, sécurisées et décentralisées que cette infrastructure sur laquelle ils reposent (L1).

Par conséquent, ces multiples mises à jour consécutives semblent progressivement s'orienter et converger vers une forme de diversification – volontaire pour certains et latente pour d'autres - des cas d'usages possibles grâce au protocole Bitcoin, sans pour autant délaisser sa finalité première, d'abord

[1541] Consultez en temps réel ces inscriptions ancrées sur la blockchain Bitcoin, en principe aussi longtemps qu'elle existera, via le site internet suivant. Un autre protocole aux finalités similaires est né quelques mois suivant Ordinals, il s'agit de « *Bitcoin Stamp* », dont le fonctionnement demeure plus coûteux mais plus fiable et résilient pour ancrer des informations au sein des blocs Bitcoin.

[1542] Pour illustrer en temps réel la note de bas de page précédente, voici un exemple d'*inscription* sur *Ordinals* et un exemple de *stamp* sur *Bitcoin Stamps*.

monétaire. Bitcoin deviendrait ainsi, à terme, une infrastructure numérique universelle permettant à tous types d'acteurs d'y ancrer immuablement des jeux de données plus ou moins complexes et toujours aussi immuables et valorisables. Ainsi, Bitcoin conserve actuellement sa pertinence dans au moins deux domaines, à savoir le secteur financier et celui de la preuve de jeux de données. Le cas d'utilisation de la preuve de données peut être appliqué à de nombreux secteurs, mais cela nécessite de se conformer aux règles de droit en vigueur, une recherche de conformité juridique qui n'est pas – et ne sera probablement pas - une priorité pour les développeurs de la blockchain Bitcoin qui cherchent avant tout à assurer sa résilience et sa décentralisation informatique et sociale.

Focus 5 : Le pseudo-anonymat comme gage de résilience pour Bitcoin

A l'origine, accéder au réseau Bitcoin ne nécessitait pas la création d'un compte auprès d'un service en ligne spécialisé (comme aujourd'hui)[1543], mais simplement le téléchargement d'un logiciel spécifique (portefeuille numérique)[1544] puis l'achat de bitcoins auprès d'une personne physique ou morale qui en possédait. L'anonymat était ainsi fondamental au lancement de Bitcoin, c'est-à-dire une norme technique et communautaire par conception. Concrètement, une adresse bitcoin correspond mathématiquement à une clé publique unique et ressemble à ceci « *bc1qq2zpjy6qs7cxm25779wutw8w9450hzxfmdwsw7* »[1545]. Chaque fraction de bitcoins appartient cryptographiquement à la personne qui en possède la clé privée associée, lui permettant ainsi de signer (d'envoyer) des transactions avec celle-ci. Par l'intermédiaire de son portefeuille virtuel compatible avec Bitcoin, chaque personne peut générer et posséder plusieurs adresses de ce type, chacune avec son propre solde. Cela rend plus ou moins difficile de savoir quel utilisateur possède quel montant en bitcoins, selon les efforts déployés par celui-ci pour ne pas être identifié à posteriori via l'utilisation de ses adresses. Avec le fonctionnement ingénieux et fiable de ces adresses et signatures cryptographiques, le pseudo-anonymat par conception de l'identité numérique (crypto)financière des utilisateurs de bitcoins pourrait demeurer encore quelques années au sein de cet écosystème. Néanmoins, depuis environ 2017, les règlementations internationales obligent une identification préalable à l'achat ou vente de bitcoins par des personnes physiques, et parfois un enregistrement spécifique pour les personnes morales opérant dans ce secteur (ce qui sera probablement la norme d'ici quelques années), comme cela a été étudié dans cette recherche (*v.* également l'Annexe 14). En définitive, le pseudo-anonymat inhérent au fonctionnement de Bitcoin s'érode d'année en année face aux normes et aux régulations strictes de LCB-FT. Force est de constater que cette lutte ne se fonde pas toujours sur une compréhension

[1543] Initialement (avant 2012), aucune adresse électronique, aucun nom d'utilisateur ou encore mot de passe n'était nécessaire pour détenir ou dépenser des bitcoins. Avec l'essor de son adoption et utilisation, une majorité des utilisateurs acquièrent des crypto-actifs via des plateformes d'échanges de crypto-actifs, aujourd'hui toutes soumises à une identification systématique conformément au droit bancaire et financier. Cette tendance se renforce d'année en année au sein d'une majorité des juridictions internationales.

[1544] Download Bitcoin. 2022. Bitcoin.org, *v. supra*, II, Titre 1, 1.3.1.3

[1545] Chaque adresse bitcoin est publiquement visible sur une interface visuelle directement reliée à cette blockchain pour permettant une meilleure lecture de ses informations (adressses, transactions, solde actuel). Pour visualiser cette adresse, consultez le lien suivant

raisonnable et proportionnée des risques qu'elle fait courir à la majorité des utilisateurs honnête de bitcoins, mais plutôt sur une volonté de sur-identification qui contribuerait à progressivement altérer la perception de la valeur des bitcoins en les discriminant, comme déjà supposé au cours de cette thèse[1546].

Focus 6 : Bitcoin en tant que bien commun capitalistique et social universel

Le protocole Bitcoin est un outil qui favorise la liberté en ligne des individus en leur permettant de communiquer, de s'exprimer et d'entreprendre librement. La Cour Suprême américaine a ainsi confirmé que le mécanisme de la « *Preuve de travail* – PoW », présenté dans l'Annexe 6, est protégé par le droit fondamental à la liberté d'expression, en vertu du Premier Amendement de la Constitution des États-Unis[1547]. Cette reconnaissance souligne l'importance de la liberté d'expression dans le monde numérique et renforce la reconnaissance juridique et sociale accordée aux blockchains publiques en tant que garantes cryptographiques de cette liberté. La contribution sociale du système Bitcoin – permettant une nouvelle forme de bancarisation 3.0 - est considérable et permet progressivement depuis 2010 l'achat de biens et de services en ligne[1548]. A terme, il pourrait également offrir la possibilité de créer des identités numériques décentralisées pour accéder à divers services en ligne tels que des réseaux sociaux 3.0, des assurances 3.0, des crédits 3.0, et progressivement instaurer sa comptabilité à triple entrée à ces services. La blockchain Bitcoin offre une protection inédite aux utilisateurs honnêtes contre la censure et les manipulations numériques, bien qu'elle permette(ra) toujours à une minorité malhonnête d'effectuer des actions illégales (un problème qui ne peut être résolu ou évité par aucune technologie existante). Bitcoin a donc, en réalité, un impact principalement positif sur la société, en facilitant les transactions en ligne, en protégeant les droits des internautes et en offrant des opportunités pour l'innovation des secteurs clés que sont les services économiques et financiers.

En outre, Bitcoin est un protocole informatique apolitique, socialement agnostique et qui contribue à « *dépolitiser la monnaie* »[1549] pour ne pas dire à questionner ses fondements mêmes. Par son ouverture absolue, il introduit pour la première fois, grâce à son système économique ingénieux couplé à sa décentralisation informatique, la notion de rareté numérique sur Internet. Il s'agit de le percevoir comme un outil d'émancipation au service de certains droits fondamentaux des personnes comme le droit au respect de la vie privée, à l'intégrité numérique et même à l'auto-détermination informationnelle mentionné dans cette recherche. Grâce à son utilité, à sa neutralité, à sa sécurité cryptographique et à sa communauté croissante qui semble incoercible, Bitcoin semble être une (r)évolution qui traversera le temps, c'est-à-dire un système qui n'a besoin que de temps pour que la majorité des internautes prennent conscience de sa proposition de valeur numérique et sociale sans pareil (par rapport aux autres crypto-

[1546] V. *supra*, I, Titre 2, 2.5
[1547] DANIEL Aaron, « New York's Proof-of-Work ban violates Bitcoin miners' right to free speech », in *Bitcoin* Magazine, disponible en ligne, traduction libre de l'anglais « La jurisprudence de la Cour suprême montre que le moratoire de New York sur le minage de la preuves de travail viole les droits du premier amendement des mineurs de bitcoins ».
[1548] HOWELL James, « What Is Bitcoin Pizza Day ? », 2023, in *101 Blockchains*, disponible à l'adresse suivante
[1549] De MOMBYNES Yorick, Conférence à Surfin' Bitcoin, 2022, « Dépolitiser la monnaie », YouTube. Consulté à l'adresse suivante

actifs). Nul doute que dans les prochaines décennies et à la condition que certaines règlementations ne contreviennent pas à son utilisation (interdiction totale, identification systématique et disproportionnée de tous les détenteurs de bitcoins), Bitcoin sera probablement perçu à terme comme une infrastructure informatique favorisant l'émancipation individuelle des personnes, en réponse à certains maux d'une société ultra connectée, déjà sujette à une surveillance constante des internautes.

En résumé :

Fort de ces propos, il est possible de suggérer un condensé en trois temps de ce que le protocole Bitcoin représente en 2023, de ce qu'il ne sera probablement pas d'ici 2025, et enfin de ce qu'il pourrait être dans un temps plus long, c'est-à-dire après 2025. Ces postulats et conjectures se fondent sur les idées développées dans cette recherche et finalement mises en évidence de façon synthétique dans ce tableau :

<table>
<tr><th><u>Ce qu'est Bitcoin</u>
Constats depuis 2020
(Objectivité élevée)</th><th><u>Ce que ne sera pas Bitcoin</u>
Constats jusqu'à 2025
(Objectivité relative)</th><th><u>Ce que pourrait devenir Bitcoin</u>
Conjectures après 2025
(Objectivité faible)</th></tr>
<tr><td>La monnaie d'Internet :
Reconnaissance sociétale majoritaire</td><td>Une infrastructure numérique conforme aux textes de droit étudiés :
Reconnaissance sociétale majoritaire</td><td>Une monnaie légalement et mondialement reconnue :
Probabilité relative</td></tr>
<tr><td>Une monnaie légalement et mondialement reconnue :
Reconnaissance sociétale minoritaire</td><td>Un actif privilégié pour le financement d'activités illicites (blanchiment, terrorisme) :
Reconnaissance sociétale minoritaire</td><td>Un protocole multimodal monétaire, financier, de stockage et de tokenisation d'actifs :
Probabilité importante</td></tr>
<tr><td>Un bien commun numérique résilient et immuable :
Reconnaissance sociétale majoritaire</td><td rowspan="2">Un système informatique souple et malléable aux changements de son environnement socio-économique :
Reconnaissance sociétale majoritaire</td><td>Un registre et socle informatique ouvert et de confiance pour des INAS :
Probabilité relative</td></tr>
<tr><td>Un actif financier légalement et mondialement reconnu :
Reconnaissance sociétale majoritaire</td><td>Une infrastructure numérique favorisant la transition énergétique[1550] :
Probabilité relative</td></tr>
</table>

[1550] V. Annexe 6, Focus 1.

Légende :
Reconnaissance sociétale minoritaire = succès dépendant d'une reconnaissance individuelle par une minorité d'internautes et de citoyens, mais sans reconnaissance collective des secteurs publics et privés.
Reconnaissance sociétale majoritaire = succès dépendant d'une reconnaissance individuelle et collective majoritaire par les internautes/citoyens ainsi que par le secteur public et privé.
Probabilité relative = succès dépendant d'une reconnaissance individuelle et collective partielle et inégale par les internautes/citoyens ainsi que par la puissance publique.
Probabilité importante = succès dépendant d'une reconnaissance individuelle par les internautes/citoyens, couplées d'une reconnaissance collective par la puissance publique.

Annexe 4 : L'utopie d'un État blockchain autoproclamé (Liberland)

Comme précédemment évoqué, les défenseurs des technologies blockchains tendent initialement à ne faire confiance qu'à la programmation et aux mathématiques grâce aux algorithmes et à la cryptographie. Cette volonté de désintermédiation concerne tous les tiers de confiance, y compris les Etats. Les technologies blockchains permettent d'imaginer des relations sociales et économiques supposées totalement désintermédiées (« décentralisées »), par exemple avec une nation utilisant toutes les nouvelles technologies de rupture à sa disposition. Ce rêve communautaire a ainsi été imaginé par des techno-libertariens et mis en œuvre via un projet grandeur nature désormais accessible à tous en quelques clics : le « *Liberland* ». La République libre du Liberland est une île d'une surface de 7 km² situés sur la rive occidentale du Danube, entre la Croatie et la Serbie, partageant une frontière terrestre avec la première et une frontière fluviale avec la seconde. Le Liberland a été (auto)proclamé le 13 avril 2015 par son Président Vít Jedlička. Si la Croatie ne reconnaît pas le territoire du Liberland comme étant le sien, elle déclare paradoxalement qu'il n'est la terre de personne (« *terra nullius* »)[1551]. Cela implique qu'il devrait appartenir soit à la Serbie soit à la Croatie, qui s'en écarte en considérant ce territoire comme une frontière pour des raisons historiques et politiques. Cet Etat auto-proclamé développe depuis huit ans un cadre juridique comportant une Constitution[1552] ainsi que des lois[1553], toutes d'inspiration libertarienne[1554]. Soulignons que cette Constitution programmée grâce à une blockchain - supposément ouvertes - ne possède à ce jour qu'une reconnaissance juridique aux yeux des citoyens de ce territoire qui n'est pas officiellement reconnu au regard du droit international public. Cette nouvelle composante informatique que représente une blockchain (v. ci-après) donne ici naissance à un Etat dématérialisé, supposé décentralisé, dans l'attente de l'appropriation d'un territoire non revendiqué mais qu'il réclame. Ce nouveau mouvement mené par des technophiles et des libertariens vise à instaurer une démocratie directe en utilisant la technologie blockchain pour ses élections représentatives. Le but est de garantir une transparence absolue dans le processus électoral, en permettant aux électeurs de voter directement grâce à une blockchain supposée publique mais en réalité étatique (donc il s'agit d'une blockchain hybride), permettant d'assurer la vérifiabilité des résultats. En outre, un parlement est élu pour travailler en collaboration avec ce dispositif de démocratie directe. Sur le site officiel du Liberland, il est indiqué en 2022 que plus de 500 000 personnes attendent la citoyenneté et qu'un millier d'entre elles ont déjà la citoyenneté du Liberland. Seulement 17 000 citoyens du Liberland pourraient un jour peut être devenir physiquement résidents sur les 4 km² disponibles de ce territoire[1555]. Le Liberland produit déjà ses titres

[1551] Ce terme fait référence à un « *territoire sans maître* ». Il s'agit d'un terme utilisé en droit international public pour décrire un espace qui peut être habité mais qui n'appartient pas à un État, ce qui signifie que la terre n'est la propriété de personne. Selon certains juristes ce principe peut être utilisé pour justifier la revendication selon laquelle un territoire peut être acquis par l'occupation de celui-ci par un État.
[1552] Liberland. 2022. « The Constitution of the Free Republic of Liberland ». liberland.org
[1553] Liberland. 2022. « The Articles of the Provisional Government of the Free Republic of Liberland ». liberland.org
[1554] Sa Constitution et ses lois s'inspirent de la tradition du libéralisme classique, mettant fortement l'accent sur le droit de propriété et les libertés individuelles
[1555] BINSKY Drew, « The Country That Doesn't Yet Exist (Liberland) », 2022, YouTube

d'identité (cartes d'identité et passeports), non reconnus à l'international, au seul profit de ses e-résident et citoyens (v. ci-après). A terme, le Liberland fournirait à chaque citoyen une citoyenneté symbolisée sous la forme d'un ou plusieurs jetons numériques directement accessibles dans leur portefeuille de crypto-actifs, c'est-à-dire grâce à un NFT de citoyenneté[1556]. Pour cela, l'utilisation des « *Soul Bound Token* »[1557] semble une piste privilégiée en 2023. Cette tokenisation de l'identité numérique des citoyens du Liberland (proche de l'INAS étudiée) ne semble toutefois pas tendre vers une conformité avec le RGPD ni le Règlement eIDAS, ce qui suscite également des questions quant à la conformité de cette micro-nation autoproclamée face à d'autres Règlements ou amendements en cours d'adoption (MiCA, TFR, Data Act). Le budget de cet État semble minimal, avec seulement quatre ministères et une justice qui pourrait d'ailleurs être décentralisée grâce au protocole Kleros.

En 2015[1558], le Liberland avait annoncé l'adoption officielle du Bitcoin comme monnaie nationale[1559], faisant de lui le premier État (auto-proclamé) au monde à prendre une telle décision. Cette initiative a donc été mise en place avant le Salvador[1560] qui a adopté le Bitcoin comme monnaie légale en 2021. Cependant, en mars 2019[1561], le Liberland a lancé sa propre crypto-monnaie, le « *Liberland Merit - LLM* », qui a d'abord été consacré sur la blockchain publique « *Bitcoin Cash* »[1562], puis finalement abandonnée en 2020[1563]. À la suite de cet échec, le Liberland a décidé d'adopter une nouvelle infrastructure blockchain, nommée « *Polkadot* »[1564], qui est inspirée et liée à la blockchain publique Ethereum[1565]. Cette infrastructure prend en charge les contrats intelligents et vise à créer une incitation économique similaire à celle de la blockchain publique Bitcoin, notamment en instituant une supposée rareté programmée des jetons en circulation sur ce réseau. En réalité, ce processus de rareté artificielle devenant éventuellement pure dans un temps long semble impossible à atteindre[1566], ce que seul Bitcoin a réussi jusqu'à aujourd'hui. En réalité, il semble que le Liberland balbutie depuis plusieurs années

