Blockchain et identification numérique

Sophie Coutor, Christine Hennebert, Mourad Faher

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

BLOCKCHAIN ET IDENTIFICATION NUMERIQUE

Restitution des ateliers du groupe de travail « blockchain et identité » (BCID)

Co-auteurs et Comité de pilotage :

Pour le Ministère de l'Intérieur, Sophie COUTOR, *administratrice générale, en charge de la normalisation numérique.*

Pour l'IRT Nanoelec, Christine HENNEBERT, *PhD, experte au CEA-LETI en sécurité des systèmes embarqués.*

Pour Thales, Mourad FAHER, *Engineer Scientist/Fellow.*

Octobre 2020
Version 1.0

NANOELEC.

THALES
Building a future we can all trust

Co-auteurs et comité de pilotage

Sophie Coutor, haut fonctionnaire, est ancienne élève de l'Ecole Normale Supérieure. Entrée au ministère de l'Intérieur il y a plus de 30 ans, elle a occupé plusieurs postes de sous-préfet et a été détachée pendant quatre ans comme directrice des relations institutionnelles de Numéricable. En administration centrale, elle a occupé des postes très divers, du contentieux à la prospective, et a été pendant six ans directrice d'un important projet numérique régalien en lien avec les collectivités territoriales. Depuis 2015, elle suit, auprès du secrétaire général du ministère, les sujets de *blockchain*, d'identité numérique, d'intelligence artificielle et de cybersécurité sous l'angle de la normalisation et siège pour le compte du ministère de l'intérieur dans les instances de normalisation de l'Afnor et de l'ISO.

Christine Hennebert, ingénieure chercheuse, est experte en sécurité des systèmes embarqués au CEA LETI. Elle a travaillé sur plusieurs démonstrateurs de communication sans fil et sur des applications intégrées pour Network on Chips. Elle a participé à plusieurs projets européens visant à assurer la sécurité d'objets connectés et le respect de la vie privée des utilisateurs dès la conception. Elle s'intéresse actuellement à la technologie *blockchain* et aux *smart contracts* pour des applications telles que l'autoconsommation d'énergie ou la robotique pour l'industrie 4.0, dans le but d'assurer dès la conception la sécurité, la confidentialité, la confiance et la valeur. Elle participe au développement de dispositifs intégrant des composants matériels de sécurité pour communiquer avec une *blockchain* notamment au sein de l'IRT Nanoelec. Elle est auteure et co-auteure de plusieurs brevets et publications scientifiques internationales dans le domaine de la cybersécurité.

Mourad Faher, *Engineer Scientist/Fellow* chez Thales, a contribué activement ces vingt dernières années au développement de l'identité numérique et à sa sécurité, notamment à base de cartes à circuit intégrés, dans les comités normatifs (ISO, CEN/CENELEC, GlobalPlatform). Il est intervenu dans la conception et spécification d'instruments d'identification personnelle et de leur environnement respectif de déploiement à travers des projets mettant en œuvre des exigences sécuritaires et la protection de données personnelles. Il participe à la réalisation de solutions régaliennes sur dispositif mobile, et à leur généralisation pour des cas d'usages plus variés, qui s'appuient par exemple sur les technologies de vérification distribuées. Il est éditeur et co-éditeur de plusieurs normes internationales. Il compte plusieurs brevets à son actif.

Remerciements aux participants au groupe de travail « *blockchain* et identité » (BCID)

Par ordre alphabétique :

- **Michèle Abraham**, avocate du Cabinet Michèle Abraham,
- **Claire Anderson**, ANSSI,
- **Cécile Assie**, *Cybersecurity Strategy & Marketing Director*, Thales,
- **Raphaël Bartolt**, préfet honoraire, premier directeur de l'ANTS, consultant de l'imprimerie nationale,
- **Jean-Charles Bastoul**, ministère de l'intérieur, DNUM,
- **Julien Bringer**, directeur de Kallistech (*startup)*,
- **Sylvain Cariou**, directeur de CrystalChain (*startup*), président de la commission de normalisation *blockchain* à l'Afnor,
- **Laurent Castillo**, *Transversal Governance Director,* Thales,
- **Amélie Favreau**, maitre de conférence, HDR, Université Grenoble Alpes, Laboratoire CUERPI-CRJ,
- **Alban Féraud**, IDEMIA,
- **Romain Ferrari**, ingénieur étude et développement, Thales,
- **Sébastien Keller**, Architecte Logiciel, Thales,
- **Yves Lequerrec**, président du comité stratégique ICN à l'Afnor, La banque postale
- **François Lobbit**, préfet honoraire,
- **Marc Loutrel**, ministère de l'intérieur, DNUM, directeur technique du programme France Identité Numérique,
- **Christophe Ozcan**, directeur technique de Crypto4all *(startup),*
- **Rémi Ozcan**, directeur général de Crypto4all *(startup),*
- **Michel Papaud**, préfet, directeur général des services de l'agglomération Grenoble-Alpes Métropole,
- **Valérie Péneau**, inspectrice générale de l'administration, directrice du programme interministériel France Identité Numérique,
- **Jérôme Pons**, directeur de Music won't stop (*startup*),
- **Alain Roset**, conseiller du directeur du groupe La Poste,
- **Olivier Senot**, directeur de l'innovation numérique et des relations institutionnelles, Docaposte.

Résumé

Les deux concepts de *blockchain* et d'identité que nous examinons tout au long du document sont complexes. C'est pourquoi nous avons délibérément choisi d'introduire, préalablement à la discussion, de nombreux apports didactiques sur ces deux sujets. C'est l'objet du **chapitre 2** dans lequel nos deux « mascottes », **Alice & Bob, dialoguent et concluent quelques transactions** en toute sécurité grâce à la *blockchain*.

Dans le **chapitre 3**, nous constatons qu'en dépit de la numérisation des supports qui permettent de la décliner, **la notion d'identité reste juridiquement inchangée, qu'elle soit attestée par un support papier, un support numérique ou électronique et/ou un réseau électronique**. En discutant la notion d'identité « pivot » (le corpus minimal d'informations pour identifier une personne de façon universelle), nous soulignons la difficile émergence de la notion d'identité numérique, qu'il serait plus précis de désigner par l'expression « moyens d'identification électroniques sécurisés ». A travers l'examen des menaces et des impératifs de sécurité publique sur la numérisation de l'identité, nous étudions dans quelle mesure le développement de la technologie offre l'opportunité de surmonter la contradiction entre la protection des libertés individuelles et les nécessités de l'ordre public.

Notre **chapitre 4** présente les besoins d'identité lors de l'usage d'une *blockchain*, à travers **sept cas d'usages** qui vont de l'établissement de documents d'état civil non falsifiables à la gestion de l'auto-consommation d'énergie en copropriété. Pour chaque cas, nous discutons l'apport spécifique de la *blockchain* dans le processus. Ainsi, l'emploi d'une *blockchain* en complément d'autres infrastructures dans un système complexe **pourrait aider à dissocier identification et authentification**. Par l'usage du numérique, il s'agirait de reconnaitre des droits aux individus sans qu'ils aient besoin de justifier de leur identité, tout du moins tant qu'ils ne sont pas sujet d'un contrôle (contrôle aux frontières, contrôle routier…) par une autorité habilitée.

Au **chapitre 5**, nous rappelons les raisons pour lesquelles l'identité numérique est au cœur des enjeux de l'économie numérique : la détention des données personnelles des usagers constitue l'une des bases du modèle économique des géants du numérique. Néanmoins, pour l'instant, les écosystèmes d'identité existants sont assez peu adaptés aux nouveaux défis tels que la protection de la vie privée (RGPD), la mise en conformité avec les nouvelles régulations anti-fraude, ou encore avec la prévention du vol d'identité. Le concept d'identité auto-souveraine (*Self Sovereign Identity*, SSI) est une piste de réponse à ces défis. Supporté par une *blockchain* intrinsèquement sécurisée, il offre la faculté, de détenir et de contrôler la numérisation de son identité sans l'intervention d'une instance centralisant les données. Cette configuration n'exclut nullement le fait que l'identité juridique demeure garantie par l'Etat : elle permet seulement à l'individu de rester maitre de la communication de ses données personnelles dans un contexte autre qu'administratif et régalien, y compris en usant d'un pseudonyme.

Nonobstant ses atouts, dans quelles mesures la *blockchain* peut-elle s'intégrer dans l'environnement numérique existant ? C'est la question que nous instruisons au **chapitre 6**, par rapport à l'écosystème technique et juridique européen, aux services numériques déployés dans le cadre européens et nationaux (RGPD, eIDAS, FranceConnect). Nous indiquons notamment comment une infrastructure sécurisée fonctionnant sur *blockchain* pourrait gagner en crédibilité grâce à une qualification au titre des services de confiance selon eIDAS. L'Europe dispose d'un projet initié par le partenariat européen pour la *blockchain* (*European Blockchain Partnership*, EBP) : l'*European Blockchain Service Infrastructure* (EBSI).

En conclusion, nous proposons plusieurs actions à mettre en œuvre conjointement par les pouvoirs publics, les instances de normalisation, les ingénieurs et experts techniques et les centres de recherche.

Executive summary

The two concepts of blockchain and identity that we examine throughout the document are complex. This is why we have deliberately chosen, prior to the discussion, to introduce numerous didactic contributions on these two topics. In **chapter 2**, two parties talk to each other and conclude a few transactions in complete security thanks to the blockchain.

In **chapter 3**, one notes that despite the digital media that conveys it, the notion of identity remains legally unchanged, whether it is attested by a paper medium and/or a digital or electronic medium and/or an electronic network. When it comes to pivotal identity (i.e. the subset of attributes to identify a person), one underlines the difficult emergence of the notion of digital identity, which should rather be referred to as secure electronic means of identification.

Through an examination of the threats and public security requirements surrounding the digitalization of identity, chapter 3 investigates the extent to which the development of technology mitigates the contradiction between privacy and regulation.

Chapter 4 describes seven use cases relying on blockchain for identification spanning from the establishment of tamper resistant official documents to the management of self-consumption of energy in co-ownership. For each use case, we discuss the specific contribution of the blockchain in the process. Thus, the use of a blockchain as a complement to other infrastructures in a complex ecosystem could help to dissociate identification and authentication. By using digital technology, it would be a matter of conferring rights on individuals without their having to prove their identity, at least as long as they are not subject to control (border control, road control…) by an authorized authority.

Chapter 5 reiterates the reasons why digital identity is at the heart of digital economy challenges: holding of users' personal data is one of the foundations of the business model for dominant IT stakeholders. Nevertheless, for the moment, the existing identity ecosystems are not well adapted to new challenges such as the protection of privacy (RGPD), compliance with new anti-fraud regulations, or the prevention of identity theft.

The concept of Self Sovereign Identity (SSI) is one way of tackling these challenges. Supported by an intrinsically secure blockchain, it means the ability for transacting parties to own and control the digitalization of their identity without the intervention of a centric trusted third party or an administrative authority. This configuration in no way excludes the fact that legal identity remains vetted by the government: it enables the individual to control the disclosure of their personal data in a context other than administrative or institutional, including by using a pseudonym. This scheme makes the communicating parties interact in the digital world with the same confidence as in the physical world.

Despite its advantages, to which extent could the blockchain be integrated into the existing digital environment? This question is addressed in **chapter 6**, in relation to digital services deployed in the European technical and legal frameworks (RGPD, eIDAS, FranceConnect). For example, a secure infrastructure relying on a blockchain could gain credibility through qualification as a trusted service in terms of eIDAS requirements. The European Commission steers several projects initiated by the European Blockchain Partnership (EBP): the European Blockchain Service Infrastructure (EBSI) whose aim is to specify the cross-border public services at EU level.

As a conclusion, one propose several actions to be carried out by public instances, normalization bodies, engineer and technical experts and research centers.

Table des matières

Avertissements au lecteur :

A l'heure de la publication de ce Livre Blanc, la Commission Européenne a entrepris une consultation publique pour recueillir les avis sur les évolutions souhaitables du schéma d'identification eIDAS afin de faciliter les transactions transfrontières entre Etats Membres. Parmi d'autres, un ensemble de recommandations provenant d'Eurosmart peut être téléchargé[1]. La proposition d'Eurosmart porte sur un ensemble d'améliorations possibles se rapportant respectivement aux trois options privilégiées par la Commission. Cette consultation devrait durer jusqu'à fin Octobre 2020 voire début Novembre. Une évaluation complète du Règlement eIDAS doit être présentée au Parlement Européen fin 2020. En fonction de son contenu, un dialogue interinstitutionnel entre la Commission EU et le Parlement EU sera entrepris pour en faciliter l'adoption. Selon l'avancement des travaux, l'adoption finale d'une révision pourrait au plus tôt survenir au troisième trimestre 2021. Il importe aussi de savoir que les référentiels ANSSI utilisés dans ce Livre Blanc comme base de travail pour l'évaluation de la *blockchain* au regard des exigences du règlement eIDAS pour la qualification des services de confiance, sont en cours de révision par les experts de l'ANSSI.

Le travail présenté dans ce livre blanc reste perfectible malgré les efforts pour rendre compte de l'état de l'art dans le domaine de l'usage de la *blockchain* au service de l'identification numérique.