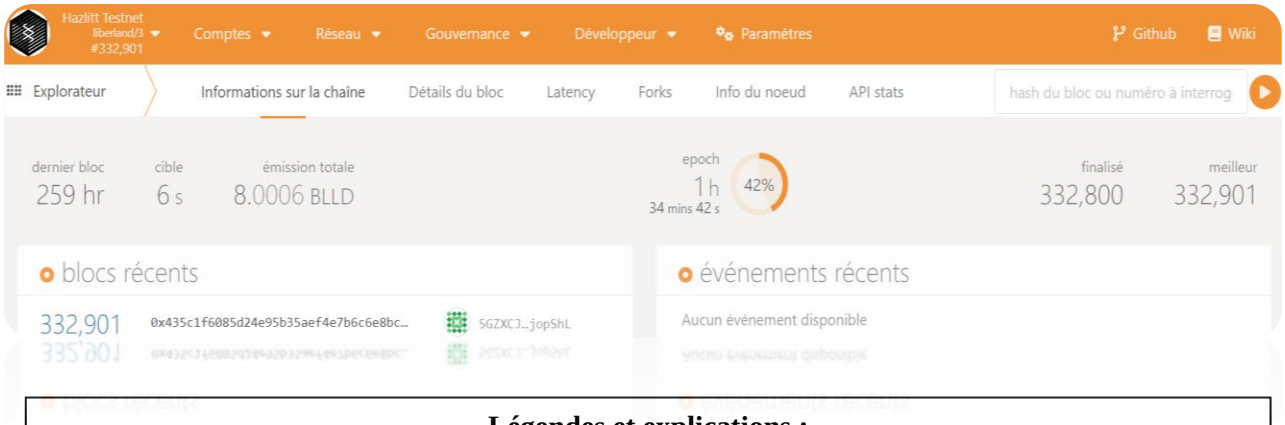
[1556] Le jeton de citoyenneté contiendra : une photo de l'identifiant de citoyenneté, un lien vers le compte Liberland du propriétaire (*v.* compte expérimental d'un e-resident), le nombre de *Liberland Merits (LLM)* mis en jeu dans la citoyenneté et l'historique de ce jeton de citoyenneté particulier, in *docs/Blockchain Strategy.md at master* · liberland/docs. GitHub
[1557] V. *supra*, I, Titre 1, 2.3.1.1
[1558] NewsBTC, « Liberland Chooses Bitcoin as National Currency », 2015, disponible en ligne
[1559] Soit sept années avant le Salvador tout en sachant que le Liberland n'est pas reconnu comme un pays officiel à ce jour, contrairement au Salvador.
[1560] V. Annexe 5.
[1561] DIXON Brent, « Liberland's Merit Token Built on Bitcoin Cash », 2021, disponible à l'adresse suivante
[1562] Il s'agit en quelque sorte d'une copie (« *Fork* ») de la blockchain Bitcoin originelle. Cette blockchain copiée est aujourd'hui peu reconnue et adoptée par la communauté Bitcoin originelle.
[1563] « En 2020, nous avons décidé de transférer notre concept de gouvernance électronique par blockchain de la technologie EOS.IO à notre propre écosystème Polkadot qui sera lancé au quatrième trimestre 2021 », in *The free republic of Liberland ministry of finance*, 2021, Liberland, p.3, disponible à l'adresse suivante
[1564] *Polkadot* est un protocole de communication ainsi qu'une plateforme dite « *multi-chain* » c'est-à-dire permettant de faire communiquer en théorie tous types de blockchains (et leurs applications) ensemble. Disponible en ligne
[1565] Il est possible d'observer l'historique des transactions de cette blockchain via l'adresse suivante (lien visité le 02/01/2023)
[1566] Pour rappel, il est souligné que ces mécanismes algorithmiques et matériels qui ont pour objet et effet de générer une raréfaction numérique sont à l'origine artificiels dans le sens où ils sont programmés et souhaités (contrairement à la disponibilité de l'or par exemple). Toutefois, cette raréfaction devient progressivement *pure* et non plus *artificielle*, car les personnes à l'origine de ces mécanismes n'en possèdent plus le contrôle et ne peuvent plus exercer d'influence sur ces concepts qui tournent ainsi au service de tout le réseau et par conséquent du bien commun.

concernant sa stratégie de déploiement relative à sa blockchain et à son jeton numérique[1567], pourtant essentiels à son modèle de gouvernance numérique 3.0 qui est supposé résilient et décentralisé. En effet, tant concernant sa DAO gouvernementale que concernant son jeton LLM et plus généralement sa blockchain officielle (v. ci-après la « *Liberland Smart Chain - LSC* »), il apparaît que sa stratégie numérique demeure encore floue et ambigüe, en dépit des progrès annoncés. Début 2023, la blockchain déployée par le Liberland souffre d'un manque apparent de développement informatique et commercial comme en témoigne la seconde capture d'écran qui suit. Fin 2021, le Liberland avait également annoncé développer son propre Métavers, le « *Liberland Metaverse* »[1568], aux fins de renforcer sa présence en ligne et surtout d'attirer de nouveaux capitaux étrangers. D'ici fin 2023, l'ambition de cet e-Etat autoproclamé est de déployer progressivement ces multiples composantes techniques au service de ses e-résident et citoyens. A cet égard, il est possible que le Liberland s'empare du sujet de l'INAS afin de proposer à ses citoyens de se connecter à ses services en ligne, à l'instar de la gestion de sa société qu'il est possible d'enregistrer au Liberland[1569]. Si cette hypothèse n'est à ce jour qu'une fiction, un tel évènement confèrerait au Liberland une place de chef de file en matière d'utilisation massive des technologies 3.0. Toutefois, l'utilisation théorique de ces technologies 3.0 serait à comparer à leurs utilisations effectives qui pourraient rapidement mener à des désillusions, voire à des dérives. Pour illustration, chaque e-resident n'a pas un droit de vote égal au Liberland, mais seulement le pouvoir de voter en fonction du montant investi dans le Liberland, créant ainsi un système ultra-capitalistique potentiellement source de conflits sociaux ultérieurs.

Finalement, si le Liberland représente peut-être en 2023 une utopie politique de citoyens désabusés par leur nationalité d'origine, force est de constater que son développement progressif sur le plan social et informatique fait de cette expérimentation un projet inédit à l'ère d'une dématérialisation quasi totale des interactions sociales et administratives. Si le Liberland représente un écosystème particulièrement enclin à tendre vers l'avènement d'une identité universelle et doit à ce titre être suivi avec attention, il demeure en réalité un écosystème juridiquement et politiquement fermé et circonscrit à ses citoyens, contrairement au protocole de Proof of Humanity[1570]. Selon un article académique publié en 2016 dans le Chicago Journal of International Law, la reconnaissance juridique internationale du Liberland dépend[1571] strictement de sa reconnaissance par un nombre suffisant d'États, qui se reconnaissent par

[1567] Le Liberland est à la recherche de développeurs, une ressource aujourd'hui très prisée que le Liberland semble avoir du mal à attirer au regard des avancées parsemées de son développement informatique accessible publiquement sur son compte Github. *Call for Developers*. 13 janvier 2022, liberland.org
[1568] « World Liberland Metaverse ». Pour plus d'informations, consultez l'adresse suivante
[1569] Tous les *e-résident* ont accès à une plateforme officielle du Liberland permettant de proposer des produits et services comme l'enregistrement d'une société au Liberland. Consultable à l'adresse suivante
[1570] V. *supra*, I, Titre 2, 2.9
[1571] Traduction libre de l'anglais, « [...] il existe deux voies potentielles par lesquelles le Liberland pourrait obtenir une reconnaissance. Premièrement, le Liberland pourrait convaincre la communauté internationale que le territoire qu'il revendique est terra nullius en raison des renonciations informelles de la Serbie et de la Croatie à leurs titres de propriété sur ce territoire. Le Liberland devrait alors satisfaire aux critères de Montevideo. Toutefois, le Liberland ne pourrait pas satisfaire à une application stricte des critères de Montevideo, car il ne dispose pas d'une population résidente permanente, d'un gouvernement

ailleurs entre eux. Même si le Liberland obtenait une reconnaissance juridique partielle, il serait tout de même contraint de se conformer à de multiples règlementations avant de pouvoir établir des relations avec des pays respectant les règles internationales. Cette contrainte pourrait ainsi entraver les ambitions libertariennes du Liberland, dont le territoire physique lui demeure inaccessible depuis presque 10 ans. En l'absence d'une reconnaissance internationale par des pays développés à l'avenir, il est fort probable que le Liberland se concentre sur des relations commerciales avec des pays en voie de développement[1572] dans l'espoir de bâtir des relations internationales alternatives suffisamment solides pour démontrer que son utopie n'était pas qu'un simple rêve. Dans un avenir proche, peut-être d'ici une ou deux décennies, le monde assistera soit à la plus grande arnaque et tentative de création d'un nouveau pays, soit à l'émergence d'un nouvel État 3.0 forgé de toutes pièces par des individus partageant des aspirations sociales communes et des idéaux variés.



Légendes et explications :

Les deux photos précédentes, représentant un scan d'une carte d'e-resident du Liberland puis une capture d'écran de la blockchain du Liberland (LLC) au 02/01/2023. Combinées, elles permettent de se faire une idée du développement et du lien qui existerait entre les titres d'identité revendiqués par le Liberland et sa blockchain supposée publique, décentralisée et incensurable. L'intégration d'une puce électronique dans ces titres permettrait dans un avenir relativement proche d'effectuer des actes immuables reconnus par la Constitution et les lois du Liberland.

opérationnel à l'intérieur de ses frontières et, sans doute, de la capacité de nouer des relations avec d'autres États. […] la communauté internationale a considéré avec beaucoup de scepticisme la revendication du Liberland en tant qu'État. Il est peu probable que la communauté internationale choisisse d'appliquer la version la moins stricte des critères de Montevideo et permette au Liberland d'obtenir la reconnaissance qu'il recherche ». ROSSMAN, Gabriel, 2016, « Extremely Loud and Incredibly Close (But Still So Far): Assessing Liberland's Claim of Statehood », in *Chicago Journal of International Law*: Vol. 17: No. 1, Article 10. Disponible en ligne

[1572] En février 2023, le Liberland a ouvert son premier bureau (ambassade) à l'international, au Mexique. Pour plus d'informations consultez le lien suivant, « Grand Opening of the Liberland Office in Mexico City ».

Annexe 5 : Reconnaissance et adoption du bitcoin comme monnaie légale au Salvador

En 2021, le Salvador est devenu le premier pays au monde à reconnaître le bitcoin comme une monnaie ayant cours légal, via l'adoption de la loi Bitcoin (« *Ley Bitcoin* ») par le Parlement salvadorien le 9 juin 2021[1573]. Le Président du Salvador, Nayib Bukele, avait annoncé cette volonté le 6 juin 2021, créant ainsi un précédent pour l'univers des crypto-actifs et surtout pour l'écosystème de la blockchain Bitcoin. Cette loi confère au bitcoin un statut officiel dans tout ce pays, qui compte près de 7 millions d'habitants[1574]. Il convient de noter que si le Liberland a adopté le bitcoin dès 2015, il ne s'agit pas d'un État reconnu sur le plan international, ce qui ne lui confère donc que de façon relative la place de premier État à légaliser le bitcoin en comparaison au Salvador[1575]. La loi du 9 juin oblige les acteurs économiques salvadoriens à accepter cette monnaie virtuelle comme moyen de paiement pour leurs transactions courantes, ce qui marque un tournant important pour la facette monétaire de cet actif. C'est la première fois qu'un État de droit reconnaît officiellement le statut de monnaie et de devise au bitcoin, lui reconnaissant pour la première fois un cours légal[1576]. Le gouvernement est donc tenu de fournir les ressources informatiques nécessaires pour mettre en œuvre cette loi, mais les infrastructures techniques limitées et la volatilité du cours du bitcoin suscitent autant d'enthousiasme que de préoccupations chez certains acteurs économiques locaux, citoyens et institutions financières internationales. Dans les pays développés, les citoyens ont accès à une monnaie fiable et stable. Ce constat ne s'applique pas à la majorité des pays dans le monde, car les pays en voie de développement représentent environ 85% de la population mondiale[1577]. En effet, la majorité de ces pays en développement n'ont pas la chance d'avoir un système bancaire et financier aussi développé, stable et fiable que ceux des pays occidentaux. Cela signifie que les populations confrontées à un manque de bancarisation ont tendance à percevoir le bitcoin comme une solution plus viable que leur monnaie officielle, dont la confiance ne peut souvent pas être assurée en raison de régimes politiques et/ou de systèmes monétaires instables. Ainsi, le bitcoin répond tout particulièrement à certains besoins bancaires et financiers pour ces pays[1578], ce qui est le cas du Salvador qui soutient fermement cet actif numérique. Afin d'éviter les confusions courantes autour de la valeur attribuée aux bitcoins, cette étude distingue deux de ses caractéristiques principales : la capacité du bitcoin à servir de réserve de valeur, déjà reconnue en raison de son adoption et de son prix à la hausse depuis plus de 14 ans, et de sa fonction de valeur refuge, qui est pertinente dans les périodes

[1573] « Ley Bitcoin | Asamblea Legislativa de El Salvador », 9 juin 2021, disponible à l'adresse suivante
[1574] HETZNER Christiaan, 14 mars 2022, « El Salvador's millennial president launching Bitcoin 'volcano bond' in major bet on cryptocurrency craze », disponible à l'adresse suivante
[1575] D'ANCONIA Frisco, 16 novembre 2016, « Free Republic of Liberland Values Bitcoin, But Ready to Move on to Dash », disponible à l'adresse suivante
[1576] LAURANT Dominique, avocat au Barreau de Paris, 21 octobre 2021, « Puisque le bitcoin est la monnaie du Salvador, il faut en tirer les conséquences fiscales en France », « Manifestement, depuis le 7 septembre 2021, le bitcoin est la monnaie légale du Salvador. Il a donc le statut juridique d'une monnaie au Salvador, comme le franc suisse en Suisse, ou le rouble en Russie. On voit mal comment dire que le bitcoin n'aurait pas 'le statut juridique d'une monnaie'. Depuis cette date, ce n'est donc plus un actif numérique au sens de l'article L 54-10-1 du CMF, et il n'est donc plus concerné par les dispositions fiscales de l'article 150 VH bis du CGI », disponible à l'adresse suivante
[1577] Consultez le site donnéesmondiales.com pour observer la liste des 152 pays en voie de développement.
[1578] Toutefois, pour que les pays en question puissent utiliser le bitcoin comme monnaie alternative à grande échelle, il est essentiel qu'ils aient une couverture Internet adéquate permettant des transactions en masse.

de crise telles que sur les marchés financiers ou encore en période de tensions géopolitiques internationales (Ukraine, etc.). Pour nuancer, le bitcoin semble depuis quelques années seulement bénéficier du statut de valeur refuge, un statut que l'or a acquis au fil des millénaires.

L'objectif politique assumé du Salvador est de s'affranchir du système monétaire et financier traditionnel en adoptant une technologie au potentiel à ce jour sous-estimé par certaines institutions occidentales (FMI)[1579]. Pour atteindre cet objectif, il s'agit de bancariser un maximum sa population en lui offrant un accès simplifié et industriel à des portefeuilles numériques (compatible au L1 et L2 de Bitcoin), celui du gouvernement salvadorien se nommant « *Chivo* »[1580]. Grâce à plusieurs communautés qui forment progressivement la population sur le terrain, bitcoin est ainsi devenu un moyen de paiement largement adopté par une partie de la population pauvre du pays[1581]. Cette adoption du bitcoin par le Salvador relève d'une logique économique spécifique : obtenir un moyen d'échanges peu coûteux, fiable et rapide, permettant de renforcer l'inclusion financière et la croissance économique du pays. A l'instar d'une monnaie numérique nationale créée de toute pièce comme l'euro cryptographique[1582], le Salvador a plutôt décidé de profiter directement des qualités du réseau Bitcoin pour ses différents atouts, tels que son effet de réseau, son immuabilité et son accessibilité déjà étudiés. Il faut également souligner que les projets de l'énigmatique et controversé Président du Salvador (v. ci-après) ne se limitent pas à cette reconnaissance juridique et financière du bitcoin. En effet, ce dernier compte faire de son pays une « *Bitcoin-nation* » avant-gardiste en proposant notamment l'offre d'obligations d'Etat en bitcoins (« *volcano bonds* »)[1583], pour une valeur d'un milliard de dollars. Le produit de cette émission d'obligations à destination d'investisseurs du monde entier soutiendra la construction d'infrastructures publiques comme le développement d'une exploitation minière de bitcoins *directement* alimentée par les volcans du pays (géothermique), ou encore pour construire une « *Bitcoin city* »[1584] au pied du volcan Conchagua.

Cependant, il semble en pratique que l'adoption du bitcoin en tant que monnaie soit paradoxalement associée à une utilisation généralisée du Dollar. En effet, les fournisseurs de portefeuilles numériques qui permettent aux citoyens d'échanger des bitcoins dépendent d'un accès partiel ou total à des comptes et des systèmes libellés en Dollars (des sociétés américaines spécialisées sur bitcoin proposant désormais

[1579] FMI, « IMF executive board concludes 2021 article IV consultation with El Salvador », in *Press release n°22/13,* 2022, traduction libre de l'anglais « Ils [Le Conseil d'administration du FMI] ont insisté sur la nécessité d'une réglementation et d'une surveillance stricte du nouvel écosystème de Chivo et de Bitcoin. Ils ont insisté sur le fait que l'utilisation de Bitcoin présente des risques importants pour la stabilité financière, l'intégrité financière et la protection des consommateurs, ainsi que pour le passif fiscal éventuel associé. Ils ont exhorté les autorités à réduire le champ d'application de la loi sur le bitcoin en supprimant le statut de monnaie légale du bitcoin. Certains administrateurs ont également exprimé leur inquiétude quant aux risques liés à l'émission d'obligations adossées à des bitcoins », disponible à l'adresse suivante
[1580] Pour plus d'informations, consultez Shivowallet.com, 2021.
[1581] Cinq millions de Salvadoriens auraient adopté le bitcoin comme moyen de paiement selon le Président du Salvador Nayib Bukele, 3 mai 2022, « The World's Coolest Dictator » [Vidéo], 1,52 sur 13,38 minutes, *Découvre Bitcoin*. 24 novembre 2021, « L'adoption du Bitcoin au Salvador (Débrief à chaud) » [Vidéo]. YouTube.
[1582] V. *supra*, II, Titre 2, 2.4.
[1583] R, Rémy. (2023b, janvier 23). « Volcano bonds de Bitcoin : Le Salvador adopte la loi sur l'émission de crypto-actifs ». Journal du Coin. Disponible à l'adresse suivante
[1584] BUKELE Nayib, Président du Salvador, 10 mai 2022, « Bitcoin City is coming », [Tweet]

leurs au Salvador). Cette interdépendance est ainsi nécessaire aux agents économiques pour promouvoir et utiliser des bitcoins, ce qui peut, paradoxalement, limiter son statut en tant que monnaie cryptographique. Il convient également de souligner que si le Président actuel du Salvador a été élu démocratiquement, il semble exister un sérieux risque de dérive politique vers une dictature dans les prochaines années[1585]. Cela pourrait amener les opposants à Bitcoin à invoquer le poncif selon lequel un État dictatorial utiliserait le réseau Bitcoin pour renforcer son pouvoir ou même pour blanchir des fonds publics, ce qui serait catastrophique pour l'image de ce réseau informatique qui est en réalité factuellement apolitique depuis 14 ans. En fin de compte, le Salvador et le Liberland sont tous deux des exemples d'expérimentations sociales, économiques, monétaires et informatiques inédites, qui ont des effets juridiques et politiques incertains. Bien que certains considèrent ces expériences comme utopiques, il est important de ne pas tomber dans l'illusion de penser que construire une société entièrement 3.0, c'est-à-dire exclusivement bâtie sur des crypto-actifs, serait viable. La réalité sera probablement plus nuancée et il y aura certainement une coexistence ou une fusion entre les systèmes conventionnels bien établis 1.0 et 2.0, avec ceux de troisième génération (3.0), voire de dernières générations (4.0 ou 5.0). Bien que l'initiative du Salvador soit perçue comme une menace et un risque par les acteurs du système traditionnel[1586], elle représente un formidable laboratoire d'innovation sociale pour les technophiles et mérite pour cette raison d'être soutenue. Les choix structurels qui y seront faits seront scrutés de près par le monde entier dans les années à venir.

[1585] ARTE. 21 mars 2023, « Salvador : vivre sous Bukele » | *ARTE Reportage* [Vidéo]. YouTube
[1586] MAIRE Vincent, 12 février 2023, « Salvador : le FMI se méfie toujours du Bitcoin, mais semble adoucir légèrement son discours ». *Cryptoast*. Disponible à l'adresse suivante

Annexe 6 : Focus et analyse des mécanismes et consensus blockchains

La notion de consensus

Le terme de consensus provient du latin « *consentio* » qui signifie une adhésion et une unanimité à propos de quelque chose. Aujourd'hui, obtenir un consensus signifie l'obtention d'une entente et d'un accord direct ou latent entre plusieurs personnes. Au sein d'une technologie blockchain et de ses multiples composantes, le consensus fait référence aux méthodes algorithmiques et organisationnelles grâce auxquelles une blockchain et ses acteurs conviennent de la validité de son historique, c'est-à-dire de la validité et de l'ordre de ses blocs de transactions. Parfois désigné par le terme de « *mécanisme de consensus* », un tel algorithme représente concrètement la gouvernance ou la méthode avec laquelle une blockchain parvient à un consensus, c'est-à-dire à faire communiquer des machines de façon harmonisée par rapport à des règles et à des informations communiquées en ligne. Concrètement, son objectif est d'assurer la fiabilité des enregistrements et des copies des blocs que synchronise chacun de ses nœuds.

Focus 1 : La résilience et la stabilité de la Preuve de travail (*Proof of Work - PoW*) comme justification face à sa consommation électrique

En complément des informations soutenues dans l'Annexe 6 (Focus 1), la Preuve de travail (« *Proof of Work - PoW* ») est un système utilisé par certaines blockchains publiques pour garantir la validité et la sécurité des transactions, Bitcoin lui ayant donné naissance[1587]. En sciences de l'informatique appliquée à la technologie blockchain, une attaque Sybil est une attaque informatique au cours de laquelle un acteur manœuvre de nombreux nœuds qui prétendent être des nœuds honnêtes (en réalité malveillants) afin d'inciter d'autres nœuds du réseau identifiés comme honnêtes à accepter des données invalides ou fausses. Une telle attaque vise donc à contraindre le comportement de nœuds honnêtes en les trompant, en les corrompant. A cet égard, l'invention de l'algorithme de consensus de Nakamoto par la preuve de travail, en hommage à son créateur, a entre autres été spécifiquement conçue pour empêcher les attaques Sybil à destination d'un réseau pair à pair (P2P) et décentralisé. Effectivement, la Preuve de travail (PoW) permet de résister aux attaques Sybil en censurant l'acteur qui essaie de démultiplier son identité afin de prendre le contrôle du réseau. Le PoW représente depuis plus de 14 ans le mécanisme le plus éprouvé en tant que source de vérité pour les blocs d'une blockchain publique comme Bitcoin. Aux débuts de Bitcoin, Satoshi Nakamoto souhaitait que tout participant puisse ajouter un bloc à la suite des blocs précédents. Toutefois, choisir un utilisateur au hasard revient à ouvrir le réseau à des individus pouvant prétendre être plus nombreux qu'ils ne le sont réellement. C'est l'une des raisons pour lesquelles Bitcoin utilise ce mécanisme de la Preuve de travail : chaque bloc validé est issu d'un travail unique et théoriquement impossible à reproduire ou falsifier dans un temps court. La PoW est un mécanisme de consensus dans lequel chaque bloc est « *miné* » par un groupe d'individus qui possèdent des machines

[1587] En réalité, le concept de *preuve de travail* a d'abord été imaginé et proposé dans un article en 1993 par les informaticiens Moni Naor et Cynthia Dwork puis développé et formellement nommé comme tel en 1997 dans un article publié par Adam Back et enfin cité plus tard dans le *White Paper* de Bitcoin en 2009.

de travail dédiées au réseau. Elle permet donc de sécuriser le réseau Bitcoin[1588] tandis que tous les nœuds du réseau vérifient cette Preuve de travail dans un second temps, comme évoqué dans l'Annexe 3.

En d'autres termes, certains ordinateurs dont l'usage est désormais exclusivement dédié à la blockchain Bitcoin intègrent des puces spécifiques de type ASIC (« *Application-specific integrated circuit* »)[1589]. Un ASIC est ici un dispositif informatisé qui utilise des microcircuits dans le seul but d'extraire des bitcoins de son protocole (un processus nommé le « *minage* » ou « *mining* » en anglais). Ces machines, ci-après désignées par le terme « ASIC » permettent d'assembler un puzzle de transactions continues qui est ensuite automatiquement vérifié par d'autres ordinateurs conventionnels (des nœuds qui font fonctionner le logiciel Bitcoin Core[1590]). Ces derniers (nœuds) vérifient ensuite simplement l'exactitude de ce puzzle cryptographique. Ce mécanisme de fonctionnement rend la blockchain Bitcoin extrêmement sûre et résiliente à toute tentative de corruption de ses blocs. Concrètement, la PoW demande à des utilisateurs volontaires et rémunérés (« *miners* ») de démontrer de manière objective et quantifiable qu'ils ont dépensé de l'énergie, éliminant ainsi ceux dont la dépense d'énergie et le travail ne respecteraient pas certaines conditions définies en amont par les développeurs de la communauté Bitcoin. Par conséquent, le coût d'une attaque Sybil est possible mais prohibitif sur ce réseau (v. tableau suivant). Un mineur malveillant, pour réussir son attaque, doit consommer une quantité d'énergie très importante afin de produire des blocs pour tenter de priver la chaîne de blocs de ses transactions légitimes. Lorsqu'un mineur malveillant tente une attaque en produisant des blocs invalides, ce dernier consomme de l'électricité inutilement et doit en payer le coût et prix correspondant. En résumé, grâce au PoW, les attaques Sybil ne peuvent pas tromper un nœud Bitcoin en lui faisant accepter une fausse copie de l'historique des blocs précédents. En effet, ce nœud n'a besoin que d'une connexion à un nœud honnête pour résister à cette attaque, puisque le consensus de Bitcoin est basé sur le principe de la preuve de travail la plus importante qui a été réalisé sur la chaîne, permettant ainsi de garantir qu'il s'agit de la copie légitime de la blockchain escomptée.

Sur le plan strictement informatique, lors du processus de *minage*[1591], une machine de type ASIC reçoit via les protocoles conventionnels d'Internet (TCP/IP) un problème et un calcul mathématique à résoudre. Une fois ce défi mathématique reçu, l'ASIC le résout localement grâce à sa puissance de

[1588] GRUNSPAN Cyril, PEREZ-MARCO Ricardo, « double spend races », traduit librement de l'anglais, « Le protocole de consensus et la sécurité du réseau Bitcoin reposent sur le processus de minage des bitcoins et de validation des transactions », in *arxiv.org*, 2022, disponible à l'adresse suivante, p.5.
[1589] Il s'agit d'un type de micropuce spécialement conçu pour exécuter une seule tâche ou un petit ensemble de tâches (calculs). Les ASIC sont souvent utilisés lorsqu'un dispositif et une machine doit exécuter une fonction particulière avec un haut niveau d'efficacité ou de rapidité. Ces circuits sont généralement conçus pour réaliser une tâche à la fois, mais très rapidement, et par conséquent, ils sont souvent plus efficaces dans l'exécution de leur tâche désignée qu'un microprocesseur conventionnel dont l'usage est général, c'est-à-dire multitâches. Les ASIC sont plus coûteux à produire que les microprocesseurs conventionnels.
[1590] *Op. cit.* Début 2023, plus de 43 000 nœuds Bitcoin sont recensés et estimés par Global Bitcoin Nodes (un chiffre qui dépasse de loin le nombre de nœud des autres blockchains) - in *Bitnodes*. Consultez en temps réel ces statistiques en ligne, *v.* également le téléchargement du logiciel *Bitcoin Core* permettant de 'devenir' un *nœud Bitcoin* via son ordinateur conventionnel, disponible à l'adresse suivante
[1591] Consultez la capture d'écran ainsi que les explications ci-après. Source issue de la vidéo suivante ainsi que d'un entretien avec Guillaume Girard, Bitcoin expert chez Galaxy Digital Mining le 14 octobre 2021. V. également, « Blockheader Research-Rachel Rybarczyk » [Vidéo] disponible sur YouTube

calcul[1592] puis le diffuse en P2P via une connexion internet pouvant être minime. Une fois diffusé, il soumet à confirmation sa solution aux autres ASIC puis nœuds du réseau qui l'audit, c'est-à-dire vérifient que cette preuve de travail résolue est correcte. Une fois une unanimité atteinte à 51% au regard du calcul et d'autres informations nécessaires[1593], un bloc de transactions contenant cette preuve de travail est rattaché à ladite chaîne. Par conséquent, même si un attaquant dépasse 51% du de la *puissance de calcul* du réseau (« *puissance minière* » ou « *hashrate* »), il ne peut pas modifier l'historique de la blockchain Bitcoin sans dépenser à nouveau au moins la même quantité d'énergie que celle utilisée pour le créer. Cela est presque impossible en pratique en raison du nombre important - et de la dispersion géographique - de ces ASIC, estimé au nombre de 2,9 millions en août 2022[1594]. Fin 2022, un attaquant – un Etat(s), une entreprise(s) - nécessiterait environ 1,5 millions d'ASIC pour s'attaquer à Bitcoin de façon effective. Sur le plan financier, cela couterait environ 260 000 dollars par heure d'attaque pour corrompre le réseau[1595], une attaque informatique qui ferait ainsi paradoxalement perdre à son attaquant les milliards de dollars d'ASIC mis en jeux. Il est donc pratiquement impossible d'allouer les ASIC et l'énergie afférente nécessaires tout en exploitant un ou plusieurs sites de minage industriel de cette taille et capacité[1596]. Cela semble encore moins probable que la communauté bitcoin s'en appercevrait et pourrait réagir en conséquence. Il devient de plus en plus difficile de l'attaquer au fil du temps, car si une entité avait voulu s'attaquer au Bitcoin, il aurait dû le faire il y a dix ans. En conclusion, non seulement il serait impossible de réaliser une attaque à 51% sur le réseau Bitcoin en raison de la quantité massive d'ASIC et de l'énergie nécessaire, mais, même si un acteur en était capable, il y aurait une forte dissuasion financière à le faire.

Par ailleurs, il s'agit de comprendre comment fonctionne une transaction en bitcoins sur la blockchain Bitcoin (L1) et son réseau natif[1597] : lorsqu'un utilisateur effectue une demande de transaction en BTC, elle est tout d'abord envoyée sur une liste d'attente nommée la « *Mempool* »[1598]. La taille de chaque bloc

[1592] Ces machines sont conçues et spécifiquement optimisées pour ce processus de minage et peuvent tester plusieurs centaines de milliards de combinaisons par seconde pour essayer de trouver une clé gagnante (un *hash* commençant par une suite de « 0 » et nommé un « *nonce* », v. l'illustration ci-après) et sa récompense associée. Ce fonctionnement implique ainsi que plus une personne possède de machines de type ASIC, plus il est capable de trouver ces combinaisons et donc augmente sa rémunération totale en bitcoins.

[1593] Voir sur la capture d'écran qui suit les deux cadres verts qui représentent en couleur les informations (« *version, Query chain* », etc.) contenues dans chaque *hash* unique issu d'un bloc précédent.

[1594] VICE News, « The Future of Bitcoin Mining and the Environment », 2022 [Vidéo] YouTube

[1595] MITCHELL, « En supposant un prix modeste de 6¢/kWh, pour une consommation de 3,05 kW des XP, chaque machine coûterait 0,183 $ par heure de fonctionnement (1 411 347 * 0,18 $ ~= 260 000 $ par heure d'attaque. Par ailleurs, l'atttaquant pourrait miner (6 blocs par heure * 6,25 BTC par bloc * 51%) ~19,125 BTC par heure, ce qui équivaut à ~573 750 $. », 2023, disponible en ligne sur Twitter.

[1596] Faire fonctionner 1,5 millions d'ASIC qui consomment chacun autant d'énergie que 5 réfrigérateurs est une tâche redoutable et aujourd'hui impossible.

[1597] Satoshi Nakamoto explique le fonctionnement de Bitcoin en ces termes (traduction libre de l'anglais) : « Les étapes pour faire fonctionner le réseau sont les suivantes : 1. Les nouvelles transactions sont diffusées à tous les nœuds. 2. Chaque nœud rassemble les nouvelles transactions dans un bloc. 3. Chaque nœud s'efforce de trouver une preuve de travail difficile pour son bloc. 4. Quand un nœud trouve une preuve de travail, il diffuse le bloc à tous les nœuds. 5. Les nœuds n'acceptent le bloc que si toutes les transactions qu'il contient sont valides et n'ont pas déjà été dépensées. 6. Les nœuds expriment leur acceptation du bloc en travaillant à la création du bloc suivant dans la chaîne, en utilisant le hachage du bloc accepté comme hachage précédent. », *op. cit*. Bitcoin Whitepaper, p. 3.

[1598] Consultez en temps réel les blocs de transactions en cours de validation à l'adresse suivante

étant limitée à environ 2000 transactions par blocs, cela implique que chaque ASIC va essayer de valider les transactions qui lui rapporteront les frais les plus élevés. Ce mécanisme similaire à une enchère numérique permet aux utilisateurs de positionner leurs transactions de façon plus ou moins favorable dans cette Mempool : plus un utilisateur choisit des frais importants pour faire valider sa transaction par un *miner*, plus il a de chance que sa transaction soit sélectionnée pour faire partie du prochain bloc. Une fois qu'un mineur a trouvé un *hash* gagnant (ci-après « *nonce* » dans l'illustration), et si aucune triche n'est repérée par les nœuds du réseau, alors la transaction est quasi-instantanément et sans effort informatique inclue dans un bloc. Le *miner* est récompensé par 6,25 bitcoins[1599] plus les frais de chacune des transactions incluses dans ce bloc. Cette logique et ces processus se répètent inlassablement et sans interruption toutes les 10 minutes depuis 14 ans, ce qui vaut à Bitcoin l'appellation de « *Timechain* » en référence à sa fiabilité presque horlogère.

En résumé, l'activité de *minage* sécurise la blockchain Bitcoin grâce au tirage au sort d'un mineur qui génèrera le prochain bloc. Ce tirage au sort ne peut pas être truqué, car pour y participer chaque mineur dépense obligatoirement de l'énergie électrique pour tenter de gagner la mise associée. Ensuite, dans un second temps relativement court, les blocs sont validés et vérifiés par les nœuds du réseau (une activité qui ne nécessite pas comme la loterie précédente de dépenser beaucoup d'électricité, puisque les mineurs ont déjà procédé au tirage au sort validé entre eux). Il peut être conclu que le mécanisme de PoW est fiable, résilient, stable et confère aux blockchains ouvertes qui l'utilisent une protection optimale en termes de résilience, car reposant d'après plusieurs études sur la thermodynamique[1600], la théorie de

[1599] En 2008, la récompense par bloc était de *50 bitcoins toutes les dix minutes* ; elle a été automatiquement *divisée par deux* le 28 novembre 2012 (*25 bitcoins* émis toutes les dix minutes) ; puis à nouveau par deux le 9 juillet 2016 (*12,5 bitcoins*) et encore une fois le 11 mai 2020 (*6,25 bitcoins*). En mai 2024, cette même récompense de *6,25 bitcoins* émis toutes les dix minutes évoluera automatiquement à *~3,12 bitcoins* émis toutes les dix minutes.
[1600] « Définition de thermodynamique », 2022, in *cnrtl.fr*, disponible à l'adresse suivante

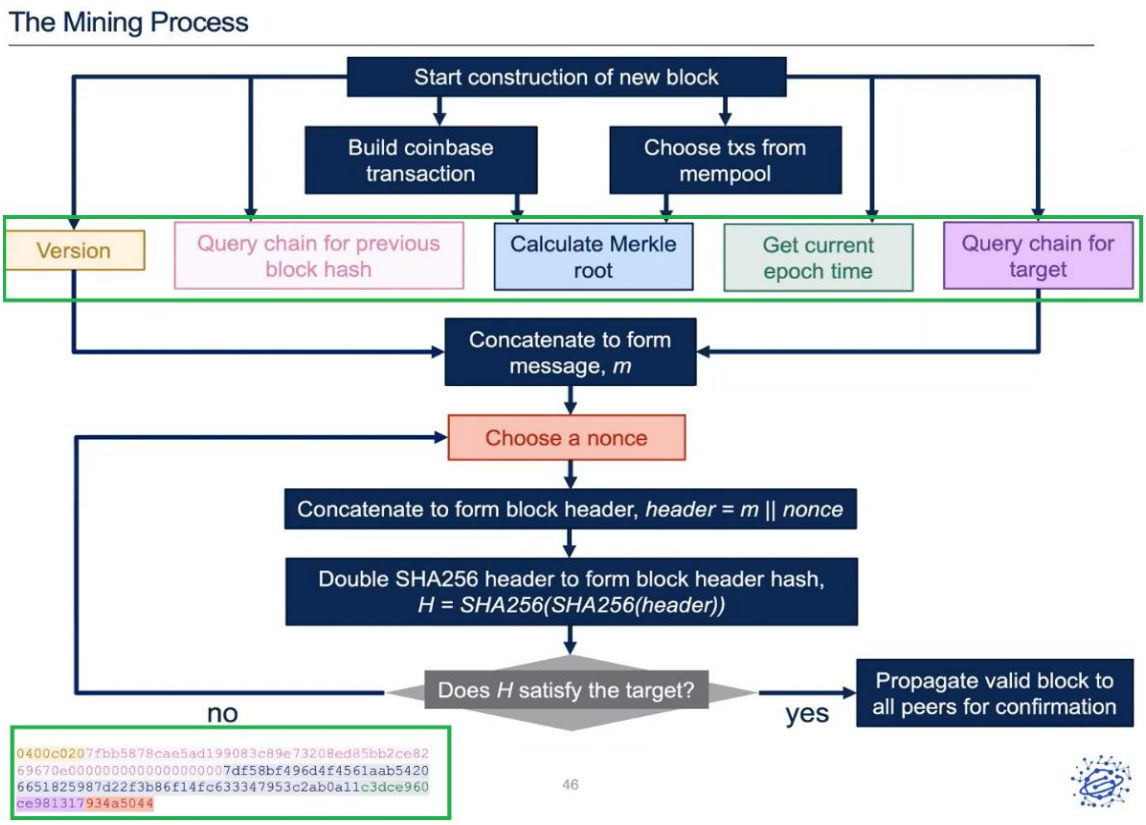
l'information[1601], la théorie des jeux[1602] et la théorie de l'évolution de Darwin[1603]. Finalement, ce mécanisme de consensus informatique inédit est parfois désigné comme s'inscrivant dans un mouvement de « *SoftWar* »[1604], en référence à une révolution logicielle et sociale pacifique. Le schéma suivant illustre l'agencement et le fonctionnement cryptographique et logiciel qui composent une partie du processus de la Preuve de travail que réalisent les ASIC. Pour le comprendre dans sa forme la plus simplifiée, il convient tout d'abord d'observer que les deux cadres verts. Ils correspondent aux mêmes séquences d'informations combinées et formant un *hash unique* ou « *nonce* » (second cadre vert en bas à gauche).