Pour les lecteurs généralistes, certains chapitres techniques peuvent se révéler ardus pour les néophytes.

[1] *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/F549006*

Avant-Propos

Le présent Livre Blanc est issu de la réflexion collégiale d'un groupe de travail associant des représentants du public et du privé, qui s'est réuni au ministère de l'intérieur de novembre 2018 à février 2020 afin de réfléchir aux usages de la technologie de la *blockchain* en lien avec l'identité. Ce groupe de travail intitulé « *Blockchain* et identité », (BCID), constitue une initiative originale, car comme toute institution administrative, le ministère de l'intérieur est peu coutumier des activités situées en marge de la conformité institutionnelle.

Pour autant, la création du BCID procède d'une juste compréhension du rôle de l'Etat-stratège, une compréhension modernisée par les défis de l'actualité que sont la mondialisation des enjeux et la numérisation de nos sociétés et de nos vies. Or, qui dit stratégie nationale et projection dans l'avenir dit concertation avec les forces vives de la nation que sont les centres de recherche et les entreprises.

L'intérêt du ministère de l'intérieur pour cette démarche tient à son implication dans une conception opérationnelle de la souveraineté. Il est particulièrement important que toute révolution technologique en cours soit évaluée en fonction des atteintes qu'elle est susceptible de porter à l'incarnation de la souveraineté nationale, ou à l'inverse, en fonction des facilités qu'elle peut lui procurer.
Aussi, le BCID s'est-il donné pour mission implicite de mettre au jour des cas d'usage fonctionnant par interfaçage d'une *blockchain* avec la future carte nationale d'identité électronique, la CNIE.
Dans ce cadre, l'implication du ministère de l'intérieur tient surtout aux caractéristiques de la *blockchain* qui nous permettrait d'échapper à une aporie, source de nombreux affrontements sociétaux, entre la sécurité publique et la protection de la vie privée ainsi que des données personnelles.

Car, au-delà de l'aspect technologique, la disruption qui pourrait être apportée par la *blockchain* est sociétale, voire philosophique : elle consiste à replacer l'individu au cœur de sa projection numérique, en lui garantissant la libre communication des éléments de son choix, dans le respect des prérogatives régalienne.

L'objectif est bien de concilier harmonieusement les impératifs de sécurité publique et le respect de la vie privée des individus, en garantissant à chaque personne physique ou morale la maitrise des informations la concernant, dans le respect des impératifs de l'Etat de droit.

C'est tout l'enjeu du concept d'identité autogérée, ou d'« autodétermination informationnelle » (ou encore *Self Sovereign Identity* en anglais[2]*)* qui fait l'objet de développements dans le corps de ce Livre Blanc.

La *blockchain* peut également revêtir une grande importance en matière de souveraineté numérique ; en effet, elle permet par construction de réserver les échanges autour d'un cas d'usage à un public autorisé.

Outre sa fonction exploratoire, ce Livre Blanc se veut également didactique.

Que la *blockchain* soit souvent évoquée comme un mot à la mode ne doit pas nous faire ignorer ses particularités : pour le non initié, il est très difficile d'avoir une représentation mentale de la *blockchain* : à cause de la complexité de l'objet technique lui-même, mais aussi à cause de la multiplicité des formes revêtues par cette technologie, substantiellement différentes les unes des autres. Cette diversité rend d'autant plus difficile la vulgarisation du concept et son appropriation par les décideurs.

[2] Le concept universellement connu sous le nom de *Self Sovereign Identity* a pour origine un concept allemand qui traduit en français, devient « autodétermination informationnelle ». On lui préfère généralement dans notre langue la formule d'« identité autogérée ».

Car ce sont bien les « décideurs » qu'il convient d'acculturer à cette notion aussi globale que disruptive. Le présent Livre Blanc, composé sous l'égide du ministère de l'intérieur, a pour objectif essentiel de fournir des représentations mentales susceptibles de leur inspirer des usages en lien avec l'identité qui garantissent le niveau de sécurité le plus exigeant de l'identification. Les destinataires du Livre Blanc sont bien évidemment les fonctionnaires d'Etat, et, dans un premier temps, tous ceux du ministère de l'intérieur, mais aussi les décideurs du monde de l'entreprise, car ce Livre Blanc se veut aussi un appel à l'imagination, un ferment de créativité pour tous.

La vulgarisation du concept prend une dimension stratégique en facilitant son appropriation au sein de la collectivité nationale, ce qui explique l'empirisme de la démarche suivie et la focalisation sur les cas d'usage.

Il est à l'honneur du ministère de l'intérieur de s'être emparé de cette mission.

Jean-Benoit Albertini,
Secrétaire Général du ministère de l'intérieur

Le mot de l'IRT Nanoelec

Les technologies au service de la confiance

Depuis sa création en 2012, l'Institut de Recherche Technologique Nanoelec[3] est devenu un acteur notable de la filière semi-conducteur, unique en France dans son approche multi-partenariale au sein du secteur électronique et fédérant les efforts des acteurs clés du domaine autour d'axes technologiques structurants. Pour conduire son action, l'IRT Nanoelec s'appuie sur un réseau solide de partenaires industriels et académiques. Ses programmes technologiques mis en œuvre depuis maintenant 7 ans commencent à impacter directement l'activité des fabricants de composants ou d'équipements.

La confiance numérique est désormais un enjeu de société capital. L'avènement d'un monde hyper connecté et les potentialités ouvertes par les nouvelles technologies numériques rendent possibles la mise en place de nouveaux services permettant selon les cas d'optimiser l'efficacité énergétique des bâtiments, accompagner les personnes âgées en perte d'autonomie, automatiser certaines fonctions critiques en mobilité ou dans les usines. La performance de ces services repose sur la qualité des données, généralement produites dans des objets miniaturisés et communicants, et qui une fois transférées, agrégées et traitées permettent de prendre les bonnes décisions. Tout au long de la chaîne informationnelle, il est essentiel de garantir que ces données soient authentiques et non altérées, avec parfois la nécessité de les chiffrer afin de préserver la vie privée des personnes.

La valeur de ces données renforce l'intérêt des pirates qui essaient de les voler, les espionner ou les altérer et il devient indispensable de les protéger et d'en assurer la traçabilité. La technologie *blockchain* a émergé ces dernières années comme une technologie numérique à fort potentiel dans ce domaine et de premières applications ont percé dans les domaines de l'agroalimentaire et de la finance. Mais si la *blockchain* est parfaitement adaptée aux données dématérialisées, son utilisation sécurisée au service de l'internet des objets reste encore un champ de recherche pour comprendre les fonctionnalités à intégrer dans les composants électroniques.

Avec ses partenaires, Nanoelec s'est investi dans le domaine au sein de son programme technologique PULSE[4]. Ses experts ont ainsi réalisé plusieurs démonstrateurs, dont un de « Smart Robotique » permettant d'étudier l'intérêt d'une *blockchain* pour tracer les actions et les responsabilités d'opérateurs de robot industriel. En parallèle, ils ont apporté leur expertise en sécurité matérielle au groupe de travail AFNOR TC307 pour la normalisation de la *blockchain* aux normes internationales (ISO), ainsi qu'au BCID, un groupe de travail dédié à l'étude de la mise en œuvre de la *blockchain* dans les applications d'identité numérique. Ces travaux font l'objet du présent Livre blanc.

En publiant cette synthèse, conjointement avec le ministère de l'Intérieur et Thales, Nanoelec montre sa capacité à être un trait d'union entre le secteur public et le secteur privé, et à conduire des travaux de recherche de ruptures aux frontières des mondes du logiciel et des composants électroniques. Les développements menés au sein de Nanoelec, dont les solutions examinées dans ce Livre blanc peuvent aussi bénéficier d'une large diffusion technologique à travers le programme de dissémination de l'IRT et ses deux outils (Easytech pour les ETI et PME, System Lab pour l'innovation ouverte). Notre ambition est de partager les apports de ces travaux le plus largement possible.

Hughes Metras,
Directeur de l'IRT Nanoelec

[3] L'IRT Nanoelec est mis en place par le gouvernement dans le cadre du programme aux investissements d'avenir, et est opéré par le CEA-LETI.

[4] Le programme PULSE étudie comment les nouvelles technologies peuvent renforcer la confiance dans le numérique en apportant des solutions aux enjeux de sureté et cybersécurité, mais également d'ergonomie, un des grands défis pour l'acceptabilité et la simplification des déploiements de la cybersécurité.

Le mot de Thales

La confiance est essentielle au développement de nos sociétés, dans un monde où tout est connecté et où mobilité et nomadisme sont la norme.

Chez Thales, nous transformons les technologies les plus innovantes en solutions créatives, résilientes, sécurisées et fiables pour permettre à nos clients d'affronter leurs défis et le monde de demain : transports connectés, passages aux frontières dématérialisées, protection des données sensibles et souveraines…

C'est dans cette logique que Thales a investi il y a plusieurs années déjà, dans la technologie *blockchain* y voyant un intérêt pour la traçabilité et la non répudiation dans des écosystèmes où interviennent plusieurs parties prenantes, et présentant des enjeux économiques voire même vitaux quand il s'agit de valider la chaine de production de médicaments ou chaine alimentaire : provenance des composants, opérations effectuées, transports réalisés, horodatage…

Avec le clair besoin de souveraineté numérique, l'identité dématérialisée doit faire naturellement l'objet de toutes les attentions et précautions due à l'intensification de la cybercriminalité, et en particulier de l'usurpation de l'identité. L'examen des solutions de vérification d'une telle identité offre un panel de choix technologiques parmi lesquels une technologie comme la *blockchain* peut faire sens quand les conditions pour son usage sont remplies. On est ici en droit de s'interroger sur la manière dont la *blockchain* s'inscrit dans un concept comme celui de la territorialité numérique. La *blockchain* laisse en effet entrevoir des questions nombreuses et pertinentes que ce Livre Blanc a tenté d'adresser.

Avec le recul nécessaire, on pourra à court terme tirer les conclusions d'une telle solution pour la mise en œuvre d'une identité forte dématérialisée, au regard des services qu'elle aura rendu et surtout des ajustements qui auront été nécessaires pour son adoption par ses multiples usages et usagers. Ce Livre Blanc dessinant les lignes fortes de réflexion sur ce sujet avec les dépositaires même de l'identité était un impératif pour bien éclairer les avantages et exigences du choix de cette technologie sans occulter les alternatives.

Marc Darmon,
DGA de Thales et Président du CSF

Glossaire de la *blockchain* et de l'identité

Assertion

Enoncé ou déclaration portant sur un attribut d'identité qualifié juridiquement de « donnée personnelle », pouvant se présenter sous la forme d'un document authentique, considéré comme « vrai ». L'assertion accompagnée d'une (ou de plusieurs) **preuve**(s) permettant sa vérification est dite « vérifiable ». La validité d'une assertion peut être vérifiée sur une *blockchain*.

Attestation

Justificatif « fait pour valoir ce que de droit », délivré par un organisme habilité authentifiant des informations et ayant valeur de **preuve**. La vérification de cette preuve peut être effectuée en s'appuyant sur la *blockchain*.

Attributs d'identité

Elément caractéristique d'une personne, qualifié juridiquement de « **donnée personnelle** » ou de « **donnée à caractère personnel** », susceptible d'être utilisé pour authentifier cette personne (au sens, soit de confirmer son identité, soit de la faire reconnaitre comme détentrice d'un droit). Sont par exemple considérés comme attributs d'identité le nom de naissance, la couleur des yeux, l'âge, l'adresse de résidence ou l'obtention d'un diplôme. Certains attributs comme la date et le lieu de naissance sont invariants, tandis que d'autres tels que la taille ou l'adresse de résidence varient au cours du temps. Dans le cadre de la protection de la *privacy* (protection de la vie privée et des données personnelles), l'utilisation d'attributs d'identité est particulièrement encadrée. Les attributs d'identité sont conservés par l'utilisateur et ne sont jamais enregistrés en clair sur la *blockchain*.

Authentification

Opération consistant à produire l'existence d'une confirmation ou d'un élément sur un support quelconque pour attester d'un droit et en faire reconnaitre la légitimité. Cette opération peut être réalisée par la production d'un document ou d'un jeton (tous deux ayant alors valeur d'autorisation). Le document ainsi produit peut lui-même faire l'objet d'une authentification pour attester la légitimité de son origine et son intégrité.

Dans un contexte électronique, la définition retenue par le règlement européen eIDAS (article 3, alinéa 5) fait de l'authentification « 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 ». Il arrive que l'on utilise l'expression « d'authentification d'une personne » au sens de la confirmation de l'identité produite par cette personne ; dans ce cas « l'authentification » doit être interprétée seulement comme la « confirmation » de l'identification alléguée, ainsi que le formule explicitement le règlement eIDAS. Actuellement, dans le domaine de l'identification, l'authentification est souvent considérée comme la capacité de confirmer par la biométrie que le titre physique est bien attaché à la personne physique qui le présente.

Mais, au sens propre, l'authentification d'une personne devrait être réservée, à la reconnaissance d'un droit à son profit : par exemple, une personne a le droit d'acheter de l'alcool en ligne si elle s'authentifie comme majeure. Il n'y a pas de nécessité de dévoiler son identité et un des avantages de la *blockchain* consiste à **dissocier l'authentification de l'identification** (par la seule production d'éléments attestant de son droit, sans référence à un élément susceptible de l'identifier).

Bloc

Ensemble de données incluant des transactions, structuré en vue d'un enregistrement périodique. Le bloc contient un en-tête, une structure d'empreintes cryptographiques garantissant l'intégrité de son contenu, les *smart contracts* sous forme compilée, les transactions, et les données, ainsi que son maillage avec le bloc précédent.

***Blockchain* ou « chaîne de blocs »**

On appelle *blockchain* la suite de transactions organisées en **blocs** qui relie le **bloc** « genèse » au **bloc** le plus récent [1]. Cette « chaîne de blocs » est donc constituée d'un historique de **transactions** horodatées cohérent sur lequel tous les **nœuds** (tous les ordinateurs composant le réseau qui sert de support à la *blockchain*) doivent s'accorder. Cette chaîne constitue le registre (*ledger*) de la *blockchain*. Dans le texte de l'ordonnance [2] du 28 avril 2016 relative aux « minibons », qui contient la première mention juridique française d'une « chaîne de blocs », la *blockchain* est définie comme « un dispositif d'enregistrement électronique partagé permettant **l'authentification** de ces opérations ».

Blockchain « permissioned »

Blockchain où la participation au mécanisme de **consensus** est soumise à autorisation préalable délivrée par les autorités qui assurent la **gouvernance** de la *blockchain*.

Blockchain « permissionless »

Blockchain où la participation au mécanisme de consensus n'est soumise à aucune autorisation préalable.

***Blockchain* privée**

Seuls les membres ou utilisateurs autorisés peuvent accéder au registre distribué. La nature, le statut, ou l'identité des participants à la *blockchain* sont déterminés dès l'origine.

***Blockchain* publique**

La *blockchain* publique est conçue pour que tout le monde soit en mesure d'accéder au registre distribué, moyennant une éventuelle **authentification**. C'est le modèle retenu dans la plupart des *blockchains* dédiées à la création de crypto-actifs. Elles sont généralement ***permissionless***.

Bytecode

Le *bytecode* correspond à la description du *smart contract* sous forme binaire. Il est enregistré dans un **bloc** par l'intermédiaire de la transaction dédiée à son déploiement.

Consensus

Accord des différents **nœuds** du réseau sur la validité des données et des transactions qui détermine leur incorporation à la fin du registre dans le **bloc** en construction, selon une périodicité préalablement déterminée.

Ce consensus obtenu sur l'état du registre, est régi par des règles et des procédures communes partagées entre les nœuds du réseau pair-à-pair, selon une périodicité déterminée, y compris en présence de nœuds défaillants. Il existe plusieurs types de mécanismes de consensus selon le protocole utilisé : le *Proof of Work* (PoW), *le Proof of Stake* (PoS), le *Proof of Authority* (PoA), le *Proof of Elapsed Time* (PoET)…

Crypto-actif
Actifs virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement d'effectuer des transactions sans avoir à recourir à une monnaie légale.

dApp
Une application orchestrée par des *smart contracts* enregistrés dans une ***blockchain*** est appelée une *dApp* pour Application distribuée.

Document source
Titre ou document authentique délivré par un organisme habilité comme une préfecture, une mairie, une compagnie d'assurance, une banque… Sur les sujets d'identité, le document source par excellence est l'acte de naissance, qui est à l'origine de la confection du passeport, de la carte nationale d'identité et de tous les autres documents ou moyens d'établir son identité.

Données à caractère personnel ou « données personnelles »
Toute information se rapportant à une personne physique identifiée ou identifiable. Les **attributs** d'identité et les documents sources sont des données à caractère personnel (ces dernières peuvent aussi être considérées comme la matérialisation de ces données sur support papier ou électronique). Des informations techniques telles que le numéro de téléphone, les adresses IP, les diverses traces laissées sur les réseaux sociaux sont également considérées comme des données à caractère personnel. Les **données d'identité pivot** font parties des données à caractère personnel.

Ces données doivent être protégées pour défendre l'individu auxquelles elles se rapportent des diverses agressions que sont les identifications intempestives (atteintes à la vie privée), les usurpations d'identité (atteintes aux biens et à la réputation), et les profilages (atteintes au libre arbitre par conditionnement).

Données « pivot »
Cf. **Identité « pivot »**.

Empreinte
Suite de bits de longueur déterminée, résultat d'une fonction de hachage. L'empreinte numérique est le condensé d'une donnée ou d'un ensemble de données. Ici, le terme « empreinte » ne fait pas référence à une empreinte dactyloscopique.

Enrôlement
Enregistrement d'une personne physique ou morale dans la liste des utilisateurs pouvant s'authentifier sur un système.

Fonction de hachage
Fonction mathématique à sens unique, utilisée en informatique et en cryptographie pour calculer l'**empreinte** de données afin de garantir leur intégrité, ne permettant pas de remonter à la donnée d'entrée.

Fork (ou « embranchement »)
Division de la ***blockchain*** (fortuite ou intentionnelle) en deux (ou plusieurs) branches, chacune partageant l'historique commun mais divergeant sur les nouvelles règles de validation d'un **bloc** :

- **Hard fork** : les règles et procédures de mise à jour sur la branche la plus longue ne sont pas rétro-compatibles avec les anciennes règles (avant le *fork*).
- **Soft fork** : les règles et procédures de mise à jour sur la branche la plus longue sont rétro-compatibles avec les anciennes règles (avant le *fork*).

Fournisseur d'identité
Organisme public ou privé fournissant un moyen d'**authentification** et sa garantie aux utilisateurs pour l'accès à des biens ou des services sur Internet.

Gouvernance
Règles et procédures permettant de prendre des décisions quant à l'évolution et à la maintenance du système distribué ou encore de déterminer le contour des rôles des acteurs.

Quand le terme de gouvernance désigne la charte établie par les fondateurs d'une ***blockchain*** et en charge de veiller à son maintien en condition opérationnelle, on emploie alors aussi l'expression de « directoire » d'une ***blockchain***.

Identifiant décentralisé (DID)
Identifiant généré par l'utilisateur et utilisé pour s'authentifier en ligne afin d'accéder à un service distant. Dans le cas d'une ***blockchain***, l'identifiant décentralisé peut être l'adresse de compte de l'émetteur.

Identité pivot
Notion apparue lors de la numérisation de l'identité. Il s'agit des caractérisations minimales de la personne physique que l'on retrouve dans les trois documents fondamentaux en droit français, l'acte de naissance, la carte nationale d'identité (dont les mentions identifiantes sont énumérées dans la loi du 27 mars 2012 relative à la protection de l'identité) et le passeport.

On peut désormais ajouter à ces trois sources nationales, l'énumération de « l'ensemble minimal de données pour une personne physique » figurant dans le règlement d'exécution (UE) 2015/1501 du règlement européen eIDAS, et l'arrêté du 8 novembre 2018 relatif au « téléservice » FranceConnect, lequel énumère les données obligatoires à renseigner pour accéder au service. Les données situées à l'intersection de ces cinq documents ou titres, bien que variant à la marge, peuvent être considérées comme le « noyau identifiant » de la personne physique auquel on donne le nom de « données pivot ».

On considère généralement que ces éléments suffisent pour discriminer les personnes avec précision. Il s'agit du nom, du ou des prénoms, du lieu et de la date de naissance et de la nationalité. La réglementation européenne y joint le numéro d'identification unique, ce qui suscite des réserves dans notre pays. La notion « d'identité pivot » n'étant pas définie juridiquement, on y ajoute parfois le sexe, toujours susceptible d'être considéré comme donnée sensible (et évolutive) dans certaines circonstances.

Identité numérique
Cette expression n'est pas attestée dans les textes juridiques ; le règlement européen eIDAS, lui préfère « identification électronique » et le décret du 1er aout 2018 pris pour l'application de la loi informatique et liberté utilise l'expression « données d'identité numériques ». Le grand succès de cette expression dans la vie quotidienne ne doit pas nous dissimuler qu'il n'existe pas d'identité numérique à proprement parler, mais seulement la faculté de transcrire des éléments d'identité sur un support numérique, lequel permet de remonter à l'identité juridique. En dépit de sa consécration par l'usage, il serait plus précis d'employer l'expression « moyens d'identification électroniques sécurisés » pour désigner les différents supports numérisés utilisés pour s'identifier en ligne ou dans le monde physique (lors de franchissement de frontières par exemple). De ces moyens d'identification électroniques sécurisés peuvent être dérivés des **identifiants décentralisés** (DID). L'expression « identité numérique » est indifféremment utilisée pour des personnes physiques ou morales.

Identification

Opération consistant à identifier une personne, c'est-à-dire, dans le langage courant, à la nommer à l'aide de ses nom et prénoms usuels. Selon la loi française, l'identité se prouve par tous moyens, et la détention d'une carte nationale d'identité (CNI) n'est pas obligatoire. Pour autant, dans la pratique, cette identification est réalisée avec une certitude suffisante par la production de deux titres, le passeport ou la carte d'identité (cette dernière, bientôt électronique). Mais dans de nombreux contextes jugés moins sensibles, la production de n'importe quel titre administratif avec photo peut suffire. L'ordonnance du 4 novembre 2017 prévoit de mettre sur le même plan que la CNI et le passeport un « moyen d'identification électronique », mais en l'absence de décret d'application, cette faculté ne fait pas partie du droit positif à ce jour. Les deux défis posés par l'identification sont, d'une part, celui de l'univocité de l'identification, un individu renvoyant à une identité et une seule, et vice versa (sujet qui incite à l'utilisation de la biométrie, et surtout de l'identité génétique), et, d'autre part, la protection de l'individu contre les identifications intempestives (lesquelles, à l'inverse, prescrivent d'encadrer scrupuleusement l'utilisation de la biométrie et de la génétique).

La notion d'identification renvoie aux notions de données d'**identité pivot**, ou données pivot ou identification pivot, de **données personnelles**, d'**authentification** et d'**individualisation**.

Individualisation

Les auteurs de la présente étude proposent de distinguer le concept « d'individualisation » du concept plus global **d'identification**. Si l'identification consiste à nommer quelqu'un, l'individualisation consiste simplement à le discriminer par rapport à un ensemble, par exemple un internaute est individualisé par un pseudonyme, ou un individu est repéré par son attitude ou son habillement sur un enregistrement vidéo. Dans les deux cas, la personne est « individualisée », repérée ; pour autant, elle n'est pas identifiée tant qu'elle n'est pas nommée. On peut considérer que, dans la plupart des cas, l'individualisation constitue une étape préalable à l'identification, mais cela n'est pas toujours le cas, et il parait préférable de distinguer les deux opérations, juridiquement et techniquement.

Message

Ensemble de données émis depuis un dispositif vers un autre dispositif généralement distant, comportant un en-tête et une charge utile avec les données à transmettre.

Minage

Activité numérique liée à la notion de preuve de travail (ou *Proof of Work*, PoW) introduite par la ***blockchain*** Bitcoin, consistant à construire, puis à relier les nouveaux **blocs** à la chaîne existante. Le minage est utilisé par un grand nombre de ***blockchains*** « *permissionless* » ; il consiste à résoudre un défi de « force brute »[5] cryptographique.

Cette activité nécessite des ressources importantes en calcul et en énergie. On parle alors de ressource de minage.

Mineur

Machine, appelée « **nœud** de réseau », qui effectue une activité de **minage** avec une preuve de travail (ou *Proof of Work*, PoW).

Mintage

Activité numérique liée à la notion de preuve d'enjeu (ou « *Proof of Stake* », PoS), consistant à construire, puis à relier les nouveaux **blocs** à la chaîne existante, en gageant une somme de **crypto-actifs** pour être autorisé à soumettre un nouveau **bloc** au **consensus**. A noter que la terminologie n'est

[5] On appelle « force brute » un calcul qui ne peut pas être simplifié par un algorithme et qui donne lieu à des itérations systématiques jusqu'à découverte d'un secret ou l'obtention d'un résultat

pas encore totalement fixée. Dans ce rapport, les auteurs ont fait le choix de désigner par le terme « *mintage* » une validation opérée grâce à une preuve ne requérant pas une dépense excessive d'énergie, comme par exemple une preuve d'autorité (« *Proof of Authority* », PoA), ou encore une preuve du temps écoulé (« *Proof of Elapsed Time* », PoET). On utilise aussi parfois le mot « forgeage ».

Minteur
Machine, appelée « nœud de réseau », qui effectue une activité de **mintage** avec une preuve d'enjeu (« *Proof of Stake* », PoS), voire toute autre catégorie de preuve autre que la preuve de travail (« *Proof of Work* », PoW).

***Incentive* (ou « Incitation »)**
Dans certaines catégories de ***blockchains*** (telle que la *blockchain* Bitcoin), la motivation désigne la perspective d'une récompense obtenue par le **mineur** qui a trouvé le premier une solution au défi cryptographique posé pour valider un **bloc** donné. Cette récompense peut être fournie sous la forme de **crypto-actifs**.