[1601] « La théorie des communications s'intéresse aux moyens de transmettre une information depuis une source jusqu'à un utilisateur. », BELHADJ Besma, « Introduction à la théorie de l'information », 2011, p.1, disponible en ligne

[1602] Terme issu de l'anglais « Game theory ». Le protocole Bitcoin répond au « Problème des généraux byzantins », en anglais « Byzantine General's Problem », qui est une mécanique en théorie des jeux. Il s'agit d'une problématique théorisée en 1982 par Leslie Lamport, Robert Shostak et Marshall Pease et appliquée au domaine de l'informatique distribuée. Elle énonce la difficulté à laquelle font face des généraux - dont certains peuvent être des traîtres - qui doivent parvenir à un accord commun sur la question de savoir s'il faut attaquer une ville ou battre en retraite, mais qui ne peuvent communiquer qu'en envoyant des messagers. La problématique est de trouver une stratégie commune permettant de s'assurer que les généraux loyaux arrivent à se mettre d'accord sur un plan de bataille malgré la trahison de certains traîtres qui battront en retraite pour faire échouer l'attaque. Cette problématique est systématiquement résolue (l'attaque sera un succès) dès lors que les traitres sont minoritaires et restreints. L'objet de cette catachrèse imagée permet de répondre à certaines difficultés pour des ordinateurs distribués de communiquer ensemble (grâce à des algorithmes) tout en sachant que certains de leurs pairs (ordinateurs) sont défectueux, voire malicieux. En d'autres termes, ce défi de synchronisation prend tout son sens lorsqu'il est appliqué à des réseaux P2P de nœuds souhaitant se mettre d'accord sur le contenu d'un registre électronique : Bitcoin se base sur un réseau de participants qui entretiennent chacun le registre des transactions réalisées (l'enjeu est de se mettre d'accord sur qui possède quoi de manière décentralisée, sans reposer sur une autorité centrale). A l'instar des algorithmes traditionnels, « l'algorithme de Nakamoto » novateur utilisé par Bitcoin permet à un très grand nombre d'ordinateurs de participer au registre de transactions de manière totalement ouverte, décentralisée, et sans que son fonctionnement en souffre. Finalement, le protocole Bitcoin répond informatiquement pour la première fois au « Problème des généraux byzantins », c'est-à-dire à cette problématique de confiance numérique, sans reposer sur un tiers de confiance centralisateur et tout en conservant le pseudo-anonymat de ses participants.

[1603] Traduction libre de l'anglais, « Dans cet article, certaines similitudes entre les crypto-monnaies et les systèmes biologiques ont été mises en évidence. [...] L'analogie entre la théorie de Darwin et la cryptofinance évolutive peut être élaborée. Une crypto-monnaie gagnante attire des capitaux en raison d'un ratio de Sharpe supérieur et d'autres caractéristiques attrayantes du protocole. Il ne s'agit pas d'un problème statique mais dynamique, car les promoteurs tentent d'obtenir un avantage en guidant le prix de l'actif et en améliorant le protocole », BERNHARD K. Meister, C.W. PRICE Henry, « Darwin Among the Cryptocurrencies », Department of Physics & Centre for Complexity Science, Imperial College London, disponible en ligne

[1604] SCHRECKINGER Ben, « Space Force major to Pentagon: Mine Bitcoin ! », in *Politico*, 2023, disponible à l'adresse suivante



Source : RYBARCZYK Rachel, in Galaxy Digital Mining, « Blockheader Research », 2022, YouTube

Sur la blockchain Bitcoin, chaque bloc se compose d'un « *header* » et d'un « *body* », ce dernier étant lui-même constitué de multiples transactions. Pour avoir un bloc valide, un *miner* (ASIC) doit *hacher* ces informations via l'algorithme SHA-256 afin de produire un nouveau *hash* commençant par un certain nombre de « 0 » (ici par exemple cinq zéros « 00000e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77 »).

Ce nombre plus ou moins important de 0 représente la *difficulté de minage*. Celle-ci est une mesure statistique du nombre de *hash* qui doivent être générés pour trouver la solution valide permettant de résoudre le prochain bloc. Un ajustement périodique de cette *difficulté du réseau* permet de maintenir l'émission des blocs à une moyenne d'environ 10 minutes entre chacun d'entre eux, ce qui explique in fine pourquoi un utilisateur doit attendre au moins ~10 minutes pour qu'une transaction bitcoin soit validée dans un bloc.

Cette difficulté est déterminée par le nombre de 0 qui doivent figurer en tête du *hash* de sortie du travail réalisé par un *miner*. Plus il y a de 0 dans le *hash* de sortie, plus la difficulté est élevée et inversement, moins il y a de 0, plus il est facile pour un *miner* de trouver c'est-à-dire de calculer cette solution. Au fil du temps cette *difficulté du réseau* augmente et implique d'optimiser sans cesse les *miners* pour assurer leur rentabilité.

Puisque pour rappel chaque *hash* est unique et lié à une donnée d'entrée, la partie du bloc qu'un mineur modifie pendant le processus de minage/hachage précité se nomme le « *nonce* » en rouge sur la capture d'écran ci-dessus. Il s'agit d'une suite exclusive et à usage unique de chiffres et de « *bits* » utilisés dans un ensemble d'opérations cryptographiques). Ainsi, modifier cette donnée d'entrée, même légèrement, change radicalement la sortie hachée de l'ensemble des données. Le travail d'un mineur est ainsi de saisir un *nonce*, de le *hacher*, puis de vérifier son travail et ce jusqu'à trouver le *nonce gagnant* (un *nonce aléatoire*, mais spécifique, qui permet de valider ledit bloc grâce au travail dudit mineur).

En d'autres termes, les mineurs devinent rapidement et de manière aléatoire ce que doit être ce *nonce*. Ils le *hachent* via l'algorithme SHA-256 jusqu'à ce qu'ils obtiennent une sortie avec suffisamment de 0 pour satisfaire la difficulté toujours changeante du réseau (soit le nombre de 0 nécessaire à trouver qui fluctue). Finalement, il est possible de vérifier cela vous-même sur le site internet mempool.space : cliquez sur le numéro d'un bloc récent puis comptez le nombre de 0 qui précèdent son *hash*. C'est ainsi que tout le réseau ou tout tiers peut savoir qu'il s'agit d'un bloc valide, car ce *hash* répond à la difficulté du réseau à l'instant de sa validation.

Après avoir discuté des principaux fondements de Bitcoin en termes de fonctionnement global, il est important d'aborder un aspect crucial de cette technologie et de son avenir : sa consommation énergétique. A cet égard, il convient de faire une distinction essentielle entre la consommation énergétique et la consommation électrique. La notion de consommation énergétique est bien plus large que celle de consommation d'électricité qui ne représente qu'un segment du marché mondial de l'énergie. Par conséquent, il est trompeur de parler de la consommation énergétique du réseau Bitcoin et il semblerait plus juste de parler de sa consommation électrique, à moins que le terme « énergétique » précédent ne soit également utilisé pour inclure les déchets matériels et électroniques comme la durée de vie des nœuds et des ASIC fonctionnant sur ce réseau (ce qui complexifierait les estimations scientifiques étudiées dans le tableau qui suit). Il est important de noter qu'une analyse de l'industrie du minage basée uniquement sur la consommation électrique brute serait trop étroite, car cette industrie entraîne des répercussions significatives sur le secteur de l'énergie dans son ensemble (positives et négatives). En effet, l'utilisation de la Preuve de travail est particulièrement critiquée pour sa nature énergivore, mais il est également important de considérer certains avantages irréfutables qu'elle apporte au réseau énergétique mondial. Pour illustrer cela, le tableau suivant relate et constate deux argumentaires opposés concernant les impacts de la Preuve de travail sur l'environnement et par conséquent sur la société. Il est remarqué à juste titre que l'ancien député Pierre Person a souligné la complexité de cette industrie et mis en garde certains acteurs institutionnels contre une analyse trop simpliste de ce sujet en réalité éminemment stratégique pour le Web 3.0[1605].

[1605] *Op. cit.,* « Monnaies, banques et finance : vers une nouvelle ère crypto. Un enjeu de souveraineté et de compétitivité économique, financière et monétaire », « (…) décrire l'industrie du minage à l'aune de sa seule consommation électrique brute serait faire preuve de myopie au regard de la complexité d'une industrie qui implique des incidences non négligeables sur le secteur de l'énergie », p.70.

Arguments CONTRE la Preuve de travail	Arguments POUR la Preuve de travail
N°1 : D'après certaines études et de multiples articles plus ou moins scientifiques, Bitcoin consomme de l'énergie avec excès (l'équivalent de plusieurs pays réunis)[1606], soit environ 0,6% de l'énergie mondiale produite[1607]. Une étude de 2022 compare ce chiffre au 0,2% qui est consommé par le système de paiement conventionnel mondial et aggloméré[1608]. Dès 2017, le Forum économique mondial (WEF) estime que Bitcoin consommerait plus d'énergie que le monde entier dès 2020[1609]. En janvier 2022, une autre étude estime que la blockchain Bitcoin a été responsable d'environ 19 000 décès en raison de son impact énergétique[1610]. En mai 2022, la Banque de France publie et estime dans une revue économique dédiée à la blockchain que « *la consommation énergétique d'une seule transaction en Bitcoin équivaut à celle de 834000 transactions par carte bancaire* […] *certains protocoles comme Ethereum prévoient d'abandonner la preuve de travail au profit notamment de la preuve d'enjeu*	**N°1' :** Il convient tout d'abord de souligner que toute action entreprise par les êtres humains requiert de l'énergie, et qu'une société en croissance est nécessairement une société qui consomme de l'énergie. La tolérance de la société vis-à-vis de la pollution engendrée par cette consommation d'énergie est directement proportionnelle à l'utilité et à la nécessité sociale de l'activité en question. Autrement dit, les conséquences environnementales d'une technologie sont plus facilement acceptées si les bénéfices qu'elle apporte sont considérés comme nécessaires par la société[1612]**.** La compréhension des bénéfices présents et futurs de Bitcoin[1613] et plus largement de son rôle dans la société est encore limitée et sous-estimée par une grande partie des agents économiques en raison de sa relative jeunesse. L'assertion selon laquelle Bitcoin consommerait toutes les ressources mondiales en 2020, avancées par le forum économique mondial (WEF), est fausse et témoigne d'une méconnaissance ou d'une désinformation délibérée, comme en témoigne une vidéo publiée sur le compte Twitter du WEF en 2022[1614]. En ce qui concerne l'étude qui relie le fonctionnement de

[1606] HUANG, J. O'NEILL, C. & TABUCHI, H, « Bitcoin Uses More Electricity Than Many Countries. How Is That Possible? », 2022, in *The New York Times*, disponible à l'adresse suivante

[1607] AGUR I. DEODORO J. LAVAYSSIERE X. MARTINEZ PERIA S. et al,, « Digital Currencies and Energy Consumptions », 2022, in *Fintech Notes*, « Au 25 avril 2022, la consommation électrique annuelle du réseau Bitcoin est estimée à 144 térawattheures (TWh) par an selon l'indice de consommation électrique de Cambridge Bitcoin. Cela représente environ 0,6 % de la consommation électrique mondiale totale », p.9.

[1608] *Ibid.* « Globalement, en regroupant ces estimations fondées sur les parties du système de paiement pour lesquelles des données sur la consommation d'énergie sont disponibles, on obtient une estimation de 47,3 TWh de consommation annuelle d'énergie par le système de paiement mondial. Cela représente environ 0,2 % de la consommation mondiale totale d'électricité. », p.27.

[1609] JEZARD Adam, « In 2020 Bitcoin will consume more power than the world does today », 2017, in *World Economic Forum (WEF)*, consulté le 28 avril 2022, à l'adresse suivante

[1610] TRUBY Jon, DEAN BROWN Rafael, et al., « Blockchain, climate damage, and death: Policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and Bitcoin », Energy Research & Social Science, Volume 88, 2022, disponible en ligne, traduit de l'anglais « […] de nombreux types populaires de blockchain ont résisté à la pression visant à réduire leur impact sur l'environnement, notamment le bitcoin, dont les émissions annuelles attribuées à 2021 produiront des émissions responsables d'environ 19 000 décès futurs. ».

[1612] Par exemple, l'aviation ou encore le nucléaire sont socialement justifiés (à l'instar de Bitcoin et sans laisser une chance à cette technologie de rupture), *v.* Parlement européen, « Le Parlement a rejeté la proposition s'opposant à l'inclusion des activités nucléaires et gazières à la liste des activités durables sur le plan environnemental », 2022, « Taxonomie : le Parlement ne s'oppose pas à l'inclusion des activités gazières et nucléaires », disponible en ligne

[1613] Pour rappel, il est fait référence aux bénéfices de Bitcoin listés ici : transactions sans frontières, rapides, actif bénéficiant d'une valeur refuge, favorisant la liberté financière, d'entreprendre, de communiquer, la résilience informatique ou encore l'indépendance et numérique et politique.

[1614] WEF, « A change in the way bitcoin is coded could almost eliminate its environmental impact », Twitter, consulté le 28 avril 2022, à l'adresse suivante

(« proof of stake ») à 99,95% moins énergivore »[1611].	Bitcoin à 19 000 décès, notre observation montre que ce type de raisonnement scientifique est décontextualisé et perd de son intérêt, nuisant ainsi à une compréhension objective des enjeux liés à ce nouveau paradigme informatique. Selon la revue de la Banque de France mentionnée qui déclare qu'une transaction bitcoin est équivalente à 834 000 transactions par carte bancaire, il apparait que cette assertion ne peut pas être vérifiée ni considérée comme valable selon les sciences de l'informatique, car elle ne possède pas de source vérifiable. De même, le chiffre avancé en faveur de la « *Preuve d'enjeux* », qui serait moins énergivore que la Preuve de travail, repose sur une assertion purement théorique au jour de la publication de cette revue. Il semble que ces chiffres et conclusions soient motivés par une volonté de communication stratégique et politique plutôt que par une exactitude et une neutralité scientifique. Cette prise de position est encore largement répandue par certains acteurs institutionnels du secteur pour freiner la compréhension et l'adoption du bitcoin par le grand public. Pour illustrer ces propos, Greenpeace, une organisation internationale qui se bat pour la protection de l'environnement, a récemment lancé une campagne aux Etats-Unis pour s'opposer au minage de bitcoins[1615]. L'artiste et le militant Benjamin Von Wong était chargé par Greenpeace de créer une œuvre d'art pour inciter l'opinion public à modifier le mécanisme de consensus de Bitcoin, depuis le PoW vers le PoS. Après avoir réalisé cette œuvre puis communiqué en ligne sur son travail, l'artiste a réalisé que cette campagne anti-Bitcoin n'était pas justifiée. Il a donc publiquement admis son erreur et a changé d'opinion sur le sujet, en soutenant maintenant le potentiel du réseau Bitcoin au service de la transition énergétique[1616].

[1611] V. Focus 2 de la présente Annexe, *v.* également « ABC l'éco en bref, la blockchain », Banque de France et EDUCFI, p.3, accessible en ligne à l'adresse suivante

[1615] CANTON Ben, « 'Changez le code, pas le climat' Greenpeace lance un nouvel assaut contre Bitcoin », 30 mars 2023, in *Journal du Coin*, disponible à l'adresse suivante

[1616] Traduction libre de l'anglais, « Le #SkullofSatoshi est un accident phénoménal. Il représente littéralement ce que les deux parties croient être vrai : que Bitcoin a le potentiel d'être plus respectueux de l'environnement ; une force positive pour l'environnement. », « Le SkullofSatoshi est un accident phénoménal », le 25 mars 2023 sur Twitter.

	En juillet 2021, le « *Bitcoin Mining Council – BMC* »[1617] a mené une enquête auprès de plus de 32% du réseau Bitcoin mondial, dont les résultats ont révélé que près de 67% des mineurs utilisent de l'électricité (« *mix énergétique* »)[1618] provenant de sources durables. Sur cette base, et compte tenu de l'expansion du réseau, il est possible que le minage devienne l'une des industries les plus efficientes et durables au monde, comme l'a également souligné un rapport de l'Assemblée nationale en 2022[1619]. D'après le BMC, Bitcoin consumerait en réalité 0,17% de l'énergie mondiale produite à date de janvier 2023[1620]. En janvier 2023, un article publié dans la MIT Technology Review met en évidence certains avantages directs du minage de bitcoins au Congo, où le parc national de Virunga est devenu le premier parc national à exploiter une mine de bitcoin afin de protéger ses forêts et sa célèbre faune[1621].
N°2 : Bitcoin n'a qu'une utilité et une valeur sociale limitées, voire inexistantes, ce qui signifie qu'il ne trouve que peu ou pas d'utilisation au sein de notre société, excepté une spéculation financière.	**N°1' & 2' :** Les méthodes, base de calculs[1622] et comparaison utilisée pour dénoncer le supposé « *gaspillage d'énergie* » du réseau Bitcoin, sont progressivement démenties[1623] au fur et à mesure de la compréhension de son fonctionnement matériel et structurel, mais aussi logiciel. En d'autres termes, plus Bitcoin sera étudié et compris, plus son caractère énergivore sera nuancé, voire socialement justifié (voir ci-après).
N°3 : Bitcoin possède une valeur économique marginale ou nulle. Le système bancaire et financier conventionnel est plus efficace et	**N°1' & 3' & 4' :** D'après une étude publiée en avril 2022, pour réfuter l'affirmation selon laquelle « *les*

[1617] Bitcoin Mining Council, « Bitcoin Mining Council Survey Confirms Sustainable Power Mix (Q2 2021) ». bitcoinminingcouncil.com

[1618] Wikipedia contributors, « Mix énergétique », consulté le 1 avril 2022, à l'adresse suivante

[1619] « Si l'extraction de bitcoins consomme effectivement beaucoup d'énergie, électricité parfois carbonée, elle peut également être une activité particulièrement efficace pour financer la transition écologique. », *op. cit.* « Monnaies, banques et finance : vers une nouvelle ère crypto. Un enjeu de souveraineté et de compétitivité économique, financière et Monétaire », p.72.

[1620] Bitcoin Mining Council, « Bitcoin Mining Council Q4 2022 Briefing », [Vidéo]. YouTube.

[1621] POPESCU Adam, « Gorillas, militias, and Bitcoin: Why Congo's most famous national park is betting big on crypto », 2023, in *MIT Technology Review*, « Dans le but de protéger ses forêts et sa célèbre faune, Virunga est devenu le premier parc national à exploiter une mine de bitcoin. », article disponible à l'adresse suivante

[1622] Selon le blog *Digiconomist* (initialement utilisé comme source pour la proposition d'amendement et d'interdiction du minage de Bitcoin pour le règlement MiCA), dont les calculs de base issus de leur *Bitcoin Energy Consumption Index* sont scientifiquement faux et biaisés, le réseau Bitcoin consommerait l'équivalent de 42,6% de l'électricité produite en France en 2022. A propos de ces bases de calculs biaisées, cela s'explique par le fait (i) que les mineurs sont localisés par pays selon leurs adresse IP alors même que beaucoup utilisent des *VPN* (les données étant donc biaisées dès le départ), (ii) on applique le *bouquet/mixte énergétique* dudit pays en question aux mineurs (sans prendre en compte la consommation réelle, unique et effective de chaque installation des mineurs). « Bitcoin Energy Consumption Index - Digiconomist. », 2022, in *Digiconomist.* Disponible en ligne

[1623] STACHTCHENKO Alexandre, « […] la plupart de ces études à charge ne comprennent absolument pas le fonctionnement de Bitcoin ni ce qu'il remplace. », 2022, « Manuel de survie dans la jungle des poncifs anti-Bitcoin (version longue) », in *Medium*, consulté le 1 avril 2022 à l'adresse suivante

fiable que le système décentralisé proposé par Bitcoin. **N°4 :** Si le Bitcoin était largement adopté avec des millions d'utilisateurs supplémentaires, il fera face à des problèmes de bogues, de congestion de réseau et de frais élevés, ce qui démontre sa non-viabilité à long terme.	*cryptomonnaies ne valent rien* »[1624], il est pertinent de comparer les performances des systèmes de paiement traditionnels avec celles du protocole Bitcoin. Selon l'étude, une transaction en bitcoin est en moyenne 288 fois plus rapide qu'une transaction de paiement classique[1625], tandis que Bitcoin consomme 56 fois moins d'énergie que le système traditionnel[1626]. De plus, l'étude suggère que Bitcoin n'est pas pleinement exploité, car il est possible d'augmenter les volumes de transactions jusqu'à quatre fois sans augmenter sa consommation d'énergie, même sur son L1, sans même prendre en compte l'existence de L2 tel que le Lightning Network. Enfin, l'auteur de l'étude souligne que même au niveau d'une transaction unique, une transaction en PoW s'avère 1 à 5 fois plus efficace sur le plan énergétique[1627]. Il convient de noter que selon l'auteur, la marge d'erreur de l'étude est de 4 % et que les chiffres sous-estiment intentionnellement les résultats[1628]. **N°1' & 2' & 3' :** Pour être rentable, le modèle économique des mineurs de bitcoins repose sur la réduction des coûts électriques, tandis que les recettes en bitcoins doivent couvrir ces coûts[1629]. Toutefois, les fluctuations du prix du bitcoin sont incontrôlables pour les mineurs, qui doivent donc adapter leur comportement en conséquence. Les mineurs sont géographiquement mobiles et indépendants, car ils se déplacent d'un pays à l'autre[1630] pour trouver des sources d'énergie à faible coût, notamment des énergies renouvelables subventionnées[1631]. Ils peuvent le faire indépendamment des infrastructures et des

[1624] KARAYAN, Raphaële, « Les cryptomonnaies ne valent rien selon Christine Lagarde », 2022, in *usine-digitale.fr*, consulté le 9 juin 2022, à l'adresse suivante

[1625] KHAZZAKA Michel, « Bitcoin: Cryptopayments Energy Efficiency », 2022, p.1., disponible à l'adresse suivante, « Une transaction de paiement classique est en moyenne 288 fois plus lente qu'une transaction en bitcoin ».