Nœud
Elément du réseau de pair-à-pair qui coopère au fonctionnement du système en validant l'accrochage des nouveaux **blocs** à la chaîne. Il s'agit de matériel informatique connecté au réseau, ordinateur, groupe d'ordinateurs, serveurs, téléphones, équipés de fonctionnalités et de capacités de calcul et de mémorisation spécifiques pour opérer cette validation. Certains nœuds bénéficient par surcroît de fonctionnalités qui leur permettent de créer de nouveaux **blocs**.

Off-chain
Elément d'un système de ***blockchain*** localisé, opérant hors du registre distribué.

On-chain
Elément d'un système de ***blockchain*** enregistré, opérant dans un registre distribué.

Oracle
Lien interface de la ***blockchain*** avec une source de données provenant du monde physique réel pour intégration dans le monde numérique virtuel de la ***blockchain***.

Prestataire de service
Organisme public ou privé proposant un service accessible en ligne.

Preuve
Elément indiscutable (différent en cela de l'« indice » ou de la « présomption ») servant à authentifier une ou plusieurs propriétés se rapportant à une personne ou à des données (ou **assertions**) : intégrité de l'information, authenticité des données, **authentification** de l'utilisateur ou d'un détenteur de document, **identification** d'une personne physique ou morale… Importante en informatique, cette notion est fondamentale pour la ***blockchain*** dont le fonctionnement repose sur un **consensus** entre machines (entre **nœuds** ou pairs) obtenu grâce à un algorithme dont le calcul sert de preuve (*PoW*, *PoS*, *PoA*, *PoET*…).

Registre (*ledger*)
Enregistrement chronologique d'une suite de données ou de transactions dont l'intégrité et l'ordonnancement sont immuables (non modifiables).

Registre distribué
Un registre distribué est un registre répliqué, synchronisé et partagé entre les différents **nœuds** d'un réseau distribué. Le propre de la ***blockchain*** consiste précisément à assurer ces fonctionnalités entre pairs. Cf. ***Système distribué***.

Smart Contract
Code informatique enregistré dans une ***blockchain*** dont l'exécution est déclenchée par une transaction et dont le résultat est soumis au **consensus** des **nœuds** validateurs avant enregistrement dans le nouveau **bloc**. L'exécution d'un *smart contract* se déroule automatiquement dans un environnement d'exécution fourni par la ***blockchain***. Le *smart contract* n'a rien d'un contrat au sens juridique du terme, même s'il peut, le cas échéant, être utilisé pour transcrire juridiquement une clause juridique afin de l'exécuter de façon automatique.

Système distribué
Ensemble d'ordinateurs indépendants (encore dénommés **nœuds** ou « pairs ») formant un réseau de pair-à-pair qui apparaît à un utilisateur comme un système unique, cohérent et synchronisé [3].

En effet, la caractéristique d'une ***blockchain*** est de fonctionner de façon distribuée ou « décentralisée », au contraire d'un système centralisé traditionnel qui fonctionne sous le mode « client-serveur », ou d'un système fédératif dans lequel des systèmes centralisés sont reliés par des passerelles (*« Gateway »)* afin de leur permettre d'échanger.

Token
Représentation numérique d'un actif ou d'un droit (par exemple, le droit d'accès à une information).

Transaction
Format de données émis depuis un compte de portefeuille, soumis au **consensus** pour être enregistré dans un **bloc.** Une transaction est à destination soit d'un autre compte de portefeuille, soit d'un ***smart contract***, et peut comporter un paiement sous la forme de **crypto-actifs**.

Vérificateur
Organisme public ou privé habilité à vérifier la validité, la véracité, l'intégrité et l'authenticité des **attributs** d'identité, **assertions** vérifiables et/ou des documents sources présentés par un utilisateur pour accéder à un service en ligne.

Validateur
Nœud participant au **consensus**, émettant un vote sur la validité des données et **transactions** incluses dans le nouveau **bloc** soumis au **consensus**. Le validateur ne dispose pas nécessairement de ressources de **minage**, c'est-à-dire qu'il n'est pas nécessairement en mesure de construire et soumettre au **consensus** un nouveau **bloc**, en revanche il détient une copie complète du **registre** (*ledger*).

***Zero Knowledge Proof* (preuve à divulgation nulle de connaissance)**
Méthode cryptographique permettant de fournir une **preuve** vérifiable de détention d'une donnée sans la révéler.

Dictionnaire des acronymes

Alicem : Authentification en LIgne CErtifiée sur Mobile

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CNI : Carte Nationale d'Identité

CNIe : Carte Nationale d'Identité électronique

CNIL : Commission Nationale de l'Informatique et des Libertés

DID : Decentralized IDentity (identité décentralisée)

eIDAS : *Electronic IDentification Authentication and trust Services* (identification, authentification électronique et services de confiance)

RGPD : Règlement Général sur la Protection des Données à caractère personnel [9]

RGS : Référentiel Général de Sécurité [10]

SSI : *Self-Sovereign Identity* (identité auto-souveraine)

1. Introduction

Quels pourraient être les apports de la *blockchain* à la gestion et à la protection de l'identité dans le contexte du développement exponentiel des usages numériques ? C'est la question que nous avons choisi d'instruire dans le présent Livre blanc.

L'identité des personnes physiques est un sujet sensible dont le traitement relève de la souveraineté nationale. Sa numérisation doit s'appréhender conformément à notre état de droit, dans le respect de notre culture administrative et politique.

Une réflexion sur la numérisation de l'identité nécessite de revenir aux fondements de l'identité en France, et aux évolutions successives qui jalonnent l'usage de l'« identité électronique » dans notre pays. Aujourd'hui, les utilisateurs sont très attentifs à la protection de leurs données personnelles et à la préservation de leur intimité. De son côté, l'Etat est incité par la règlementation européenne à déployer des solutions « d'**identité numérique** », fournissant un niveau de sécurité élevé pour déjouer les cyberattaques. Concilier les attentes légitimes de discrétion des utilisateurs dans le monde numérique, tout en permettant à l'Etat d'assurer son rôle de protection, de régulation et de contrôle, relève d'un défi multiforme, à la fois technologique et juridique.

La mise en œuvre de la technologie *blockchain* peut contribuer à relever ces défis, en observant dans le même temps que tout déploiement d'une *blockchain* nécessite de traiter l'**identification** des émetteurs et des destinataires. Ces observations conduisent à s'intéresser à la *Self-Sovereign Identity*, ou autodétermination informationnelle, comme une solution susceptible de préserver les intérêts et les droits de chacun dans un écosystème orienté vers la fluidité des usages.

Ces notions et technologies émergentes, aussi intéressantes soient-elles, ne révèleront leurs atouts qu'en s'insérant dans les infrastructures existantes conformément aux législations et aux règlementations en vigueur. C'est pourquoi une section de ce document s'attarde à étudier comment la *blockchain* et la *Self-Sovereign Identity* peuvent compléter les solutions déjà déployées. Ces sujets donnent lieu actuellement à un cadre d'expérimentation à l'échelle européenne, ainsi qu'à un travail de normalisation aux niveaux national, européen et mondial.

2. Examen des liens entre *blockchain* et identité

Les deux concepts de ***blockchain*** et d'identité que nous examinons dans ce document sont complexes. C'est pourquoi nous avons délibérément choisi d'introduire, préalablement à la discussion, de nombreux apports didactiques sur ces deux sujets.

2.1. Quand Alice et Bob communiquent sur une *blockchain*

Pour une présentation didactique du fonctionnement d'une *blockchain*, l'exécution de **smart contracts** est pris comme exemple, ainsi qu'un protocole de **consensus** basé sur une **preuve de travail**. Bien évidemment, ces exemples ne sont pas limitatifs et d'autres types de *blockchains* peuvent être considérés.

Les étapes du protocole ***blockchain***, visant à ajouter de l'information dans le **registre** (*ledger*) partagé et répliqué parmi les **nœuds** du réseau, sont détaillées sur la Figure 1.

Au préalable, les ***smart contracts*** sont développés dans un langage informatique de haut niveau, compilés, puis leur ***bytecode*** est déployé dans la ***blockchain***. Ils sont pourvus d'une adresse qui les identifie et qui permet de les désigner comme destinataire d'une **transaction**.

Dans le cas d'une *blockchain* supportant l'exécution de *smart contracts*, trois types d'information sont enregistrés dans les **blocs** formant le registre de la *blockchain* :

- le *bytecode* des *smart contracts*, c'est-à-dire le code compilé des *smart contracts*,
- les transactions effectuées depuis le dernier bloc,
- les résultats de l'exécution des *smart contracts*, déclenchés par la réception d'une transaction à l'adresse de destination exposée par le *smart contract*, et pouvant conduire à un changement d'état (changement de la valeur d'une variable du *smart contract*).

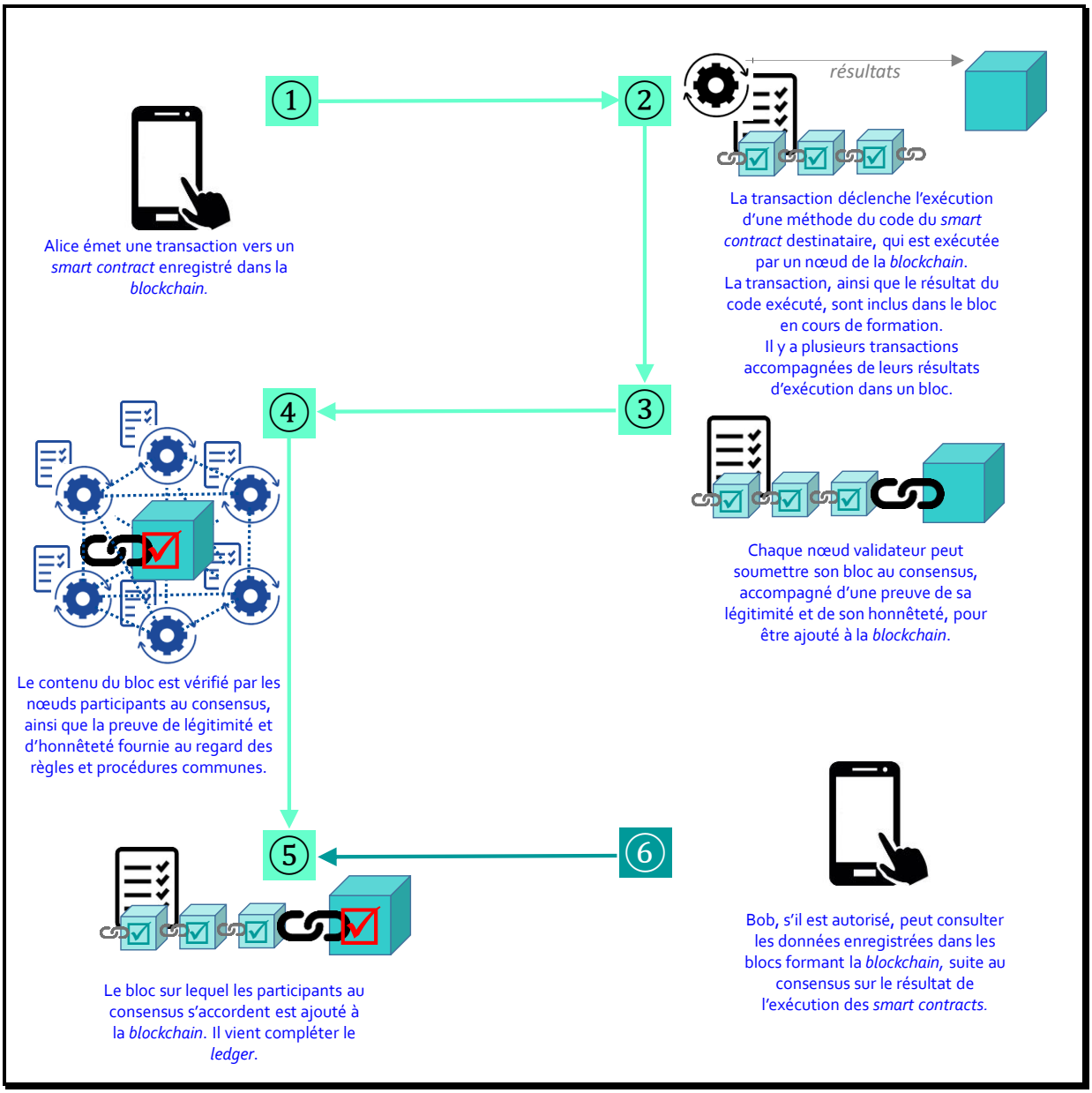


Figure 1 : les étapes de la construction d'une blockchain

✓ Etape ①

Lorsqu'Alice, souhaite envoyer des **crypto-actifs** ou des données à Bob, sur le **système distribué** par l'intermédiaire d'un *smart contract*, elle forme une **transaction** émise depuis son adresse de compte utilisateur à destination du *smart contract*, en indiquant l'adresse du compte utilisateur de Bob. Comparé à l'usage d'un système distribué de type pair-à-pair comme BitTorrent [4], l'usage de *smart contracts* exécutés par une *blockchain* apporte les garanties d'**authentification**, d'intégrité, d'horodatage, de traçabilité, de non-répudiation, et d'anonymisation (ou pseudonymisation) généralement dénommées « confiance ».

Il existe différents types de *blockchains*, dites **publiques**, **privées**, voire de consortium, qui se différencient par le niveau d'accès des utilisateurs au système. Sur une *blockchain* publique, tout le monde peut accéder au système et l'utiliser, c'est-à-dire émettre des transactions et consulter le registre. Pour cela, il suffit de disposer d'un compte d'émission pourvu éventuellement de crypto-actifs. Selon les *blockchains*, il peut être demandé de s'authentifier. Sur une *blockchain* privée, une

autorisation est requise pour accéder au système et l'utiliser, éventuellement avec un rôle défini. Les *blockchains* de consortium sont des *blockchains* privées, réservées à des groupes d'acteurs partenaires au sein d'un écosystème.

- ✓ Etape ②

La transaction envoyée par Alice est reçue par un **nœud** du réseau pair-à-pair, et ajoutée à un pool de transactions en attente d'être intégrées au nouveau bloc qui sera ajouté à la *blockchain*. A intervalles de temps régulier correspondant à l'intervalle entre deux blocs, les noeuds **mineurs** viennent chercher les transactions en attente dans le pool. Pour former le nouveau bloc, leur travail consiste tout d'abord à vérifier l'authenticité de chaque transaction et sa légitimité au regard des règles et des procédures communes décidées par la **gouvernance**. Il s'agit ensuite d'exécuter le code du *smart contract* destinataire et d'enregistrer le (ou les) résultat(s) de l'exécution, les changements d'état. Chaque mineur construit ainsi son propre bloc comportant les transactions qu'il choisit d'y insérer, les changements d'état résultant de l'exécution des *smart contracts* destinataires, ainsi qu'éventuellement de nouveaux *bytecodes* de *smart contracts* déployés dans l'intervalle de temps.

- ✓ Etape ③

Avant de soumettre son bloc au consensus, le mineur doit trouver une solution au challenge cryptographique de la preuve de travail (*Proof-of-Work*), c'est l'activité de **minage**. Pour cela, il fait appel à des ressources de minage, qui peuvent selon l'algorithme et l'implémentation retenue, être distantes et nombreuses. L'objectif de la preuve de travail est d'empêcher la reconstruction de l'historique des blocs passés et donc de garantir l'intégrité de l'ensemble du **registre distribué**. Si le mineur trouve une solution dans le temps imparti, c'est-à-dire l'intervalle de temps entre deux blocs, il soumet son bloc au consensus. Dans le cas contraire, il abandonne et passe à la construction du bloc suivant.

Les mineurs étant indépendants, dans un intervalle de temps donné, ils ne construisent pas exactement le même bloc. Les règles et procédures communes étant les mêmes, les transactions considérées légitimes sont les mêmes, mais peuvent être introduites dans un ordre différent.

Le terme de **minage** est réservé à l'activité de preuve de travail, actuellement utilisée par les *blockchains* Bitcoin et Ethereum. La preuve de travail présente l'inconvénient majeur de consommer une quantité importante d'énergie. C'est pourquoi des recherches sont en cours pour monter un autre mécanisme capable de maintenir l'intégrité du registre distribué de la *blockchain* depuis son origine. Une alternative à la preuve de travail pourrait être la preuve d'enjeu [5], qui consiste à immobiliser une certaine somme de crypto-actifs en garantie de son honnêteté. C'est l'activité de **mintage**, et on parle alors de ***minteur***, et non plus de **mineur**. D'autres alternatives sont également envisagées, comme à titre d'exemple, la preuve de temps écoulé [6], l'objectif étant de trouver un mécanisme basse consommation et de sécurité suffisamment élevée pour garantir l'historique du registre hébergeant les crypto-actifs et les *smart contracts*.

- ✓ Etape ④

Dans l'intervalle de temps entre deux blocs, chaque mineur est invité à soumettre son bloc. Les **validateurs** interviennent ensuite en participant au **consensus**. Leur rôle est d'émettre un vote en faveur du bloc qu'ils estiment le plus légitime, au regard des règles et des procédures communes, pour l'ajouter à la *blockchain*. Concrètement, chacun choisit parmi les blocs soumis celui qui lui paraît le plus légitime pour venir compléter la copie locale de son registre, et communique son choix aux autres mineurs : c'est le mécanisme de **consensus**. En principe, les règles et procédures communes doivent permettre de désigner un seul bloc gagnant, le même pour tous les validateurs. Il peut toutefois y avoir

des retards liés à la propagation des blocs sur le réseau, et parfois même des désaccords si deux blocs ont été soumis simultanément. Un embranchement (***fork***) se forme alors sur la chaîne, dans l'attente qu'une majorité de validateurs s'accorde sur l'une des branches. On considère généralement qu'un enfouissement de six blocs sur la chaîne la plus longue est suffisant pour confirmer les données qu'il contient.

- ✓ Etape ⑤

Le **mineur** ayant soumis le bloc gagnant est rétribué d'un montant de crypto-actifs appelé la **motivation** (*incentive*). L'*incentive* est une création de crypto-actifs (*ex nihilo*) destiné à rémunérer les mineurs.

Cette activité consistant à ajouter un nouveau bloc est au cœur de la *blockchain*.

A ce stade, on distingue deux types de *blockchain* qualifiés de *permisionless* et de *permissioned*. Les ***blockchains permissionless*** permettent, en principe, à tout un chacun de participer à l'activité de minage. C'est le cas de la *blockchain* Ethereum. A l'inverse, dans une ***blockchain permissioned***, seuls les nœuds autorisés, voire identifiés et répertoriés, peuvent soumettre un nouveau bloc au consensus.

Il résulte de cette distinction l'introduction de nombreux mécanismes visant à désigner le bloc gagnant, comme à titre d'exemple la preuve d'autorité [7] [8], dédiée aux *blockchains permissioned*.

- ✓ Etape ⑥

Le bénéficiaire de la transaction, ici Bob, consulte le registre de la *blockchain* pour y lire les informations qui le concernent ou lui appartiennent. Pour cela, il opère depuis son adresse de compte. Via une ***dApp***, il dispose des accès pour lire les données pour lesquelles il est autorisé. Il dispose également des fonctions lui permettant d'émettre des transactions vers le *smart contract* pour utiliser les avoirs qu'il vient d'acquérir par exemple.

2.2. Message ou Transaction entre Alice et Bob

Dans cette section, sont présentées les notions de **message** et de **transaction** numérique et ce qui les différencie. Tandis qu'un certificat numérique est généralement requis pour permettre d'authentifier, voire d'identifier l'émetteur d'un message, sur une *blockchain*, la transaction fournit, par essence, une forme d'authentification de l'émetteur sans avoir recours à un certificat numérique. Les **assertions** vérifiables sont des transactions qui incluent des affirmations vérifiables permettant d'authentifier l'émetteur. Les exemples suivants précisent chacune de ces notions.

Alice souhaite envoyer des données signées numériquement à Bob.

Pour pouvoir signer l'information, elle crée un couple de clés asymétriques (clé privée `sk`, clé publique `PK`). Elle conserve la clé privée `sk` en lieu sûr, afin qu'elle ne soit pas divulguée. Cette clé est utilisée pour signer numériquement l'information. La clé publique est transmise au destinataire, appelé Bob, pour vérifier l'authenticité et l'intégrité de l'information reçue en vérifiant la signature numérique.

Alice peut envoyer l'information signée à Bob de plusieurs façons :

1) Envoi d'un message entre deux pairs

Alice envoie l'information signée, des données personnelles par exemple, depuis son adresse email ou son adresse IP, selon le protocole de communication utilisé. A la réception, Bob utilise la clé publique d'Alice pour vérifier la signature numérique. Cela lui garantit l'intégrité de l'information, mais pas l'authenticité, car rien ne garantit que la clé publique fournie à Bob est bien celle d'Alice. En effet, ce schéma est vulnérable aux attaques de type *man-in-the-middle* (l'homme du milieu en français) où un imposteur peut intercepter l'information échangée entre Alice et Bob, en se faisant passer pour Bob vis-à-vis d'Alice, et pour Alice vis-à-vis de Bob.

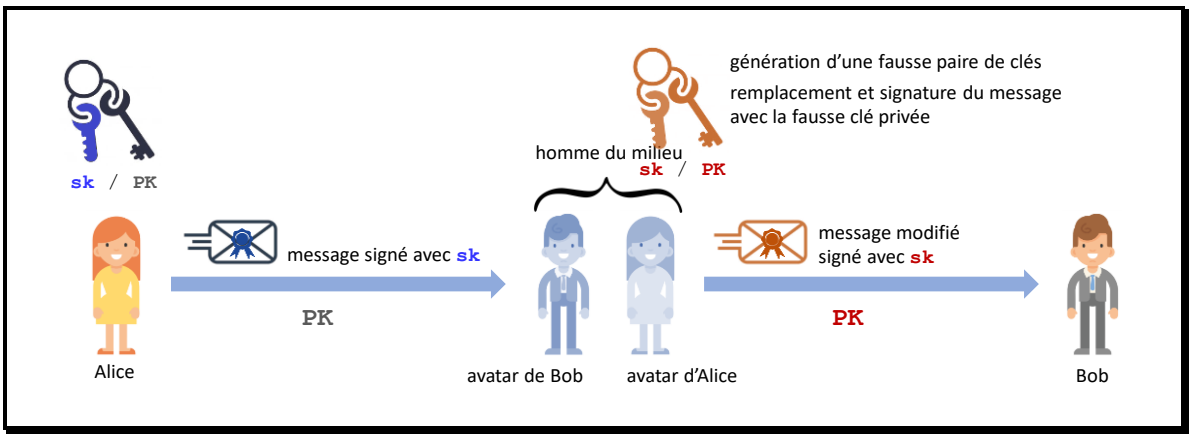


Figure 2 : principe de l'attaque dite « par l'homme du milieu »

2) Envoi d'un message authentifié par certificat numérique

Pour éviter cet écueil, on associe habituellement au message signé, envoyé par Alice, un certificat numérique. Le certificat numérique consiste à relier la clé publique `PK` d'Alice avec son instance d'identité (adresse email, adresse IP…), l'ensemble signé par une autorité de certification. A la réception, Bob fait appel à une autorité de vérification pour s'assurer de l'authenticité du certificat d'Alice et donc de son identité associée à la clé publique transmise `PK`. Bob utilise ensuite la clé publique pour vérifier la signature numérique de l'information qui garantit l'intégrité des données reçues et authentifiées. Ce schéma est très utilisé, mais il est lourd à cause de la nécessité d'assurer la maintenance du cycle de vie des certificats.

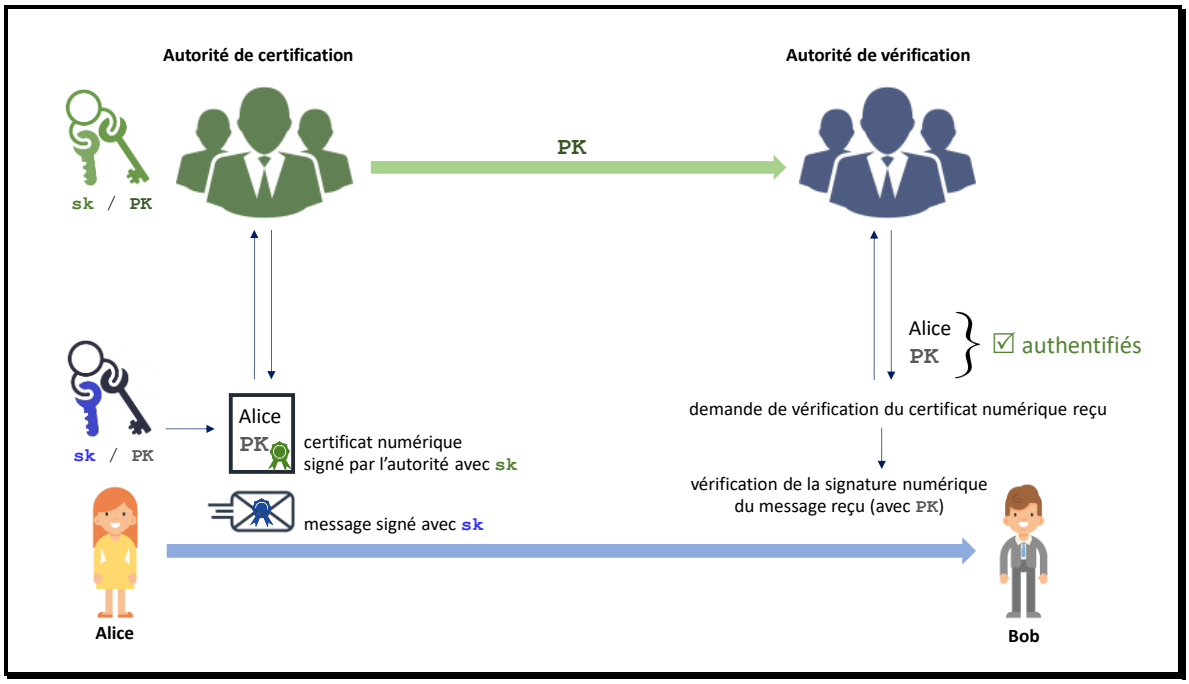


Figure 3 : envoi d'un message authentifié par un certificat numérique

3) Envoi d'une transaction sur *blockchain*

Les transactions sur *blockchain* offrent une alternative aux solutions précédentes en permettant de s'affranchir des autorités de certification et de vérification. La particularité de la transaction émise par Alice depuis son adresse de compte est qu'elle comporte une **empreinte** de sa clé publique construite grâce à une **fonction de hachage**. L'ensemble de la transaction est signé, y compris l'adresse du compte émetteur d'Alice, ce qui empêche toute modification ultérieure. La transaction est ensuite enregistrée dans la *blockchain*. Pour cela, la transaction doit être valide, c'est-à-dire que la clé publique doit vérifier à la fois la signature numérique en retournant « VRAI », et l'adresse du compte d'émission en comparant l'empreinte de la clé publique avec celle inscrite dans la transaction. Par ailleurs, l'algorithme de signature numérique utilisé pour former une transaction est particulier, dans le sens où la clé publique est incluse dans la signature numérique et peut être retrouvée moyennant des opérations mathématiques. La transaction inclut également l'adresse du compte destinataire, ici celui de Bob, transmis à Alice au préalable.