[1626] Grand Angle Crypto, « Une guerre de communication ! » [Michel Khazzaka], 2022, [Vidéo]. YouTube, « Bitcoin consomme 56 fois moins d'énergie que le système classique ».

[1627] *Op. cit.*, « Bitcoin: Cryptopayments Energy Efficiency », 2022, p.1, disponible en ligne à l'adresse suivante, « Nous démontrons que (…) même au niveau d'une transaction unique, une transaction PoW s'avère 1 à 5 fois plus efficace sur le plan énergétique. ».

[1628] « Une guerre de communication ! » [Michel Khazzaka], 6 juillet 2022, [Vidéo], YouTube.

[1629] *Op. cit.*, « Monnaies, banques et finance : vers une nouvelle ère crypto Un enjeu de souveraineté et de compétitivité économique, financière et Monétaire », « les mineurs ont tendance à rechercher les prix d'électricité les plus bas. », p.70.

[1630] *Ibid.* « Les fermes de minage étant extrêmement mobiles, les mineurs pouvaient se permettre de déplacer leurs activités en fonction des coûts de l'énergie et donc de consommer davantage sans subir de hausse substantielle de leurs coûts de production. », p.69.

[1631] Centrale hydro-électrique, géothermique, énergie solaire ou éolienne, etc. Pour plus d'informations sur le minage de bitcoins issu de la géothermie, *v.* la vidéo suivante par Grand Angle Crypto, 2022, « Miner du Bitcoin au Salvador ? . . .soyons sérieux ! » [Vidéo]. YouTube.

	ressources existantes, car seules l'électricité et une connexion Internet minimale sont nécessaires pour miner des bitcoins. Actuellement, l'énergie à faible coût se trouve dans des zones isolées où la demande d'énergie est faible, telle que la Sibérie[1632], certains pays d'Afrique et le Kazakhstan[1633], où l'électricité produite est gaspillée faute d'utilisation. Les mineurs proposent donc d'utiliser cette énergie gaspillée pour soutenir une infrastructure financière universelle, indépendante et résiliente telle que Bitcoin. Depuis 2020, les initiatives de minage vert (« *green mining* ») se multiplient, telles que l'utilisation de certaines matières polluantes et gaspillées par l'industrie pétrolière aux États-Unis[1634] ou encore les déchets animaliers provenant de fermes en Irlande[1635]. **N°4' :** Le Lightning Network (L2) offre la possibilité de réaliser des transactions de faible montant sans nécessiter l'utilisation de la blockchain native de Bitcoin (L1)[1636], ce qui permet de réduire la congestion et les frais sur ce réseau L1 principal. Avec l'arrivée de nouveaux utilisateurs, il est envisageable de rediriger progressivement ces derniers vers le L2, spécialement conçu pour des paiements de faible valeur et optimisés. A cet égard, l'un des organes de la Réserve fédérale américaine (FED) a reconnu en 2022 que le Lightning Network est une avancée significative pour le bitcoin en tant que réseau de paiement crédible[1637], en raison de sa capacité à offrir une évolutivité et une efficacité bien supérieures à celles du système de paiement conventionnel (finance traditionnelle), et en étant

[1632] CHULAIN Aisling Ni, « How this Siberian data centre is attracting Bitcoin miners with cheap, 'green' power », 2021, Euronews, consulté le 1 avril 2022, à l'adresse suivante
[1633] ARNOULT Maxime, « Le Kazakhstan attire les producteurs de bitcoins du monde entier, voici pourquoi. », 2022, in *ouest-france*. Consulté le 1 avril 2022, à l'adresse suivante
[1634] Pour plus d'informations consultez la video suivante de Forbes Digital Assets, 20 décembre 2021, « Mining Bitcoin With Natural Gas For A Clean Crypto Future », in *Business of Climate Change Forbes*, [Vidéo]. YouTube.
[1635] Pour plus d'informations consultez la video suivante de Cointelegraph, 2023, « How Irish farmers are turning cow poop into digital gold (Bitcoin) ». YouTube.
[1636] AGUR I. DEODORO J. LAVAYSSIERE X. MARTINEZ PERIA S. et al, « Digital Currencies and Energy Consumptions », 2022, in *Fintech Notes*, « Effet de substitution : pour un niveau donné de la demande de transactions d'actifs, la couche 2 [Lightning Network] réduit la demande de transactions sur la chaîne [L1] en permettant davantage de transactions hors chaîne, ce qui réduit les frais de transaction (les frais de transaction dépendent de la demande de transactions) et l'incitation à miner, ce qui réduirait à son tour la consommation d'énergie. », p.12.
[1637] ZIMMERMAN Peter, DIVAKARUNI Anantha, « The Lightning Network : Turning Bitcoin into Money », « Nos résultats suggèrent que le Lightning Network peut aider Bitcoin à atteindre une plus grande évolutivité, lui permettant de mieux fonctionner en tant que système de paiement. D'après nos résultats, si le LN avait existé en 2017, la congestion [du réseau principal (L1) Bitcoin] aurait pu être inférieure de 93 %. », p.3, disponible à l'adresse suivante

	jusqu'à un million de fois plus économe en énergie par transaction que les paiements instantanés[1638].
N°5 : L'interdiction du minage par la Chine en 2021[1639] démontre non seulement que le mécanisme de PoW n'est économiquement et écologiquement pas soutenable à long terme, mais également que les monnaies numériques de banques centrales (MNBC) sont à privilégier à l'avenir.	**N°2' & 3' & 5' :** Le Lightning Network permet déjà certains mécanismes informatiques (autres que l'IND) qui permettent à ses utilisateurs de s'authentifier sur des services financiers en ligne[1640]. Ces nouvelles initiatives 3.0, bâties et reliées au LN, se multiplient et font écho et appel au concept d'INAS. Dès lors, comme le secteur bancaire qui a dû en partie développer ses propres mécanismes d'identification, l'écosystème de Bitcoin semble progressivement construire avec succès les siens. A cet égard et pour rappel, les mécanismes d'identification et d'authentification nécessaires à l'implémentation d'une MNBC sont donc également en cours de développement sur Bitcoin, mais avec d'autres normes informatiques 3.0. **N°5' :** L'interdiction du minage par la Chine a eu pour effet final la délocalisation de milliers d'ASIC aux États-Unis (Texas), au Canada ou encore au Kazakhstan. Ainsi, la majorité de ces machines fonctionnent à nouveau et sécurisent toujours le réseau Bitcoin, qui a atteint un record inédit de puissance de calcul quelques mois seulement après cette interdiction en Chine[1641]. Cette interdiction a pour objectif politique et économique de soutenir le lancement progressif du Yan numérique à travers toute la Chine. En France, certains chercheurs proposent également d'interdire le PoW au même titre que le pseudo-anonymat associé à ce système[1642], notamment pour promouvoir les

[1638] *Ibid.* « Bitcoin: Cryptopayments Energy Efficiency », p.1, disponible en ligne à l'adresse suivante, « Lorsque la couche Bitcoin Lightning est comparée au système [conventionnel] de paiement instantané, Bitcoin gagne de manière exponentielle en évolutivité et en efficacité, s'avérant jusqu'à un million de fois plus économe en énergie par transaction que les paiements instantanés. ».

[1639] La Chine a envisagé d'interdire l'extraction de bitcoins dès 2019, mais ce n'est qu'en 2021 que les autorités ont imposé de sévères restrictions aux acteurs de cette industrie. En 2021, l'interdiction du *minage* a finalement poussé les entreprises à quitter le pays et à se tourner vers des pays comme le Kazakhstan, qui ont une position plus favorable à cette industrie. Elles ont également trouvé refuge dans des villes aux États-Unis, où les entreprises rencontrent à la fois le soutien et les critiques de la population locale ou encore de politiciens. Pour comprendre comment la Chine se positionne depuis 2013 face aux crypto-actifs et notamment au Bitcoin, V. l'article suivant « All You Need to Know About China #39 ; s Crypto Ban. », 2022.

[1640] Il est par exemple fait référence au protocole de communication « *LNURL* » entre les portefeuilles Lightning et des applications externes ou services tiers. La société française *LNMarkets* utilise « *LNURL-auth* » pour la connexion : le portefeuille de l'utilisateur dérive une nouvelle paire de clés qui est liée aux services de cette société. La clé publique du nœud est donc masquée de cette dernière, et la clé publique apparente utilisée pour la connexion sera différente lors de l'accès à chaque service.

[1641] Ces propos sont vérifiables grâce à de multiples analyses de données objectives, consultables à l'adresse suivante, « Bitcoin Hashrate Chart », in *BitInfoCharts.*

[1642] DELAHAYE Jean-Paul, « Logique & Calcul : Des crypto-monnaies sobres en énergie ? », in *Pour la science N° 536* / Juin 2022, « Malgré l'admiration qu'on doit à Satoshi Nakamoto, l'inventeur de la première cryptomonnaie que fut le Bitcoin, sa

	blockchains privées et hybrides, et probablement pour soutenir le lancement prochain d'un euro cryptographique pourtant dispensable. Face à ces constats, il semble qu'une interdiction totale du minage de bitcoins est utopique en raison de son caractère anti-fragile, c'est-à-dire conçu pour contourner toute censure.

Conclusion et perspectives

- Pour résumer et compléter les données qui précèdent, l'impact environnemental de Bitcoin varie considérablement en fonction des pays où le minage s'opère. Dans certains pays, l'électricité est produite principalement à partir de sources d'énergie renouvelables, ce qui peut réduire l'impact environnemental global de Bitcoin. Dans d'autres pays (Chine) où l'électricité était produite à partir de sources d'énergie non renouvelables, son impact environnemental ne semblait donc socialement et écologiquement plus justifiable.

- Il est actuellement difficile de déterminer dans quelle mesure les données du système financier traditionnel peuvent être comparées à celles du réseau Bitcoin en raison des biais personnels et institutionnels ainsi que des risques de désinformation politique des parties prenantes impliquées dans les études menées et mentionnées. En effet, chaque méthode de calcul utilisée est sujette à interprétation. Par conséquent, seule une analyse à long terme permettra de répondre de manière scientifique et objective à la question de savoir si Bitcoin est réellement dangereux pour la société et contraire à la volonté actuelle de lutte contre le réchauffement climatique. Pour ce faire, il serait nécessaire d'établir une liste de critères objectifs et largement reconnus par la communauté scientifique pour permettre des comparaisons valides. Ce tableau vise précisément à fournir une trace des données et des positions relatives à la Preuve de travail, concernant la période 2020-2023, pour faciliter une actualisation ultérieure par d'autres chercheurs.

- Jusqu'à présent, le travail des *miners*/mineurs consistait principalement à stabiliser le réseau électrique plutôt qu'à gaspiller de l'électricité[1643]. En effet, leur rôle était d'absorber l'excédent d'électricité produit par les infrastructures énergétiques traditionnelles[1644], qui était souvent gaspillé, car difficile à stocker ou à transporter. En comblant cette sous-utilisation des réseaux électriques de certains pays, les *miners* ont permis de financer le développement de ces infrastructures, notamment vers les énergies renouvelables, en vendant une partie des bitcoins qu'ils ont extraits. Il convient de noter que les *miners* recherchent avant tout une rentabilité économique, c'est-à-dire en cherchant à extraire des bitcoins à un coût inférieur à celui du

'preuve de travail' est indubitablement une absurdité. Il est indispensable qu'elle soit abandonnée si on souhaite réellement que cette nouvelle sorte de monnaie se développe, permettant l'existence d'un argent liquide numérique anonyme respectueux de la vie privée de chacun [euro cryptographique] ».

[1643] SANSFACON Jean-Robert, « Cryptomonnaies : pour qui l'électricité ? », « À Québec, le gouvernement Couillard est partagé entre la crainte d'être envahi par ces gaspilleurs d'énergie qui facilitent la vie du crime organisé et le risque de rater le coche des technologies de l'avenir. », 2018, in *Le Devoir*, disponible à l'adresse suivante

[1644] PERSON Pierre, Rapport de l'Assemblée nationale, *op. cit.*, « La production étant difficile à anticiper, elle induit régulièrement d'importants surplus quand les réseaux 75/204 de distribution ne sont pas suffisamment dimensionnés. Ainsi, la mauvaise répartition des réseaux de distribution et l'incapacité pour le secteur du renouvelable à stocker l'électricité produite est une aubaine pour les mineurs de bitcoins qui peuvent acheter de l'énergie à bas coût. Il s'agit d'une aubaine réciproque entre producteurs et consommateurs, cette énergie n'aurait pas trouvé preneur [sans les mineurs de bitcoins]. », p.74.

marché international[1645]. Par le passé, les États subventionnaient les énergies fossiles, ce qui avait pour effet de réduire le coût de l'électricité produite à partir de ces sources. Dans ce contexte, les mineurs étaient tentés d'utiliser ces sources d'énergie carbonée pour leurs activités, qui ne représentaient cependant que 33% de l'électricité consommée par le réseau en 2021. En 2023, les énergies subventionnées semblent principalement renouvelables, ce qui incite progressivement les *miners* à se tourner vers ces nouvelles sources d'énergie à coût décroissant[1646]. Il est important de souligner que seuls les *miners* utilisant des sources d'énergie verte seront à terme autorisés dans les pays développés, compte tenu de la prise de conscience croissante des enjeux climatiques. Il est également temps de mettre fin à l'idée reçue selon laquelle le « *minage sauvage* », c'est-à-dire dont la source d'énergie est irrégulière (non déclarée, volée et carbonées), représenterait toujours la majorité de cette industrie du Web 3.0. Force est de rappeler qu'au-delà d'une utilité sociale et économique progressivement manifeste, Bitcoin contribue, en raison de son incitation économique et de son mécanisme informatique, à innover vers une transition énergétique et de nouvelles sources d'énergies plus durables et moins coûteuses[1647]. Par conséquent, une interdiction légale du PoW serait contre-productive à la fois d'un point de vue scientifique et social. La société doit s'emparer du sujet afin de juger collectivement à quel point la Preuve de travail peut être acceptée dans certaines activités et secteurs. Cela est autant plus nécessaire pour l'avenir de l'écosystème qui ne pourrait subsister à long terme sans elle.

- En résumé, les *miners* recherchent des coûts électriques bas et des pays stables sur le plan politique pour leurs activités de minage, et de nombreux mineurs se sont par exemple installés au Texas pour fuir l'interdiction de leurs activités en Chine[1648]. Un rapport de la Maison-Blanche publié en août 2022 reconnaît pour la première fois que ces activités peuvent contribuer positivement à la transition énergétique[1649]. Un sondage mené en mai 2022 par le journal Forbes estime également que plus de 80% des Américains ne pensent pas que les investissements relatifs aux bitcoins menacent l'environnement[1650]. En revanche, en France et dans l'UE, la situation est différente, et il est nécessaire de mettre en place une législation *ad-hoc*, partiellement contraignante, mais également attrayante, pour inciter les *miners* les plus 'verts' à s'installer en Europe. Cela favoriserait la création d'emplois dans ce secteur industriel en plein essor et à forte valeur ajoutée pour tout l'écosystème blockchain européen, ce qui pourrait également profiter aux blockchains privées et hybrides étudiées. Il est

[1645] Par exemple, le 9 janvier 2023 le coût moyen d'extraction d'un bitcoin est pour un mineur de 13000$ tandis que sa valeur d'échange moyenne est de 16000$. Cette différence de 3000$ à cet instant *t* signifie qu'il est toujours rentable de *miner* pour ces *mineurs* qui gagnent les 3000$ de cette différence de prix. Prix et données issues du site suivant, in *TheMinerMag*, « Estimated Cost of Bitcoin Production ».

[1646] A titre d'exemple, les opérateurs de la grille électrique nationale du Texas (« ERCOT ») font appel aux mineurs de bitcoins pour les aider à stabiliser cette infrastructure d'énergie renouvelable qui est en forte croissance dans cet Etat et notamment durant les périodes de forte demande électrique (en période de pic les *mineurs* cessent leurs opérations et inversement), CONNELL Shaun, CARTER Nic, « Miners Are The Optimal Buyers: The Data Behind Bitcoin-Led Decarbonization In Texas », in *Bitcoin Magazine*, 2021, disponible à l'adresse suivante

[1647] *Ibid.* Rapport pour l'Assemblée nationale, « les mineurs de bitcoins semblent se diriger naturellement vers des sources d'énergie renouvelables. », p.74.

[1648] Motherboard, « How Bitcoin Mines Were Airlifted From China to the US », in *CRYPTOLAND* Episode 7, (21 avril 2022) [Vidéo]. YouTube.

[1649] Traduit de l'anglais « […] les exploitations minières de crypto-actifs qui capturent le méthane évacué pour produire de l'électricité peuvent avoir des résultats positifs pour le climat, en convertissant le puissant méthane en CO2 pendant la combustion. Les opérations minières pourraient toutefois être plus fiables et plus efficaces pour convertir le méthane en CO2. », The White House, « Climate and energy implications of crypto-assets in the united states », 2022, in *whitehouse.gov*. Consulté le 9 septembre 2022, à l'adresse suivante, p.24.

[1650] DUGGAN Wayne, « Survey : 84 % of Americans don't believe that Bitcoin investments are a threat to the environment », 2022, in *Forbes Advisor*. Disponible à l'adresse suivante

envisageable que l'Union européenne établisse une *sandbox réglementaire* dédiée, pour tester de nouveaux services financiers ou modèles d'affaires dans des conditions réelles. Les propositions de Pierre Person, ancien député, présentées dans son rapport à l'Assemblée nationale[1651], devraient être examinées attentivement. Elles incluent la promotion de partenariats entre les producteurs d'énergie et les mineurs de crypto-actifs ainsi que l'interdiction du minage de crypto-actifs à partir de sources d'énergie carbonées, en ajustant la règlementation applicable aux droits à polluer[1652].