Lorsque Bob reçoit la notification qu'il a reçu des ***tokens*** ou des données, il consulte la *blockchain* en utilisant comme pointeur d'entrée sa propre adresse de compte. Il peut alors accéder à l'information qui lui est adressée. La *blockchain* en garantit l'authenticité et l'intégrité. En revanche, la *blockchain* n'assure pas la confidentialité de l'information. Ainsi, des données sensibles, à caractère personnel, devront être chiffrées avant d'être incluses dans une transaction, ou bien transmises en dehors de la *blockchain*, on parle alors de transmission hors chaîne ou ***off-chain***.

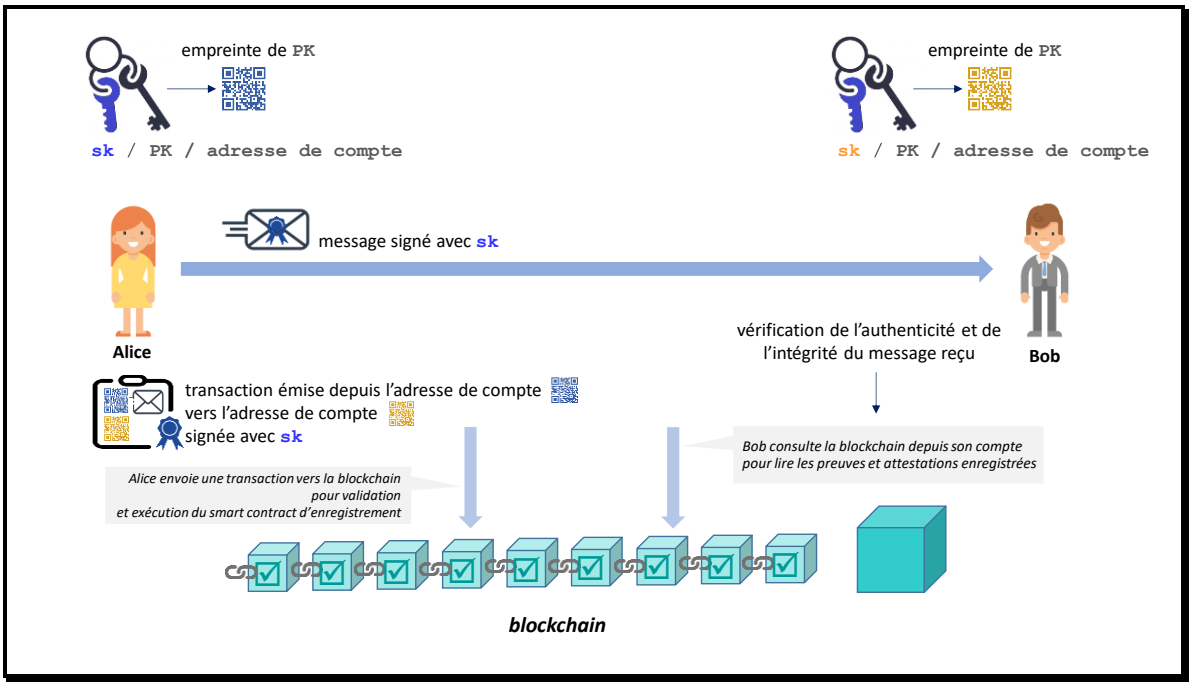


Figure 4 : envoi d'un message authentifié par une transaction

Suivant ce schéma, il n'est pas possible de modifier l'information transmise par Alice à Bob en se plaçant en *man-in-the-middle*. En revanche, Alice est authentifiée avec son adresse de compte, et non avec son identité. Or, de nombreuses applications requièrent de connaître l'émetteur, et donc de lier l'adresse du compte d'émission à l'identité de l'émetteur. La notion d'assertions vérifiables introduit un mécanisme permettant à l'émetteur de prouver son identité à partir de son adresse de compte. La preuve peut être enregistrée sur la *blockchain*, alors que la donnée personnelle que constitue l'identité est transmise au **vérificateur** de façon confidentielle. Les solutions d'identité auto-souveraine (*Self-Sovereign Identity*) exploitent les assertions vérifiables, et sont en grande majorité basées sur l'emploi d'une *blockchain* qui offre une technologie se prêtant bien à ces besoins.

Ainsi, les assertions vérifiables sont utilisées pour associer une identité à une clé publique dans un système décentralisé, là où les certificats numériques signés d'une autorité de certification sont employés dans un système centralisé.

3. Identité numérique et droits fondamentaux

3.1. L'émergence de la notion d'identité numérique

3.1.1. L'identité juridique

Le terme « identité » était peu utilisé dans le droit national (à l'exception de l'expression « carte d'identité ») jusqu'en 1994, date à laquelle il a été incorporé dans le Code Civil[6]. Cette notion était antérieurement désignée le plus souvent par le terme d'« état civil ».

La base de l'identité juridique se trouve donc dans le Code Civil, plus précisément au livre 1er « Des personnes », Titre II « Des actes de l'état-civil », Chapitre 2 « Des actes de naissance », Section 1 « Des déclarations de naissance », Article 57 : « *L'acte de naissance énoncera le jour, l'heure et le lieu de la naissance, le sexe…, les prénoms…, le nom de famille…* » ainsi que la filiation qui constitue la base de l'état civil.

C'est lors de la déclaration de sa naissance que l'identité est attribuée au nouveau-né pour toute sa vie. Cette identité :

- le relie à une famille, par son « nom de famille »,
- l'identifie au sein de cette famille par son (ou ses) prénom(s).

Elle est portée sur des registres d'état civil mis en place sous la responsabilité de l'Etat et sous le contrôle du procureur de la République. Ces registres sont tenus par des services d'état civil, encadrés par des officiers d'état civil qui agissent sous le contrôle du juge judiciaire, gardien des droits et des libertés : il s'agit donc d'un sujet très réglementé d'un point de vue procédural.

L'état civil confère une identité et l'identité confère un statut juridique (ou personnalité juridique) à la personne, c'est à dire des droits[7].

La loi du 6 fructidor an II, toujours en vigueur, précise dans son article premier : « Aucun citoyen ne pourra porter de nom ni de prénom autres que ceux exprimés dans son acte de naissance. »

Ce qui est appelé en droit français le « nom de famille » gagnerait à être renommé « nom de naissance » (par opposition au nom d'usage, par exemple le nom d'épouse des femmes mariées dont l'usage est seulement toléré par la loi).

Selon l'interprétation courante, les données d'identité fondamentales sont le nom de naissance, les prénoms, la date et le lieu de naissance, la nationalité ainsi que le sexe.

[6] A l'occasion des lois de bioéthique.

[7] A rapprocher de l'article 6 de la Déclaration Universelle des Droits de l'Homme du 10 septembre 1948 : « Chacun a droit à la reconnaissance en tous lieux de sa personnalité juridique ».

Corrélativement à son inscription à l'état-civil de sa commune de naissance, tout enfant né en France et quelle que soit sa nationalité est identifié, dès sa naissance, par son numéro d'inscription au répertoire national des personnes physiques (NIR).

Le NIR, ou numéro INSEE, ou encore numéro dit « de sécurité sociale » se compose de 15 chiffres. Il est désormais généralement considéré comme « intrusif » en droit français, car il indique de façon chiffrée mais transparente le sexe, la date et le lieu de naissance. Pour autant, le NIR répond mieux que n'importe quelle autre donnée d'identification à l'exigence d'univocité souvent requis par l'administration, même s'il n'est pas nominatif[8].

Nous verrons ultérieurement les problèmes soulevés par le numéro d'identification en droit national, en opposition sur ce point avec le droit européen.

Une partie des éléments constitutifs de l'identité présents sur l'acte de naissance se retrouvent sur la carte nationale d'identité (CNI) et sur le passeport.

En droit français, « L'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier » selon les termes de la loi°2012-410 du 27 mars 2012 relative à la protection de l'identité.

La CNI est régie par un décret de 1955 et par un règlement européen de 2019, qui succède à un premier décret datant de 1940. Auparavant, il n'existait qu'une carte d'identité pour les étrangers, laquelle est devenue aujourd'hui un « titre de séjour »[9].

La délivrance du passeport est encadrée par un décret de 2005, reprenant un règlement européen de 2004, qui succède à un premier décret datant de 1792, appliqué jusqu''à cette date.

Certains éléments qui figurent sur les deux documents figurent déjà sur l'acte de naissance (le nom de famille, les prénoms, la date et le lieu de naissance, le sexe). S'y ajoutent sur les deux titres des éléments d'identification complémentaires relatifs au porteur du titre : taille, adresse, photographie et signature manuscrite du titulaire, et des éléments relatifs au titre lui-même et à l'autorité qui l'a délivré : date de délivrance, date d'expiration, numéro du titre[10]....

La législation relative à ces deux titres d'identité et de voyage a été reprise et harmonisée dans la loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité qui précise dans son article premier que, si « l'identité d'une personne se prouve par tout moyen », il n'en demeure pas moins que « la présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier ».

L'ordonnance n°2017-1426 du 4 octobre 2017 modifiant l'article L102 du code des Postes et des Communications électroniques, dont il sera question ultérieurement, ajoute, dans son alinéa II, à ces deux titres suffisant à justifier de l'identité d'un individu « un moyen d'identification électronique ». Cette disposition attend pour entrer en vigueur la prise d'un décret en Conseil d'Etat, préalable à la rédaction par l'ANSSI d'un cahier des charges encadrant la conception de ce moyen d'identification électronique présumé fiable.

[8] Les résidents étrangers disposent également d'un numéro NIR.
[9] Un titre de séjour n'est pas un document d'identité au sens strict, cette identité étant attestée par le passeport étranger détenu par le titulaire du titre de séjour. Dans les faits, il tient souvent lieu de document d'identité.
[10] Des éléments relatifs au service instructeur et à la procédure suivie se trouvaient déjà sur les actes de naissance.

En l'attente de la prise de ces décrets d'application, le législateur établit ainsi une hiérarchie dans l'échelle des titres régaliens qui place les deux titres susnommés bien avant le permis de conduire, lequel est pourtant couramment utilisé pour décliner son identité.

De façon moins restrictive, la publication des bans d'un mariage est subordonnée depuis 2006 par le code civil à la remise de certaines pièces qui comportent la « justification de l'identité au moyen d'une pièce délivrée par une autorité publique ».

Plus libéral encore est l'article 1er de l'arrêté du 12 décembre 2013 pris en application des article R.5 et R.60 du code électoral, qui établit la liste des quatorze pièces qui permettant de justifier de son identité au moment du vote : y figurent aux côtés du passeport et de la CNI, la carte Vitale avec photographie, la carte d'invalidité civile et militaire avec photographie, la carte d'identité du fonctionnaire de l'Etat avec photographie ou encore le permis de conduire.

Tous les éléments évoqués ci-dessus concernent exclusivement les ressortissants français[11]. Le document émis par les autorités françaises assimilable à une pièce d'identité pour les résidents étrangers est la carte de séjour, étant entendu qu'il ne s'agit pas d'un document d'identité à proprement parler, la détermination de l'identité des étrangers étant exclusivement du ressort de leur pays d'origine. Pour autant, ce titre est utilisé en France dans de nombreux usages administratifs à des fins d'authentification, concurremment au passeport émis par le pays d'origine.

3.1.2. La numérisation de l'identité

En dépit de la numérisation des supports qui permettent de la décliner, la notion d'identité reste juridiquement inchangée, qu'elle soit attestée par un support papier ou sur un support numérique ou électronique et/ou sur le réseau électronique. L'identité dite « numérique » (ou « électronique ») n'est que l'émanation de l'identité juridique inscrite sur un support numérique ou électronique et dont le contenu est supposé demeurer immuable. A proprement parler, il n'existe pas d'**identité numérique**, la numérisation n'étant qu'un processus qui permet de transcrire des éléments d'identité sur support numérique, lequel permet de remonter à l'identité juridique.