- Comme exposé et supposé en amont, l'extraction de bitcoins (minage) pourrait progressivement financer le développement d'énergies propres, opportunité qui commence à être reconnue par certaines entreprises[1653] et mêmes par certaines institutions mentionnées. Ces dernières perçoivent le minage comme essentiel pour stabiliser et décarboner le réseau électrique et ses infrastructures à ce jour sous-utilisées, comme au Texas[1654] et au Salvador ci-avant évoqués. En août 2022[1655], 2% de la puissance électrique du Texas est allouée au minage de bitcoins, un chiffre dont l'interprétation positive ou négative dépend intimement de la perception de l'utilité sociale que possède ou non ce réseau monétaire et financier selon chaque observateur. Finalement, seule l'éducation du corps politique[1656] et le lobbying pourraient à terme forger une adhésion sociale partielle ou totale sur laquelle se fonderont probablement des contentieux qui en découleront (formant ainsi une jurisprudence). Bitcoin est un système qui propose un prix planché à l'énergie, car il permet de donner un prix théorique à d'importantes quantités d'énergies renouvelables à ce jour factuellement exploitée de façon sous optimale. Il s'agit finalement de ne pas perdre le contact avec la réalité du terrain sur un sujet aussi technique que transversal afin que l'écologie reste connectée au réel et qu'elle ne devienne pas une arme idéologique au service d'idéaux biaisés par une désinformation politique et/ou institutionnelle continue.

- A la lumière des informations précédentes, le minage de Bitcoin présente un *mix énergétique* d'environ 60% issu d'énergies renouvelables, ce qui signifie qu'il semble plus 'vert' que ce que peuvent le laisser les institutions les plus réticentes à son égard. Dans les prochaines années et selon un communiqué publié en 2022 par la Commission européenne, cette dernière cherche à « *promouvoir les mécanismes de consensus 'respectueux de l'environnement' par l'intermédiaire de l'infrastructure européenne de services blockchain* [EBSI] *comme norme d'or en Europe et dans le monde.* », notamment en développant « *un label d'efficacité énergétique pour les blockchains.* »[1657], ainsi qu'en publiant d'ici 2025 un rapport « *qui comprendra une description de l'impact environnemental et climatique des nouvelles technologies sur le marché des crypto-actifs. Le rapport comprendra également une évaluation des options politiques visant à atténuer les effets négatifs sur le climat des*

[1651] *Op. cit.*, PERSON Pierre, Rapport de l'Assemblée nationale, « Face à l'interdiction réclamée par certains, ce rapport défend une vision selon laquelle les pouvoirs publics doivent mettre en œuvre une politique permettant d'orienter les mineurs vers les énergies propres et de récompenser ceux qui financent la transition écologique. », p.78.
[1652] ACPR. « Une Sandbox réglementaire. Une Sandbox réglementaire - bac à sable réglementaire - pour quoi faire ? », 2019, p.1, disponible à l'adresse suivante
[1653] Blockstream, « Blockstream and Block Inc.' ; s Solar Mining Facility, Now Powered by Tesla Solar PV and Megapack », 2022. Consulté le 1 juin 2022, à l'adresse suivante
[1654] WEBB Shelby « Texas renewables generated record power in early 2022 », 2022, in *Houston Chronicle*, consulté le 3 mai 2022, à l'adresse suivante
[1655] VICE News, « The Future of Bitcoin Mining and the Environment », 2022, [Vidéo]. YouTube
[1656] Sénat, audition « Régulation et innovation dans le domaine des cryptoactifs », table ronde, intervention de Faustine Fleuret, in *videos.senat.fr*, (visionnage à 12:15).
[1657] Communication: Digitalising the energy system - EU action plan, COM(2022)552/2, traduction libre de l'anglais, consulté le 18 octobre 2022, à l'adresse suivante, p.17.

technologies utilisées sur le marché des crypto-actifs, en particulier en ce qui concerne les mécanismes de consensus. ». Si ces décisions sont nécessaires et semblent cohérentes à l'aune de la crise énergétique en 2023, il est soutenu que la motivation politique actuelle à l'encontre du mécanisme de PoW n'est que partiellement justifiée et qu'elle fait courir un risque systémique pour l'écosystème blockchain et technologique européen. Il est souligné que cette volonté politique ne semble pas seulement européenne, mais bien internationale « *Comme l'Europe ne représente actuellement qu'environ 10 % des activités d'extraction par preuves de travail* [en réalité plutôt 1,5 à 2% d'après d'autres spécialistes][1658], *une coopération internationale est nécessaire pour s'attaquer au problème de la forte consommation d'énergie de l'extraction de preuves de travail d'une manière qui ait un impact mondial.* »[1659].

- Il est important d'être pragmatique en ce qui concerne les mineurs de bitcoins, car seuls les *miners* utilisant des sources d'électricité peu coûteuses et peu carbonées (appelé « *minage durable* » ou « *green mining* ») pourront survivre à long terme (« *les survivants* »)[1660]. Ces activités sont les seules rentables et socialement acceptées dans la mesure où les autres *miners* utilisant des sources d'électricité carbonées comme le charbon ou le pétrole disparaîtront progressivement en raison d'une adhésion sociale et politique insuffisante pour soutenir leurs activités. En mars 2023, une expérience de minage de bitcoins unique, Nautilus, a été lancée dans le nord-est de la Pennsylvanie. Cette *installation minière* est mise en place par la société Terawulf et utilise pour la première fois au monde une source d'énergie nucléaire[1661], « *durable* » au sens de la Commission européenne[1662], une idée révolutionnaire pourtant impensable il y a seulement quelques années.

- D'après une étude prospective publiée en août 2022[1663], il est possible que la consommation énergétique du Bitcoin augmente considérablement si son prix atteint 2 millions de dollars en 2040 (une estimation aujourd'hui fantasmagorique mais à ne pas sous estimer dans un temps plus long). Selon cette étude, la consommation électrique de Bitcoin pourrait être multipliée par environ 10, passant ainsi de 0,05% de l'électricité mondiale en 2022 à 0,36% en 2040. Cependant, d'autres études estiment ce chiffre respectivement à 0,55% en 2021[1664] et 0,6% en 2022 (*v.* l'étude citée dans l'argument N°1 du présent tableau). La consommation énergétique de Bitcoin dépend donc de son prix, et si celui-ci atteint 500 000 dollars en 2040, sa consommation pourrait dépasser 0,1% de l'électricité mondiale, un chiffre plus plausible à ce stade. Bien que la future consommation d'énergie de Bitcoin soit incertaine et dépende de plusieurs facteurs, l'auteur de l'étude considère que le minage de bitcoins sera considéré comme une industrie à forte intensité énergétique[1665], mais elle resterait bien en dessous de

[1658] STACHTCHENKO Alexandre, Twitter. 2022, disponible à l'adresse suivante
[1659] Communication: Digitalising the energy system - EU action plan, *op. cit.*, traduction libre de l'anglais, p.17.
[1660] Grand Angle Crypto, « La théorie du dernier survivant dans le minage crypto ! », 2022. [Vidéo]. YouTube
[1661] Terawulf, consulté le 16 février 2023, *v.* projet « Nautilus Cryptomine ». Disponible à l'adresse suivante
[1662] Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur l'inclusion du nucléaire dans le volet climatique de la taxonomie européenne des investissements durables : L'inclusion de l'énergie nucléaire dans la taxonomie européenne des activités durables, in *sénat.fr*, 2021, disponible à l'adresse suivante
[1663] MELLERUD Jaran, « How much energy will Bitcoin consume in the future? », 2022, in *Arcane Research*. Disponible en ligne
[1664] CARTER Nic, traduit librement de l'anglais : « Selon le Cambridge Center for Alternative Finance, le bitcoin consomme actuellement environ 110 térawattheures par an, soit 0,55 % de la production mondiale d'électricité, ou l'équivalent de la consommation annuelle d'énergie de petits pays comme la Malaisie ou la Suède. », « How Much Energy Does Bitcoin Actually Consume ? », 2021, in *Harvard Business Review*. Disponible à l'adresse suivante
[1665] *Ibid.* Traduit librement de l'anglais : « Qu'est-ce qui détermine la consommation énergétique future de Bitcoin ? 1) Le prix du BTC 2) Les frais de transaction 3) Le pourcentage des revenus des mineurs dépensés en énergie 4) Le prix moyen de l'énergie des mineurs de bitcoin »,

secteurs tels que la production de ciment qui consomme d'ores et déjà plus de 2% de l'énergie mondiale en 2022[1666].

- En fin de compte, l'orientation clé de cette Annexe est de savoir si le fait de dépenser entre 0,17%, ou maximum 1% de l'électricité mondiale à long terme, pour rappel de l'électricité optimisée et provenant d'énergies renouvelables grâce au minage, afin de sécuriser une infrastructure financière accessible à des milliards de personnes, sera socialement bénéfique et justifié pour et par la société. Bien que les chiffres soient relativement incertains à ce stade, cette question doit être examinée de près par chacun et chacune d'entre-nous. Une première piste de réponse apparait selon Daniel Batten, investisseur, auteur et spécialiste des nouvelles technologies impactant le climat, car Bitcoin serait tout simplement une « *solution contre-intuitive* » dans la lutte contre le changement climatique[1667]. Autrement dit, ce système serait injustement systématiquement discrédité en raison d'un manque de connaissances à son égard, alors qu'il pourrait représenter un système crucial pour atteindre certains objectifs climatiques internationaux.

Focus 2 : La Preuve d'enjeux « *Proof of Stake - PoS* » comme alternative supposée au PoW

La Preuve d'enjeux (« *Proof of Stake – PoS* ») est un autre mécanisme de consensus introduit en 2012[1668]. Ce mécanisme de consensus alternatif a donc été imaginé dans la lignée du mécanisme de Preuve de travail exposé précédemment. La Preuve d'enjeux délègue la validation et le contrôle du réseau aux propriétaires des jetons du réseau. En d'autres termes, elle attribue la responsabilité de la validation des blocs aux utilisateurs en fonction de leur participation financière investie sur ladite blockchain. Plus précisément, les utilisateurs qui possèdent des jetons de ladite blockchain peuvent « *mettre en jeu* » une partie de leur participation et être sélectionnés de manière aléatoire pour valider les transactions. En pratique, des nœuds validateurs déposent et mettent en séquestre (« *stake* ») les jetons qu'ils détiennent sur un contrat intelligent spécifique[1669]. De cette façon, ce séquestre agit comme une garantie (crypto)financière. S'ils négligent les règles du réseau ou prennent des décisions frauduleuses (tentative de corruption des blocs et du réseau), lesdits utilisateurs et validateurs sont automatiquement pénalisés par l'algorithme c'est-à-dire privés de tout ou partie de leurs jetons initialement séquestrés. En ce sens, ce séquestre est parfois présenté comme une amélioration théorique par rapport au mécanisme de PoW, car il ne nécessite ni de matériel informatique spécialisé (ASIC), ni ne requiert une consommation d'électricité importante (l'empreinte énergétique du PoS est donc plus faible, le temps de validation des transactions plus court, les volumes de transactions plus importants, mais la résilience informatique globale plus faible). Si plusieurs blockchains ont tenté d'implémenter

[1666] Propos librement traduit de l'anglais et issus d'un extrait publié par Jaran Mellerud sur son compte Twitter, le 23 août 2022, « Avec une telle consommation d'énergie, l'exploitation minière de bitcoins sera considérée comme une industrie à forte intensité énergétique, mais encore bien loin d'industries comme la production de ciment, qui consomme 2 % de l'énergie mondiale ».
[1667] BATTEN Daniel, « Bitcoin Mining Can Prevent Climate Change », in *Bitcoin Magazine*, disponible à l'adresse suivante
[1668] Guest author, « The History and Evolution of Proof-of-Stake », 2017, Cointelegraph. V. également www.wenmerge.com
[1669] Pour la blockchain Ethereum et depuis fin 2022 (*v.* ci-après), un *nœud validateur* doit envoyer un montant important d'ethers (33 ethers soit environ 60 000$) sur le *contrat intelligent* suivant afin de pouvoir espérer être aléatoirement sélectionné pour valider un bloc puis obtenir la récompense associée (en ethers).

avec plus ou moins de succès le PoS, la présente Annexe se concentre sur la mise à jour de la blockchain Ethereum, qui implémente progressivement ce mécanisme depuis plusieurs années.

Ethereum est une blockchain publique avec son propre jeton numérique appelé « *ether* » (dont le fonctionnement est relativement similaire aux échanges en bitcoins). Bien qu'intimement liée à l'histoire de Bitcoin, la blockchain Ethereum diffère désormais dans sa finalité et son fonctionnement. Ethereum vise à devenir une infrastructure mondiale décentralisée pour le développement d'applications sans tiers de confiance, en offrant une puissance de calcul et d'exécution dédiée à des applications dites décentralisées. Pour utiliser cette nouvelle architecture distribuée, il est nécessaire d'utiliser son jeton natif, l'ether. En outre, les utilisateurs de cette blockchain peuvent créer d'autres jetons non natifs pour leur propre usage[1670], moyennant le paiement de frais de transaction en ether (jeton natif), pour émettre ou échanger ces premiers. Depuis son lancement le 30 juillet 2015, Ethereum est en quelque sorte devenu un laboratoire informatique dédié à la finance 3.0, c'est-à-dire un nouvel espace numérique consacré à la *tokenisation* progressive de la société. Ce réseau et bac à sable informatique 3.0 permet en comparaison plus de cas d'usage que la blockchain Bitcoin, car Ethereum est complexe, hybride (semi-décentralisée), mais évolutif, tandis que Bitcoin propose pour rappel une monnaie cryptographique résiliente et fiable, mais moins évolutive pour l'instant. Il est essentiel de remarquer que la blockchain Bitcoin est plus décentralisée que la blockchain Ethereum, un constat également similaire concernant leurs écosystèmes d'applications adjacents[1671]. Cela implique que la relative centralisation d'Ethereum peut précisément être ciblée par des régulateurs, gouvernements ou hackers, tandis que la résilience globale du protocole Bitcoin rend une telle recherche de centralisation en théorie bien plus complexe voire impraticable.

Depuis son lancement, la Fondation Ethereum[1672] a planifié et entrepris de nombreuses phases de mise à jour complexes pour soutenir le protocole Ethereum, ces améliorations étant ensuite implémentées par les « *Core développeurs* » majoritairement financés par cette même Fondation. Depuis 2022, ces étapes de développement sont au nombre de cinq : « *The Merge* » (décembre 2022), « *The Surge* » (2023), « *The Verge* » (2023), « *The Purge* » (2023) et « *The Splurge* » (2024)[1673]. Bien que les détails techniques de chacune de ces mises à jour soient complexes, elles constituent ensemble la promesse ambitieuse d'une blockchain initialement publique, devenue hybride pour finalement redevenir publique avec ce nouveau mécanisme de PoS. En cas de réussite, Ethereum pourrait se posistionner et répondre de façon inédite au triangle d'incompatibilité étudié dans la première partie de cette recherche. Depuis sa mise à jour majeure de décembre 2022 (The Merge), Ethereum n'utilise plus le mécanisme de la Preuve de

[1670] Ces jetons sont en quelques sortes des sous-jetons (non-natifs), c'est-à-dire adossés à l'ether (jeton natif), mais possédant dans certains cas leurs propres caractéristiques et synergies.
[1671] V. *infra*, Annexe 7.
[1672] Ethereum Foundation, *v.* Ethereum.org
[1673] Ethereum, « Ethereum upgrades (formerly 'Eth2') », *v.* Ethereum.org

travail jusqu'alors empruntée à Bitcoin, mais l'a remplacé par le mécanisme susvisé de la Preuve d'enjeux dont le fonctionnement peut se résumer en cinq étapes :

(i) Les utilisateurs séquestrent leurs jetons (ethers) sur leur propre nœud (ordinateur conventionnel), ou le plus souvent sur celui d'un service en ligne tiers. Cette étape est obligatoire pour que le nœud soit considéré par le réseau comme opérationnel.
(ii) Les nœuds éligibles entrent en compétition pour construire les transactions du prochain bloc, à la condition d'avoir respecté l'étape précédente.
(iii) Le protocole de la Preuve d'enjeu choisit aléatoirement un nœud pour valider et « *forger* » chaque nouveau bloc.
(iv) La récompense en ethers et d'autres données sont temporairement séquestrées jusqu'à ce que d'autres nœuds honnêtes vérifient la validité des transactions.
(v) Cette récompense est libérée et envoyée au nœud validateur (honnête) qui a forgé le bloc, mais seulement lorsque le réseau sait que l'opération n'est pas incorrecte ou frauduleuse. A cette étape, il existe plusieurs mécanismes de rémunération possibles (calcul puis distribution variable de cette récompense selon certaines situations).

Fort de ces informations non exhaustives, il est souligné le fait que le PoS entraîne une tendance de centralisation, c'est-à-dire que cette méthode de séquestre a pour effet de concentrer à court et moyen termes la validation et le contrôle du réseau auprès des détenteurs de larges quantités de jetons. En d'autres termes et selon les algorithmes régissant le PoS, plus un utilisateur possède de jetons et les séquestre sur son nœud, plus il est probable qu'il soit sélectionné pour valider des blocs, ce qui implique une centralisation de ce mécanisme de validation auprès des acteurs qui possèdent le plus d'ethers (un constat qui peut en théorie être exploité de façon malicieuse pour corrompre le réseau, par exemple en ciblant ces détenteurs les plus importants). Pour illustrer ces propos, le Trésor américain a sanctionné en août 2022 le service en ligne Tornado Cash[1674] (aujourd'hui à nouveau accessible), un logiciel open source permettant l'envoi et le mélange hautement pseudo-anonyme[1675] d'ethers sur la blockchain Ethereum. Cette action a conduit le Trésor américain à placer plusieurs adresses ethereum sur la liste d'interdiction (liste noire) du Bureau de contrôle des avoirs étrangers (« *Office of Foreign Assets Control – OFAC* »), interdisant à leurs propriétaires l'accès à tout service en ligne, y compris le transfert de leurs fonds en ethers. Cette interdiction générale de ce service d'anonymisation affecte non seulement les utilisateurs mal intentionnés (activités illicites), mais également et surtout la majorité des utilisateurs de bonne foi qui souhaitent simplement renforcer la protection de leur vie privée en ligne. En outre, cette décision pose des questions cruciales pour les nœuds validateurs d'Ethereum impliqués dans la validation – pour rappel automatique et non discriminatoire - des transactions attachées à des activités

[1674] U.S. Department of the Treasury, « U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash », 2023. Disponible à l'adresse suivante
[1675] V. *Supra*, I, Titre 2, 1.4.1

illicites. Par exemple, un validateur géré par une entreprise immatriculée aux États-Unis sera-t-il considéré comme responsable s'il inclut dans un bloc - à son insu - une transaction provenant d'une adresse identifiée comme suspecte ou interdite ? Si un validateur signe le bloc d'un autre validateur qui a inclus des transactions provenant d'adresses interdites, sera-t-il également considéré comme responsable et par conséquent sanctionné ?