La numérisation de l'identité ne crée pas un nouveau sujet de droit et, en cas de contentieux, on se réfère toujours à l'information source, à savoir l'identité juridique.

Les moyens d'identification électronique mis en place ou dont la mise en place est envisagée par l'Etat tels que Alicem ou France ID Num, ainsi que le « téléservice » FranceConnect[12], reposent tous sur l'identité juridique issue de l'état-civil, soit par une vérification des identités auprès du répertoire national d'identification des personnes physiques (RNIPP), soit par l'utilisation des titres d'identité et de voyage délivrés par l'Etat qui sont fondés sur l'état civil.

Pour autant, l'ambiguïté de cette notion d'« identité numérique » n'est pas levée par les textes juridiques nationaux où elle ne figure pas. Tout au plus peut-on trouver dans l'article 156 du décret n°2019-536 l'expression « données d'identité numériques », ainsi que dans le décret n°2018-687 du 1er août 2018 pris pour l'application de la loi « informatique et libertés » modifiée.

En revanche, l'expression « identité numérique » est couramment utilisée en matière pénale (cf. ci-après).

[11] A l'exception du permis de conduire français qui concerne aussi les résidents étrangers et sur lequel la nationalité n'est pas mentionnée.
[12] Qui fonctionne comme un service d'authentification mutualisé.

En dépit de sa consécration par l'usage, il serait plus précis de lui substituer l'expression « moyens d'identification électroniques sécurisés ».

On peut rapprocher cette expression de celles utilisées par le règlement eIDAS n°910/214 du 23 juillet 2014[13] sur « l'identification électronique » et les services de confiance pour les transactions électroniques. L'expression « identification électronique » est d'ailleurs privilégiée par la plupart des Etats membres dans l'application qu'ils font de ce règlement.

L'expression « carte nationale d'identité électronique[14] » figure également dans la loi du 27 mars 2012 relative à la protection de l'identité. Le législateur y prend soudainement conscience de la vulnérabilité de l'identité qui est présentée explicitement comme un « bien » à protéger[15].

Le code des postes et des communications électroniques a été, dans son article L102[16] qui date de 2017, le premier texte français à tirer explicitement les conséquences du changement de perspective induit par la numérisation pour l'identité :

- L'identité est envisagée sous son aspect fonctionnel d'identification dans un contexte d'échange électronique (à l'instar du règlement eIDAS),
- Il y est indiqué explicitement que le lien entre le moyen d'identification et la personne identifiée doit être univoque, (ce qui ouvre la voie à l'utilisation de tous les éléments d'identification complémentaires qu'il est possible de mobiliser, et donc à ce qui sera appelé ultérieurement les « données personnelles »),
- L'identification des personnes physiques est mise sur le même plan que l'identification des personnes morales (dans une perspective fonctionnelle),
- Il est explicitement prévu qu'un moyen d'identification électronique puisse être matériel ou « immatériel » (immatériel étant utilisé pour « électronique »),
- L'accent mis sur les moyens d'identification (et/ou d'authentification, cf. ci-après) pose la question de leur fiabilité : il est renvoyé aux prescriptions du cahier des charges établi par l'ANSSI fixé par décret en Conseil d'État. Ce cahier des charges doit se conformer aux prescriptions du règlement européen eIDAS[17][46].

Pour autant, le code des postes et des communications électroniques n'a pas pu dissiper toutes les imprécisions dues à la transposition numérique des données d'identification. Demeure, comme dans tout le droit positif, une confusion entre les notions d'identification (établissement des données d'identité) et d'authentification[18] (établissement de la légitimité à exercer un droit, à détenir un

[13]Ce règlement a pour objet d'accroitre la confiance dans les transactions électroniques au sein du marché intérieur.

[14] L'adjectif « électronique » se rapporte, non à « l'identité » mais à la carte du fait de la présence d'une puce électronique.

[15] Notons qu'en droit français, l'identité ne relève pas du droit de propriété : les données d'identité ne sont jamais considérées dans une logique mercantile, au contraire du droit américain.

[16] Il s'agit de l'ex article L136 du même code créé par la loi du 7 octobre 2016. Cet article ne fait que recopier en grande partie le règlement eIDAS. Il ajoute cependant la notion d'identité « présumée fiable » qui ne figurait pas dans le règlement européen au profit d'Alicem.

[17] L'ANSSI a souhaité cranter un niveau de sécurité supérieur aux dispositions européennes avec la notion d'identité « présumée fiable ».

[18] Il faut distinguer l'authentification d'une personne de l'authentification d'un document. Cf. le Glossaire. Parfois, identification et authentification d'une personne sont employées indifféremment : cela tient au fait que dans la vie quotidienne, il est souvent plus facile de demander à une personne de justifier de son identité pour faire état de son droit à accéder à un service ou à un lieu. Cela tient aussi au fait que l'identification suppose l'authentification d'un titre d'identité ou de voyage.

document d'identité, ou à accéder à un lieu ou à un service en ligne)[19]. C'est l'importance accordée fonctionnellement à l'authentification qui rapproche les problématiques des personnes physiques de la problématique des personnes morales évoquée ci-dessus.

Si la notion de donnée personnelle ne figure pas dans ce code, l'insistance portée à l'aspect fonctionnel de l'identification semble ouvrir la voie à l'émergence de tout élément pouvant contribuer à l'identification, y compris des éléments non institutionnels.

3.2. Importance pratique de la notion d'identité « pivot »

3.2.1. Emergence de la notion de données « pivot »

Il a toujours été considéré que c'est la combinaison « nom/prénom/date de naissance » qui désigne un être unique, même si la fréquence des homonymes requiert parfois des éléments complémentaires ; ces précautions sont jugées d'autant plus nécessaires que, comme nous l'avons vu, la reconnaissance d'une identité va de pair avec la dévolution de droits et d'obligations qui nécessitent des précisions relatives à la filiation, à la date de naissance pour établir l'âge, à l'adresse pour les services fiscaux…

Les difficultés d'identification sont résolues en fonction du contexte administratif, chaque **document source** ou titre contenant à peu près les mêmes mentions, mais susceptibles de varier à la marge en fonction de la doctrine d'emploi.

Mais l'informatisation de la société allant de pair avec la multiplication des interfaces en ligne qui nécessitent une identification ou, à tout le moins une authentification, a conduit à s'interroger plus avant sur les données qui permettent d'individualiser une personne de façon univoque dans des contextes aussi divers qu'imprécis.

Confronté à cette difficulté, le téléservice FranceConnect[20] a retenu comme données obligatoires à renseigner *a minima* le sexe, le nom de famille, le prénom, la date et le lieu de naissance et l'adresse de courrier électronique (ce dernier élément pour des raisons évidentes liées à l'utilisation de FranceConnect).

Dans la doctrine, les éléments que l'on retrouve cités dans chacun des trois documents, acte d'état civil, titre d'identité et titre de voyage sont considérés comme un « noyau d'identifiants » : ils constituent ce que l'on appelle souvent par commodité, « l'identité pivot ». Bien que cette expression ne soit consacrée par aucun texte juridique national ou européen, il est aisé de constater que, depuis les débuts de la numérisation de l'identité, ou plus exactement de numérisation sécurisée de moyens d'identification, cette notion innommée juridiquement correspond à une préoccupation continue.

C'est ainsi que la loi n°2012-410 du 27 mars 2012 citée plus haut précise dans son article 2, les données qui doivent (ou qui devront) figurer sur la carte d'identité électronique non encore déployée :

1° le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;
2° le nom usuel ;

[19] Exemple d'authentification : prouver que le titulaire a plus de 18 ans (pour acheter de l'alcool par exemple) sans qu'il ait besoin de décliner son identité ou même son âge.
[20] Article 2 de l'arrêté du 8 novembre 2018 relatif au téléservice FranceConnect : « Le téléservice a pour finalité de proposer au public de s'identifier et de s'authentifier, auprès de partenaires, fournisseurs de téléservices et de services en ligne, au moyen de dispositifs mis en œuvre par des fournisseurs d'identité partenaires de FranceConnect ». FranceConnect est un téléservice qui a pour objet de mettre en commun d'autres téléservices avec des moyens d'identification électroniques.

3° le domicile ;
4° la couleur des yeux et la taille[21] ;
5° les empreintes digitales ;
6° la photographie.

Ces données sont donc considérées comme données d'identité par le législateur, bien que certaines de ces indications soient sujettes à des variations au cours du temps comme la taille ou l'adresse.

Trois ans plus tard, le règlement d'exécution (UE) 2015/ 1501 de la commission du 8 septembre 2015 sur le cadre d'interopérabilité, visé à l'article 12 paragraphe 8 du « règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur » (appelé règlement « eIDAS »), revient sur la notion d'éléments identifiants fondamentaux dont il lui paraît indispensable de préciser les contours pour organiser l'interopérabilité numérique entre les Etats membres.

Le règlement d'exécution précise, dans son annexe, l'extension des données pivot appelée « ensemble minimal de données pour une personne physique » :

- Nom(s) de famille actuel(s) ;
- Prénom(s) actuel(s) ;
- Date de naissance ;
- Un identifiant unique créé par l'Etat membre […][22]

Tous les éléments figurant au moins sur l'un de ces actes ou titres constituent les éléments d'identité ou éléments identifiants consacrés par la pratique institutionnelle[23].

3.2.2. Caractère sensible de certaines données « pivot »

La notion de numéro identifiant unique référencé dans l'annexe de l'acte d'exécution du règlement eIDAS appelle certains développements en droit français.

Si ce numéro était déjà mentionné dans la loi « Informatique et Liberté » de 1978 et dans la loi de 2012 relative à la protection de l'identité, ce numéro NIR (pour « numéro d'inscription au répertoire ») ou numéro de sécurité sociale, est considéré en France comme une donnée personnelle à protéger tout particulièrement en raison de son caractère unique qui le rend particulièrement précieux en cas de croisement de fichiers, mais aussi parce qu'il est constitué de données personnelles codées de façon transparente (dont certaines jugées désormais sensibles comme le sexe). Aussi, l'article 30 de la loi de 1978 modifiée a-t-il prévu qu'un décret en Conseil d'Etat, pris après avis de la CNIL, déterminerait précisément les catégories de responsables de traitement qui peuvent utiliser ce numéro[24].

Dans un avis du 19 janvier 2017, la CNIL réaffirme que l'utilisation du NIR doit être réservé à la sphère sanitaire et médico-sociale et qu'elle veillera à ce qu'aucun élargissement de cet usage n'intervienne à l'avenir.

[21] Toutes ces données contenues dans le composant électronique sécurisé figurent également « en clair » sur le titre, à l'exception de la couleur des yeux qui n'est pas mentionnée en clair sur la carte d'identité et qui figurera uniquement dans la puce.
[22] Lequel comporte également une référence indirecte à la nationalité.
[23] Les éléments figurant sur la carte de séjour des résidents français d'origine étrangère sont approximativement les mêmes.
[24] Il s'agit du décret n°2019-341 du 19 avril 2019.

Dans la pratique, l'absence de référence au numéro unique d'identification sur les titres d'identité est compensée par la mention des données biométriques que sont la photographie et les empreintes digitales sur le passeport comme sur la CNIE à venir. Ces données biométriques qui correspondent à la numérisation de la mesure du vivant (selon l'étymologie du terme « biométrie ») sont un élément déterminant dans la recherche de l'univocité du lien entre un titre et son détenteur.

En dépit de cette différence de statut du numéro d'identification pour le législateur européen et pour le législateur national, laquelle crée une incertitude juridique, on peut dégager les conclusions suivantes :

- Les éléments que l'on retrouve mentionnés sur chacun des trois types de documents nationaux[25], acte de naissance, CNI(E) et passeport, et dans l'annexe du règlement eIDAS, nous permettent de dégager la notion d'éléments d'identité, une sorte de « noyau central » d'informations réputées constitutives de l'identité, à l'intérieur même des éléments identifiants : il s'agit du nom de naissance (ou usuel), des prénoms, du sexe, de la date de naissance et de la nationalité.

  Certains de ces éléments suivent la personne physique pendant toute sa vie et même au-delà, puisque le décès d'une personne n'altère pas son identité. D'autres éléments sont susceptibles de varier, comme la nationalité ou, depuis une date plus récente, le sexe.

  C'est à ces éléments-là que nous réservons l'appellation « identité pivot ».
- Les autres indications qui figurent sur les titres, documents, schémas d'identification institutionnels constituent des éléments « d'identité » ou « d'identification » complémentaires, des attributs divers dont certains peuvent renvoyer à l'aspect physique de la personne, dont d'autres se réfèrent non à la personne identifiée, mais au service de délivrance du titre et à la procédure suivie. Dans ce dernier cas, il s'agit davantage d'éléments d'authentification de la procédure suivie que d'éléments d'identification à proprement parler.

Ces éléments d'identification, complémentaires par rapport aux éléments d'identité fondamentaux, peuvent cependant être mobilisés utilement pour diligenter les opérations administratives les plus fréquentes :

- Vérifier que la personne en face-à-face est bien la titulaire du titre d'identité (notion d'identification, mais aussi d'authentification du titre et d'authentification du lien entre le titre et son porteur, soit opération 1 parmi 1),
- Retrouver une personne (disparue ou recherchée par exemple) parmi un ensemble de personnes (identification au sens de la recherche d'une personne, soit opération 1 parmi n),
- Eviter les confusions entre deux personnes ou l'usurpation d'identité (discrimination).