Au regard de ces premiers constats juridiques, le risque de censure potentielle de tout ou partie des blocs ou transactions de la blockchain Ethereum par le gouvernement américain est ainsi particulièrement préoccupant étant donné que les deux tiers des nœuds validateurs – désormais en PoS - de la blockchain Ethereum, sont situés aux États-Unis. Si le gouvernement américain décide que les validateurs sont tenus de censurer certaines transactions, cela mettrait en danger le principe même de décentralisation de cette blockchain. En effet, en cas de soupçon de blanchiment par un utilisateur, 66% des validateurs d'Ethereum seraient légalement tenus d'exclure ces transactions des blocs[1676], tandis que les 34% restants perdraient leurs ethers séquestrés s'ils tentent d'inclure et de valider ce même bloc qui contient une ou plusieurs transactions supposées illicites. En cas de renforcement de cette tendance, voire de contagion à d'autres juridictions internationales, cette menace politique et étatique latente également observée en Europe pourrait représenter une menace existentielle pour tous les mécanismes de consensus, y compris la Proof-of-Work, qui est déjà menacée d'interdiction en raison de sa consommation énergétique.

Bien que les garanties de résilience et de sécurité de la Proof-of-Stake (PoS) semblent donc inférieures à celles de la Proof-of-Work (PoW)[1677], il est possible que la centralisation qui en découle soit réduite à long terme, ce qui signifierait que la promesse informatique de la blockchain Ethereum a fonctionné. Cela nécessiterait toutefois que la PoS tienne ses promesses techniques, complexes, en matière d'évolutivité, de volumétrie et de temps de réponse, telles que décrites dans cette étude. Si cela se produit, le mécanisme de PoS pourrait devenir plus décentralisé, avec des avantages potentiels qui comblerait à long terme la sécurité et la résilience de la blockchain Ethereum. Cependant, si la PoS fera probablement ses preuves techniques sur le long terme, force est de constater qu'il n'égalera probablement pas à long terme la résilience, la décentralisation et la stabilité du protocole Bitcoin et de son mécanisme de PoW[1678]. A cet égard, chaque acteur s'impliquant dans l'écosystème blockchain

[1676] Le site internet suivant permet de suivre en temps réel le pourcentage des blocs conformes aux règles LCB-FT édictées par l'OFAC et validés sur Ethereum (par des acteurs forcés d'être en conformité sous peine de sanctions, comme le projet *Tornado Cash* mentionné).
[1677] SZTORC Paul, « Long Live Proof-of-Work, Long Live Mining », 2014, in Truthcoin.info, traduction libre de l'anglais, « Dans un avenir prévisible, il n'y a pas d'alternative significative à la preuve de travail (…) », disponible à l'adresse suivante
[1678] Une étude datant du 16 août 2022 démontre que 65 % des nœuds Ethereum sont hébergés dans des centres de données centralisés (« *data centers* »). Selon l'étude, deux tiers d'entre eux proviennent de trois grands fournisseurs de données de services web. L'étude a également révélé que les fournisseurs web centralisés contrôlent la grande majorité des 4 653 nœuds Ethereum actifs. Cela peut exposer Ethereum à des points centraux de défaillance. Outre les 69 % de modes hébergés sur le réseau principal Ethereum, Amazon Web Services (AWS) héberge plus de 50 % des nœuds du réseau Ethereum. En outre, plus de 15 % des nœuds sont hébergés par la société Hetzner et 4,1 % par la société OVH. La centralisation géographique est également un problème majeur pour la blockchain Ethereum : les États-Unis et l'Allemagne concentrent géographiquement les nœuds Ethereum, pour respectivement 46% et 13%, KASSAB Sami. « Do Ankr and Pocket Solve Web3's Node Centralization Problems? », 2022, disponible sur messari.io. V. également CRYPTOJON, « Ethereum : Le Mensonge De La Ultra Sound

recherche un degré minimum de résilience informatique auquel une blockchain doit répondre (souvent évoquée et assimilée par le terme d'immuabilité). La question est ainsi de savoir si Ethereum garantit un tel seuil aujourd'hui. Par exemple, il semble que les services financiers 3.0 souhaitent avant tout bâtir des services en ligne sur un socle informatique robuste, pérenne et véritablement décentralisée, en dépit d'un champ des possibles réduit en termes d'applications et de cas d'usage. Pour conclure, si Ethereum propose certes à ce jour des possibilités de cas d'usage que Bitcoin ne permet pas pour l'instant (contrats intelligents, finance décentralisée, stablecoins), son écosystème d'applications distribuées bâties sur Ethereum demeure immature et sujet à une recentralisation sociale, économique et juridique relativement importante. Il est par ailleurs probable qu'à l'avenir les applications décentralisées d'Ethereum soient concurrencées par les futures mises à jour du protocole Bitcoin qui ont été étudiées (Lightning Network, Taproot, Taro, Ordinals). Toutefois, cette 'censurabilité' latente du protocole Ethereum et de ses applications[1679] semble être une opportunité pour le cas d'usage de l'identité numérique distribuée qui nécessite une certaine garantie par la puissance publique concernant la délivrance d'attributs d'identité racines. Ainsi, comme l'admet en personne le co-fondateur d'Ethereum en 2020, la promesse de valeur du PoS n'en est qu'à ses débuts : « *La différence entre Bitcoin et Ethereum est que les Bitcoiners considèrent que Bitcoin est terminé à 80 %, mais les Ethereans considèrent qu'Ethereum est terminé à 55%* »[1680].

Focus 3 : La Preuve d'autorité « *Proof of Authority - PoA* »

Qu'il s'agisse de la Preuve de travail ou bien de la Preuve d'enjeux, ces deux mécanismes sont aujourd'hui principalement adoptés par des blockchains publiques. Les blockchains privées et hybrides utilisent d'autres mécanismes de consensus, dont celui prédominant est la Preuve d'autorité (« *Proof of Authority – PoA* »). A titre d'illustration, des sociétés et consortiums blockchains tels que l'EBSI[1681], la BCN[1682] ou encore Alastria[1683] utilisent ce mécanisme de consensus. Comme son nom l'indique, il s'agit d'un mécanisme de consensus accordant à quelques organisations le pouvoir et l'autorité de générer puis valider les blocs d'une blockchain. En d'autres termes, le PoA nécessite que ses organisations parties prenantes désignent certaines d'entre-elles en tant qu'autorités dument identifiées et responsables de la validation des blocs du réseau. L'identité des nœuds et des acteurs participants est ainsi dévoilée et limitée en fonction de la confiance que la réputation de chacun d'entre eux peut légitimement inspirer à toutes les parties prenantes de l'infrastructure. Lorsque cette réputation est importante, un nœud aura des capacités de validation et de vérification complète des blocs, tandis que dans le cas inverse, seule une fonction de vérification est généralement attribuée. Bien que ce mécanisme permette aux

Money » [Vidéo]. YouTube. V. également MoneyRadar Crypto. « Ethereum Menacé Les plus Grands Risques qui pèsent sur ETH », 2023, [Vidéo]. YouTube

[1679] V. Annexe 7.

[1680] LOCKE Taylor, « Vitalik Buterin says Ethereum will be '55% complete' post-merge », 2022, in finance.yahoo.com

[1681] V. *Supra*, I, Titre 1, 2.2.2.2

[1682] V. *Supra*, I, Titre 2, 2.8

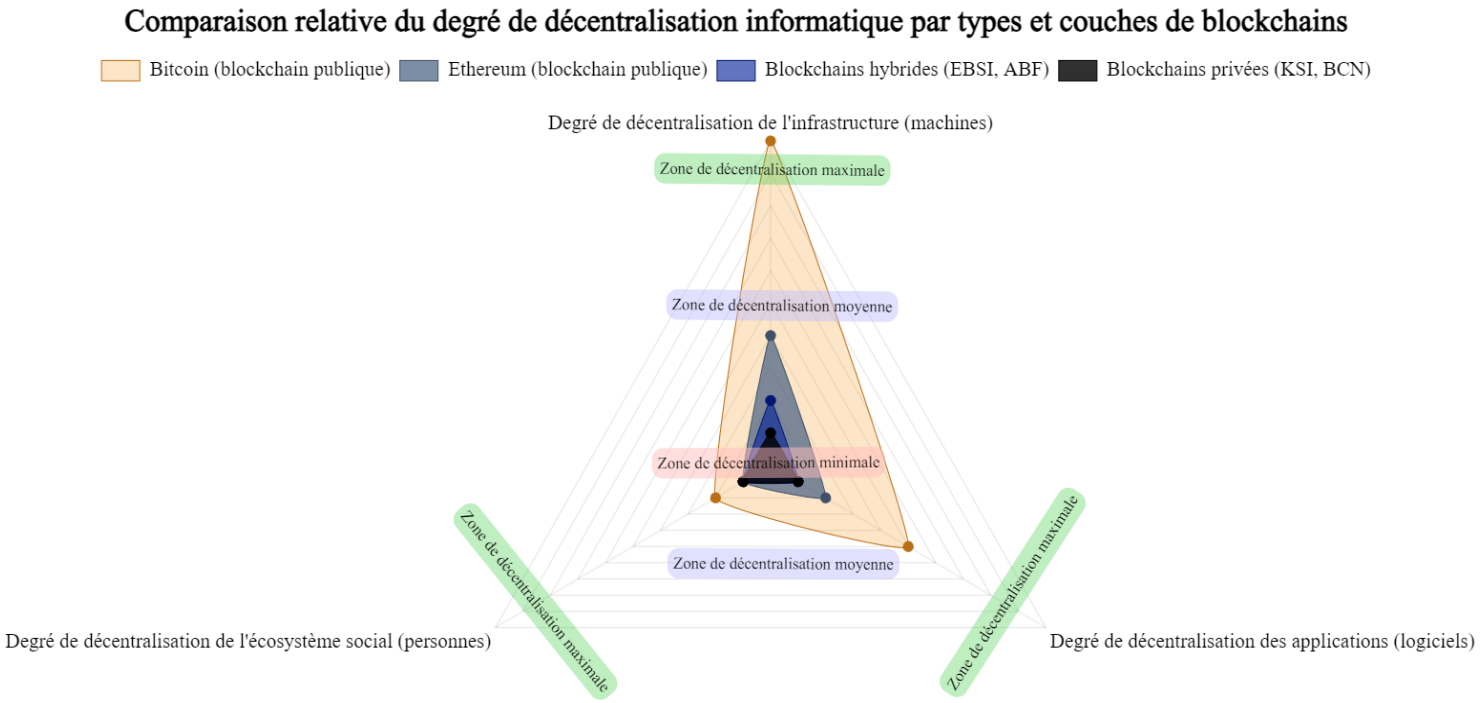
[1683] V. *Supra*, I, Titre 1, 2.2.2.1.d

organisations de concevoir un réseau informatique personnalisé et conforme aux règlementations en vigueur (RGPD, eIDAS, MiCA, Data Act), il ne permet néanmoins que la création de blockchains faiblement décentralisées. En effet, nous avons constaté que pour les réseaux consortiums de ce type, le nombre optimal de nœuds n'est que de quelques dizaines. Au-delà de ce chiffre, ces réseaux sont confrontés à des difficultés qu'ils ont du mal à résoudre[1684]. Cette difficulté est également applicable aux blockchains publiques, mais celles-ci peuvent y répondre plus efficacement grâce à leur effet d'expérience et à la taille importante de leurs communautés de développeurs. Le mécanisme de consensus utilisé peut être comparé à un protocole de vote dans lequel chaque utilisateur a un poids de vote prédéfini, basé sur la réputation de chacun des acteurs impliqués. En résumé, le mécanisme de PoA convient aux organisations qui ont un nombre restreint de membres et qui ont besoin de collaborer via un protocole informatique peu ou prou décentralisé. Le PoA offre une conformité juridique totale et permet une adaptation aux évolutions législatives et règlementaires grâce à des systèmes de vote numérique spécifiques à une gouvernance supposée modulable. En pratique, la maintenance de ces réseaux peut être fastidieuse et complexe pour ses membres, ce qui peut entraîner des délais conséquents et des surcoûts inattendus. Ainsi, certaines blockchains hybrides choisissent d'implémenter un jeton numérique publiquement, accessible ou non[1685], pour financer et assurer le développement de l'infrastructure et de ses applications associées. Cela peut rendre la frontière entre ces blockchains hybrides et les blockchains publiques moins nette sur le plan économique, informatique et social, ouvrant toutefois le champ des possibles en matière d'interopérabilité informatique.

[1684] *Op. cit.* A titre d'illustration, la blockchain *Hyperledger Indy* atteint un consensus optimal lorsque 25 nœuds sont opérationnels (très peu comparé aux blockchains publiques), et au minimum 8 nœuds sur 25 devant être fonctionnel afin d'assurer la continuité de ladite blockchain déployée (en d'autres termes, au-delà de 25 nœuds des risques fonctionnels existent pour le consensus), « Introduction to Hyperledger Sovereign Identity Blockchain Solutions: Indy, Aries & Ursa », consulté en ligne le 14/10/2021.

[1685] Il est fait référence à la blockchain hybride Arianee qui est une association loi 1901 délivrant un jeton/token à ses membres, ce dernier étant également accessible publiquement. Pour plus d'informations, consultez le lien suivant

Annexe 7 : Illustration des composantes et niveaux de décentralisation par blockchain (2022)



Annexe 8 : Tableau résumé du protocole de justice décentralisée Kleros

Pour rappel, Kleros est un ensemble de services d'arbitrage en ligne, conçus pour être décentralisés grâce à la technologie de la blockchain Ethereum. En utilisant des techniques telles que la théorie des jeux, le crowdsourcing, le pseudo-anonymat et la décentralisation, Kleros est capable de résoudre une variété de litiges, ce qui en fait un système judiciaire décentralisé à l'ère du Web 3.0. Le tableau suivant propose un résumé de certaines lignes directrices mentionnées dans la partie dédiée à cette solution 3.0[1686].

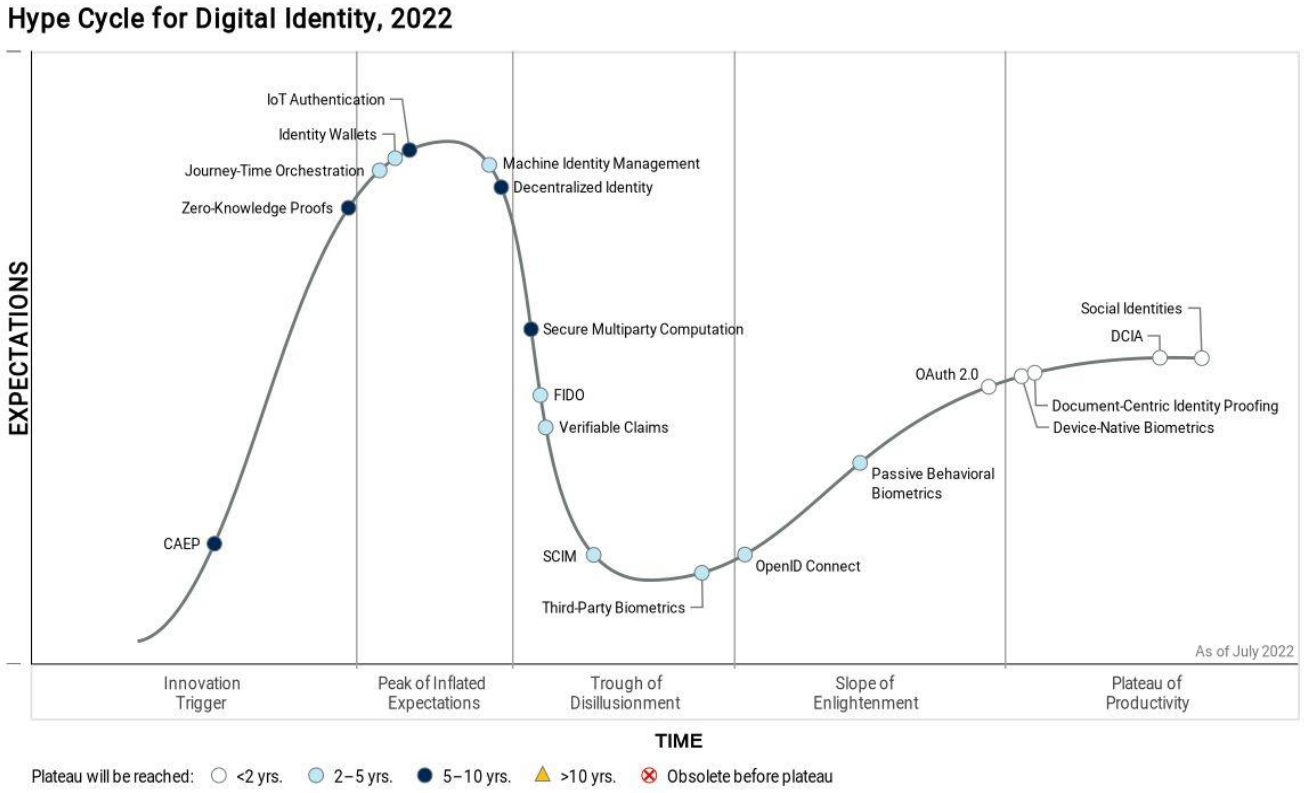
Questions	**Réponses**
Le *Modus operandi* de Kleros est-il juridiquement ou moralement juste ?	Kleros semble être moralement juste aux yeux de sa communauté actuelle qui reste limitée en nombre. Cependant, le principe de sagesse communautaire et d'incitation économique sur lequel il repose dépend d'un nombre minimal de participants/utilisateurs, qui peut varier avec le temps et affecter les décisions et vérités collectives rendues par le protocole. Bien que certains grands principes du droit servent d'inspiration pour les décisions morales prises par ce protocole, le principe de territorialité du droit n'est pas respecté (et ne semble pas avoir pour objectif de l'être à court terme).
Kleros est-il conforme au droit en vigueur, c'est-à-dire juridiquement reconnu ?	A priori, Kleros ne respecte ni le RGPD, ni eIDAS, ni les Règlements MiCA et TFR, ni les règles internationales d'arbitrage énoncées à l'article I chapitre 1 de la Convention de New York[1687], ni même les principes de territorialité. Cependant, bien que le projet Kleros ne soit qu'au début de ses promesses, une reconnaissance progressive et partielle semble envisageable à moyen ou long terme, notamment grâce à une décision de justice rendue au Mexique et à la récompense du Conseil européen de l'innovation remportée en 2020.

[1686] V. *Supra,* I, Titre 2, 2.7.2

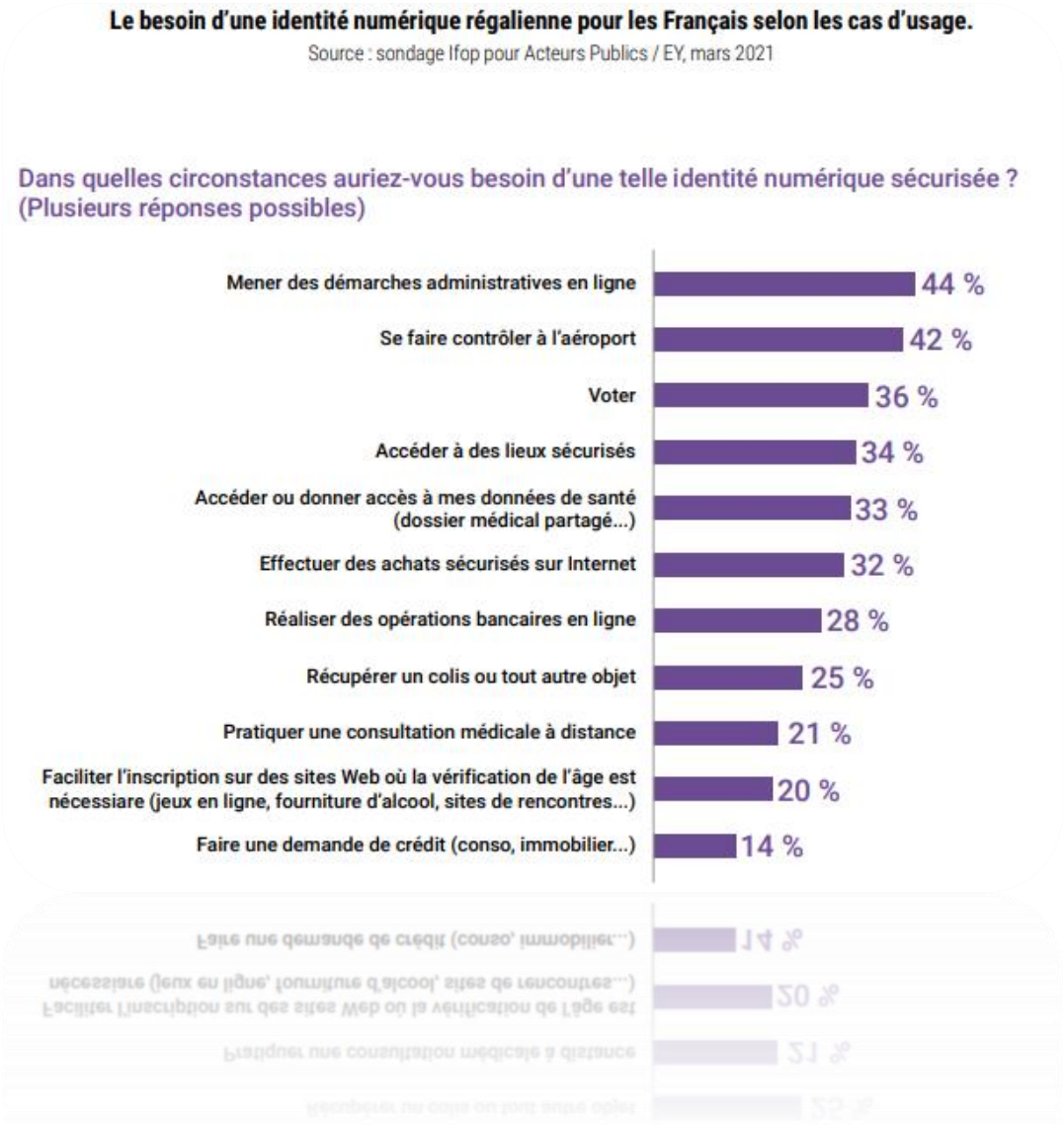
[1687] FERREIRA Leonel Constantino, « La résolution des litiges blockchain : vers un arbitrage décentralisé ? », publié en janvier 2021, in *Mémoire de Master, Université de Neuchâtel,* « Même si, en fonction des circonstances du cas d'espèce, une décision de Kleros peut théoriquement être qualifiée de sentence arbitrale étrangère au sens de la Convention de NY, la procédure souffre de plusieurs anomalies empêchant d'opérer une telle qualification » ; « Lorsque la procédure de Kleros est délocalisée, en ce sens qu'elle n'est pas liée à un ordre juridique, la Convention de New York ne trouve pas application ». p.96.

Kleros est-il informatiquement décentralisé et open source ? En termes de gouvernance ? Le pseudo-anonymat des jurés est-il assuré ? Kleros peut-il être juridiquement contraint ou politiquement censuré ?	Le protocole Kleros est plus distribué que décentralisé. Son protocole hérite d'une décentralisation partielle de la blockchain Ethereum (dont il est tributaire), au même titre que les contrats intelligents de Kleros qui sont relativement centralisés en raison de la gestion des jetons PNK qui dépendent des équipes de Kleros et ses salariés. A ce titre, l'anonymat des jurés n'est parfois qu'un trompe-l'œil en raison des regroupements et de l'influence que certains exercent entre eux sur des messageries chiffrées (Telegram, Signal), ce qui dévie les décisions supposées sages, justes et impartiales. Oui, Kleros peut être juridiquement contraint de cesser une partie de ses activités sur décision judiciaire. Par exemple, leur site internet et leur communication en ligne sont en partie hébergés sur des plateformes centralisées. L'identité des porteurs de projet est aussi (re)connue, ce qui signifie qu'une censure politique et notamment institutionnelle serait possible.
Kleros revient-il à financiariser la justice en ligne ?	Oui, l'achat obligatoire de jetons PNK pour accéder au service en ligne de Kleros revient à conditionner les décisions de ce protocole à une financiarisation forcée que de nombreux internautes ne peuvent se permettre, notamment dans les pays en voie de développement pourtant ciblés par Kleros. En d'autres termes, cela s'éloigne d'une idée de justice en ligne décentralisée, accessible pour tous et gratuite.
A quel point Kleros est-il socialement adopté, c'est-à-dire utilisé par les internautes ?	Kleros est utilisé de façon marginale depuis son lancement. Il y a peu d'utilisateurs pour l'instant, car Kleros nécessite le maniement et la compréhension de crypto-actifs via des portefeuilles numériques plus ou moins complexes. Notons par ailleurs que ses cas d'usage et son positionnement dans la sphère crypto semblent pertinents, ce qui permet l'espoir d'une adoption à terme (celle-ci étant également conditionnée au succès des mises à jour de la blockchain Ethereum mentionnées).
Kleros fait-il concurrence et peut-il se substituer à la justice actuelle ?	Non, sauf si notre société se numérise davantage comme en cas d'avènement de « *métavers immersifs* », un espace politique en ligne qui lui fait d'ailleurs défaut et pourrait être implémenté sans abandonner au moins partiellement le concept d'anonymat, certes nécessaire, mais qui pourrait par ailleurs être repensé, car menacé par les Règlements mentionnés.

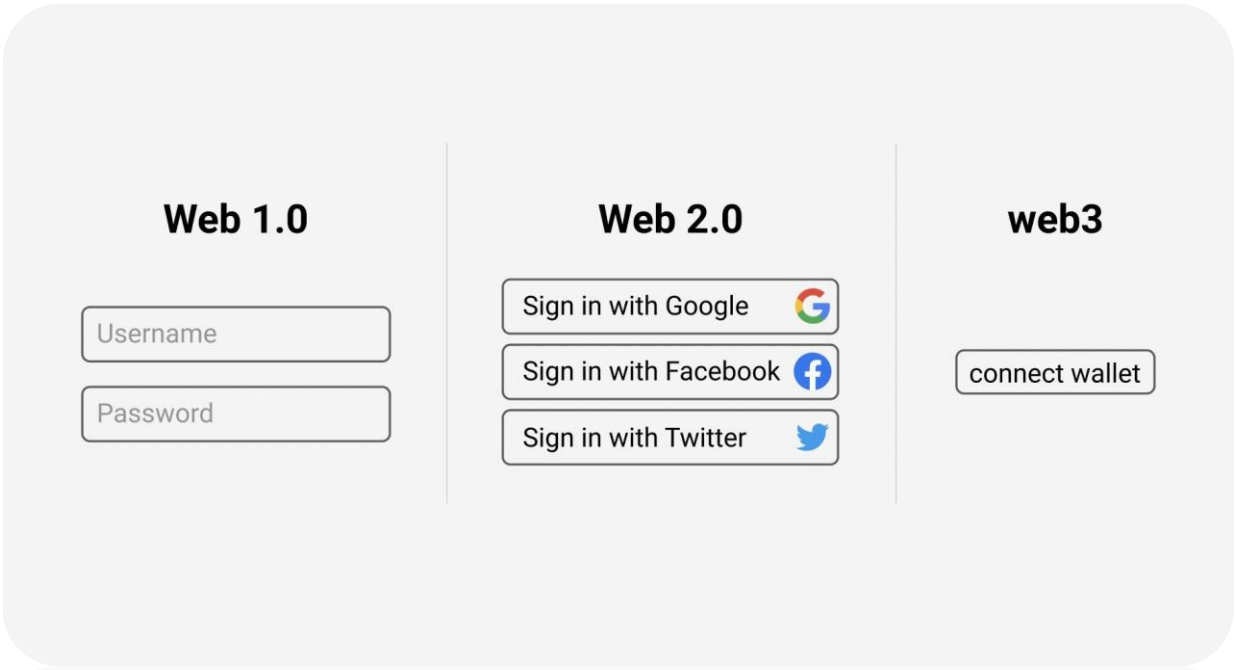
Annexe 9 : Cycle de tendance pour l'identité numérique (2022)



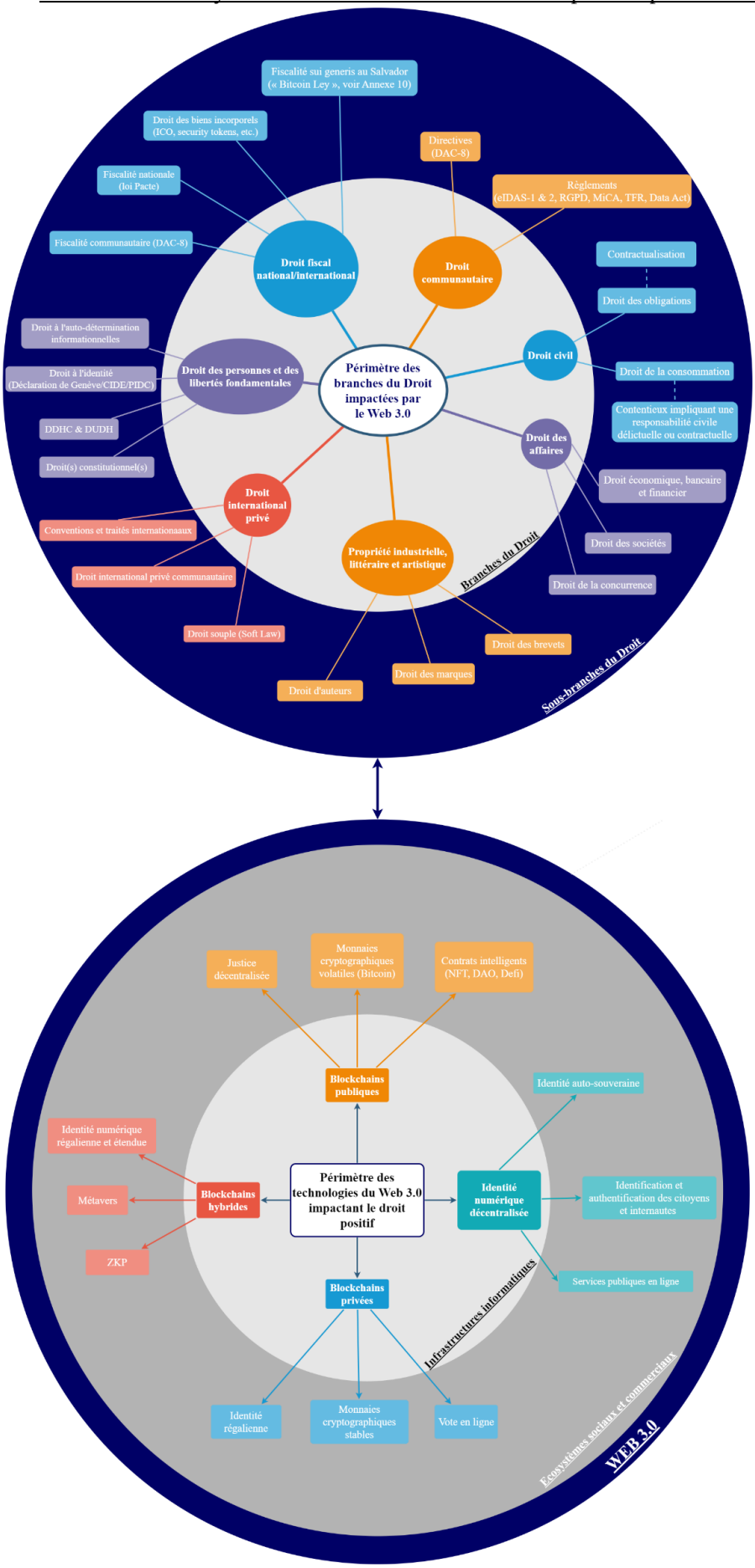
Annexe 10 : Le besoin d'une identité numérique régalienne pour les Français par cas d'usage



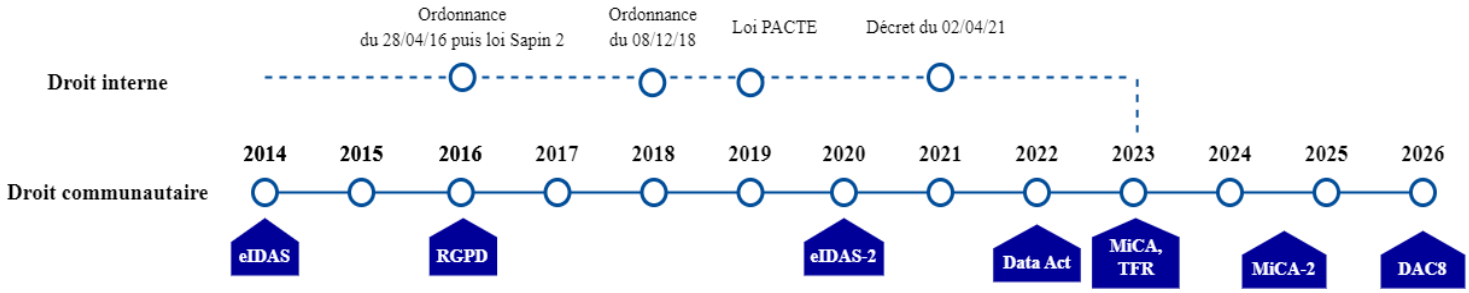
Annexe 11 : L’identité numérique 1.0, 2.0 et 3.0 résumée en une image



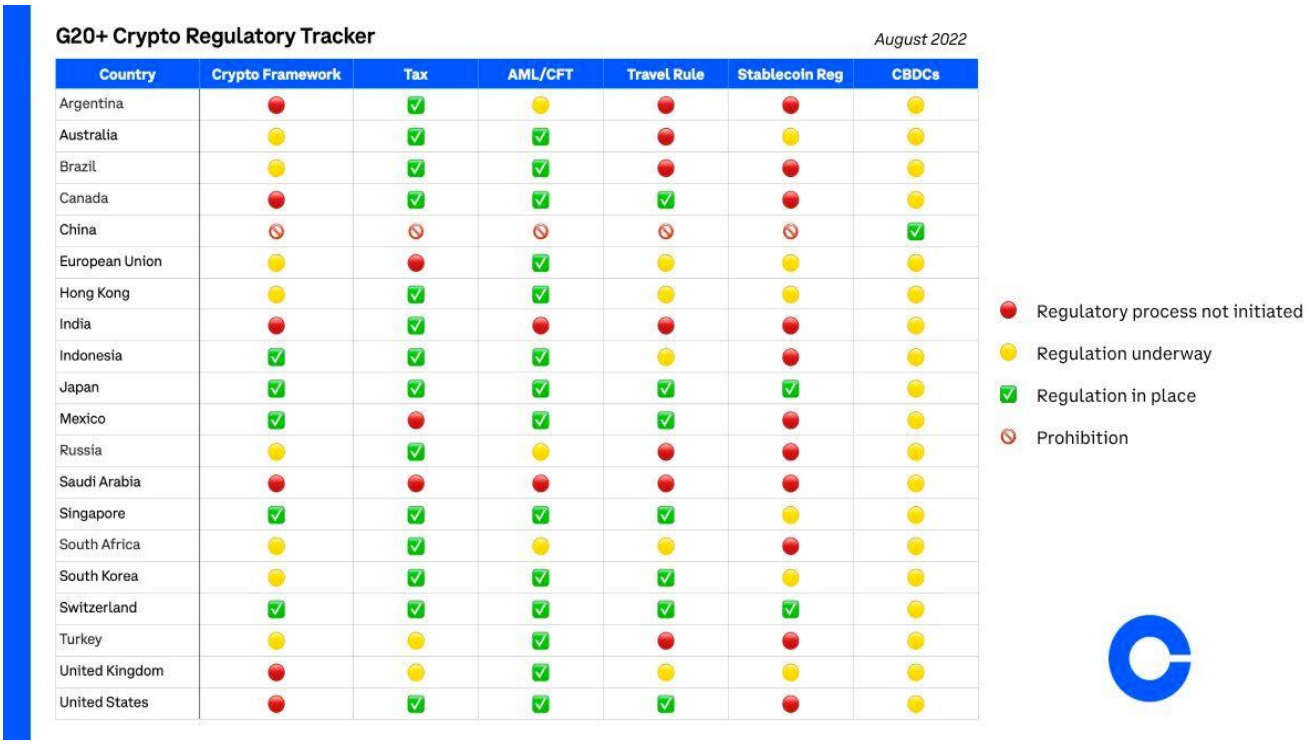
Annexe 12 : Analyse croisée des branches du droit impactées par le Web 3.0



Annexe 13 : Frise chronologique des textes internes et communautaires relatifs au Web 3.0



Annexe 14 : Etat règlementaire des crypto-actifs par pays du G20 (2022)



G20+ Crypto Regulatory Tracker *August 2022*

Country	Crypto Framework	Tax	AML/CFT	Travel Rule	Stablecoin Reg	CBDCs
Argentina	🔴	✅	🟡	🔴	🔴	🟡
Australia	🟡	✅	✅	🔴	🟡	🟡
Brazil	🟡	✅	✅	🔴	🔴	🟡
Canada	🔴	✅	✅	✅	🔴	🟡
China	🚫	🚫	🚫	🚫	🚫	✅
European Union	🟡	🔴	✅	🟡	🟡	🟡
Hong Kong	🟡	✅	✅	🟡	🟡	🟡
India	🔴	✅	🔴	🔴	🔴	🟡
Indonesia	✅	✅	✅	🟡	🔴	🟡
Japan	✅	✅	✅	✅	✅	🟡
Mexico	✅	🔴	✅	✅	🔴	🟡
Russia	🟡	✅	🟡	🔴	🔴	🟡
Saudi Arabia	🔴	🔴	🔴	🔴	🔴	🟡
Singapore	✅	✅	✅	✅	🟡	🟡
South Africa	🟡	✅	🟡	🟡	🔴	🟡
South Korea	🟡	✅	✅	✅	🟡	🟡
Switzerland	✅	✅	✅	✅	✅	🟡
Turkey	🟡	🟡	✅	🔴	🔴	🟡
United Kingdom	🔴	🟡	✅	🟡	🟡	🟡
United States	🔴	✅	✅	✅	🔴	🟡

🔴 Regulatory process not initiated
🟡 Regulation underway
✅ Regulation in place
🚫 Prohibition

Source : ARMSTRONG Brian, Président de la société Coinbase, 22 août 2022, in Twitter

Cette illustration présente les tendances législatives relatives aux crypto-actifs dans les pays membres du G20, avec une attention particulière sur la fiscalité (ci-dessus « *Tax* »). Bien que la plupart des pays aient pris des dispositions dans ce domaine, l'Union européenne semble en avance sur les États-Unis au regard de l'adoption de la proposition de Règlement MiCA et de la proposition d'amendement du Règlement TFR. Cependant, l'encadrement juridique des stablecoins et des MNBC est encore en cours de développement par la CE, comme étudié. La Chine préfère adopter pour l'instant une stratégie législative hostile envers les crypto-actifs. La Suisse, quant à elle, devient progressivement un pays incontournable pour les entrepreneurs de ce secteur. Dans l'ensemble, l'encadrement international du marché des crypto-actifs semble indiquer une adoption tumultueuse, mais progressive, par les agents économiques qui semblent se soumettre aux règles de droit en fonction de leurs stratégies commerciales.