L'ensemble des éléments évoqués ci-dessus, « identité pivot » ou éléments d'identité ou d'identification complémentaires, constituent les éléments d'identité consacrés par la pratique institutionnelle pour leur importance dans la diligence des opérations administratives.

Pour vérifier que la personne en face-à-face est bien la titulaire du document produit, lors d'un contrôle de police ou d'un passage frontière par exemple, les éléments d'identification complémentaires relatifs à son apparence physique (taille, couleur des yeux) ou, depuis une date plus récente, à ses données biométriques (empreintes digitales ou reconnaissance faciale) pourront être utilisés. Dans un but de

[25] A noter que la carte de séjour pour étrangers mentionne les mêmes données pivot que les titres pour ressortissants nationaux, mais leur fiabilité est moindre, par hypothèse.

discrimination entre deux personnes physiques, tous les éléments d'identification complémentaires pourront être sollicités, y compris les éléments procéduraux.

3.3. Données nominatives et données personnelles

Nous avons déjà évoqué les mentions qui permettent de déterminer ou de confirmer l'identité d'une personne sans faire véritablement partie de l'identité « pivot » : les éléments connexes à l'état civil tels que l'identité des père et mère (filiation), leur profession et leur domicile au moment de l'inscription de leur enfant à l'état civil (données relatives à la filiation), la profession et l'adresse du détenteur du titre (données sociales), les références à l'aspect physique de la personne (signalement), ou les données administratives relatives aux procédures d'état civil ou de délivrance de titre (données procédurales servant à l'authentification des titres). Le rôle de ces données identifiantes complémentaires, qui figurent sur les documents, titres et schémas institutionnels, est de confirmer l'authenticité des données d'identité, en les inscrivant dans un contexte familial, social, procédural (comme sur le registre d'état civil) ou en rendant possible une confirmation visuelle.

L'arrivée du numérique dans nos existences multiplie les occasions d'identification d'une personne à partir de la communication de certains **attributs d'identité**, en dehors de tout contexte préétabli, à distance, et souvent à l'insu de la personne concernée.

On passe donc de la notion de données d'identité (données « pivot » et données complémentaires institutionnelles) à la notion de données « identifiantes » qui comprend en plus tous les éléments qui peuvent, dans un contexte donné servir à identifier un individu.

Dans sa version initiale, l'article 4 de la loi de 1978 « Informatique et Liberté » (dite aussi loi CNIL) [9] introduisait la notion de « données nominatives » en posant de manière particulièrement clairvoyante que ces données pouvaient servir à identifier une personne indirectement sans qu'il soit nécessaire de la désigner nommément : « 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. »

Mais, la version de ce texte issue de la loi de 2004, qui transpose la directive européenne de 1995, opte pour l'expression plus générale de « **données à caractère personnel** » afin d'englober le plus de situations possibles (et afin de clarifier le paradoxe posé par l'article cité ci-dessus selon lequel une donnée dite « nominative » pourrait ne pas identifier une personne « directement »). Une définition en est donnée à l'article 2 de la loi : « 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 ».

Cette version a le mérite de pointer explicitement pour la première fois que c'est l'accumulation d'éléments relatifs à une même personne qui menace l'anonymat ainsi que la diversité des données accumulées, même lorsque que la personne n'est pas nommée.

La loi CNIL, dans sa version de 2004, qui consacre donc la notion de « données à caractère personnel » ou « données personnelles » en englobant les données d'identité à proprement parler, comprend toutes les données relatives à un individu qui permettent son identification. Il s'agit donc d'une notion fonctionnelle, qui s'apprécie en fonction d'un processus, celui de l'identification.

L'article 4 du Règlement de l'Union Européenne (UE) 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 du 27

avril 2016 appelé « règlement général sur la protection des données » (RGPD), revient sur cette notion en en donnant de nombreux exemples pour souligner l'hétérogénéité des données qui peuvent être mobilisées : on entend par « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; 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 ; ».

Le champ des données personnelles semble donc s'accroitre.

La philosophie de ce règlement européen est, certes, très inspirée de la loi française de 1978, acte de naissance de la CNIL, mais le texte européen va beaucoup plus loin.

On ne souligne pas assez, outre les possibilités vertigineuses offertes par le séquençage ADN, qu'une des nouveautés du règlement eIDAS consiste à introduire aux côtés des données d'identité « numérisées » (le nom transposé en octets ou les données biométriques) des données numériques *ab initio,* telles les traces laissées sur internet ou des données proprement techniques comme l'adresse IP de du point d'accès à l'ordinateur personnel.

Ce texte nous fait également passer des données proprement identifiantes (avec l'insistance sur les données physiques, physiologiques et génétiques qui semblent augurer d'un recours généralisé à la biométrie) à des données qui « caractérisent » socialement l'individu (ses pratiques culturelles, son comportement). Toutes ces données sont d'ailleurs beaucoup plus indiscrètes et menaçantes pour la vie privée car elles permettent d'en déduire des goûts et un profil psychologique, et annoncent les excès du profilage à venir.

Conformément à ces textes, on pourrait considérer l'identité et les données personnelles correspondant aux éléments relatifs à la personne, comme une série de trois cercles concentriques :

- Les informations constituant l'identité « pivot », c'est-à-dire les éléments constitutifs de l'identité communs à ces trois documents que sont l'acte de naissance, la CNI et le passeport (éléments repris sur le permis de conduire) ainsi qu'au schéma mutualisé d'authentification FranceConnect, et dans le règlement eIDAS.
- Les informations relatives au corps humain, biométrisées[26] ou pas (empreintes, photo visage... tout ce qui, dans une situation de face-à-face, permet de faire le lien entre un titre et une personne physique). Mais, sont aussi rapportées au corps humain les éléments d'identifications physiques rendues possibles par les développements scientifiques relatifs à la physiologie, la génétique et même le psychisme.
- Les informations diverses (notamment l'ensemble des traces laissées sur Internet) que ces informations soient numérisées ou numériques *ab initio* : traces de navigation, adresse de la messagerie électronique, adresse IP, goûts, habitudes… toutes les données personnelles, qui ne sont ni éléments d'identité, ni éléments d'identification au sens propre, mais dont l'accumulation et le croisement peuvent servir à identifier une personne dans une sphère sociale et anthropique. Cet ensemble hétérogène regroupe des éléments comportementaux et des éléments techniques.

Les données d'identité ou d'identification consacrées par la pratique administrative comprennent l'ensemble des données pivot et un certain nombre de données appartenant à la deuxième catégorie

[26] La biométrie est l'application de la métrique au vivant.

des informations relatives au corps humain (avec l'importance croissante accordée à la biométrie) et à la troisième catégorie plus hétérogène.

3.4. Menaces sur les droits de l'individu liées à la numérisation de l'identité

Les services de l'Etat, garants de l'équilibre entre les aspirations légitimes à la vie privée et les nécessités de la sûreté et de la sécurité, doivent faciliter l'action des forces de l'ordre luttant contre la criminalité et le terrorisme : il importe de faciliter cette action par une identité traçable et fiable, c'est-à-dire à une identité régalienne (dont l'Etat est le garant).

Pour autant, un équilibre doit être trouvé entre les aspirations individuelles énoncées ci-dessus et les enjeux liés à la protection sociale de la collectivité nationale et internationale : le développement de la technologie offre-t-il l'opportunité de surmonter la contradiction entre la protection des libertés individuelles et les nécessités de l'ordre public ?

3.4.1. L'identification malveillante et « l'individualisation »

Pour les législateurs, national ou européen, il convient d'abord de protéger l'individu de toute identification intempestive, c'est-à-dire, de toute identification hors d'un cadre légal et hors de la connaissance et du consentement éclairé de l'individu. C'est un sujet de protection de la liberté, la liberté étant conçue comme englobant le droit à l'intimité et à l'anonymat. Il s'agit de lutter contre la menace bien connue d'un espionnage permanent déjà identifiée par la CNIL, et par le législateur européen auteur du RGPD, et de la directive Police-Justice 2016/680 qui constitue la base de la licéité du traitement des données personnelles par les Etats membres, article 8 et article 10 pour les données biométriques.

Cette protection du droit à l'intimité et à la vie privée (*privacy*) s'opère en protégeant l'ensemble des données personnelles des individus, toutes ces données étant susceptibles de servir à l'identification par un tiers (même en l'absence d'éléments d'identité légale). La protection de la *privacy* consiste à faire en sorte qu'aucun individu ne puisse être identifié nommément, hors de son consentement et hors des cas prévus par la loi. En effet, le RGPD (article 6) reconnait l'intérêt public comme étant un motif de licéité du traitement des données à l'insu des personnes concernées : tel est le fondement juridique, avec l'article 31 de la loi informatique et liberté modifiée et la directive police justice, des fichiers de police ou judiciaires[27].

A l'époque de la création de la CNIL, c'est l'Etat régalien qui était la première cible des soupçons d'atteintes aux libertés individuelles ; cette crainte est particulièrement importante dans notre pays pour des raisons historico institutionnelles. La loi informatique et liberté était clairement dirigée contre un Etat soupçonné de vouloir faire « la chasse aux Français[28] » en interconnectant les fichiers administratifs. Cette crainte a été réactivée au moment de la mise en place du « mutualisateur d'identité » FranceConnect avant d'être désamorcée par la mise en place d'une architecture préservant les données personnelles selon le modèle appelé « *privacy by design* ». Le concept de « *privacy by design* » a pour objectif de garantir que la protection de la vie privée soit intégrée dans les nouvelles applications technologiques et commerciales dès leur conception.

[27] Ces textes servent aussi de fondement juridique à toute la réglementation sur les fichiers et les traitements développés pour les nécessités de la police administrative.
[28] Projet « Safari », bien mal nommé.

Le problème est que ce « *continuum* » de données référençant une personne est difficile à appréhender. Comment repérer les données personnelles qui, pouvant servir à l'identification, doivent être protégées ?

De manière très pragmatique, le RGPD a dégagé la notion « d'identifiabilité » pour apprécier plus finement les dangers d'identification intempestive encourus. Il indique, dans son considérant 26, qu'il convient pour apprécier le risque « d'identifiabilité » de prendre en compte « des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ».

Dans une circulaire précisant la portée de l'article L226-4-1 du code pénal, il est précisé qu'est protégée « toute donnée permettant [de l]'identifier : au-delà des nom et prénoms d'une personne, il peut donc s'agir d'une adresse électronique, du numéro de sécurité sociale, d'un numéro de téléphone, d'un numéro de compte bancaire, d'un pseudonyme… ».

Les données personnelles destinées à être protégées se caractérisent donc par un périmètre évolutif et dépendant du contexte.

Mais le repérage d'un individu ne doit-il pas être appréhendé selon un prisme plus large que l'identification ? Tel est l'avis du groupe 29, émanation des « CNIL européennes », désormais désigné sous l'appellation de « Comité européen de la protection des données », qui précise : « Sans même s'enquérir de son nom et de l'adresse de la personne, on peut la caractériser en fonction des 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 la révélation de son identité au sens étroit du terme ». Il faut donc considérer que la personne peut être repérée chaque fois qu'elle peut être individualisée, discriminée, sans avoir pour autant besoin d'être nommée. Dans certaines circonstances, des données personnelles ne permettront pas de l'identifier, c'est-à-dire de lui attribuer un nom, mais seront suffisantes pour l'individualiser, pour la repérer sans que son identité soit dévoilée.

Il est intéressant de constater que la protection ne vise plus seulement à empêcher l'identification, c'est-à-dire la possibilité de nommer une personne *a posteriori*, mais aussi à faire obstacle à l'**individualisation**. L'intimité et la vie privée d'une personne est menacée simplement si on peut comprendre de qui il s'agit, même si la personne en question n'est pas nommée, ce qui explique la protection du pseudonyme.

Cette interprétation semble bien être celle de la CNIL qui entend assurer une protection très large de toutes les informations se rapportant à une personne physique.

3.4.2. Risque de traitement des fichiers par algorithmes et profilage

La suspicion à l'égard de l'Etat était liée à sa capacité à détenir et à croiser de nombreux fichiers.

C'est à cette tentation que la loi de 1978 créant la CNIL a mis un frein.

Si le soupçon à l'égard de l'Etat n'a pas disparu, notamment sous l'effet de la montée en puissance d'Etats ayant une culture politique très différente de la culture libérale démocratique et individualiste occidentale, l'Etat n'est plus perçu comme le principal ennemi de l'intimité.

On a récemment pris conscience que cet espionnage malveillant pouvait être le fait d'entreprises privées étrangères, notamment les géants de l'Internet, GAFAMI[29] ou BHATX[30]. Et désormais, la crainte n'est plus l'identification, ou même l'individualisation ; la multiplication des données personnelles de toute nature mises à disposition sur Internet a créé une nouvelle atteinte aux personnes, sans commune mesure avec la situation antérieure : le profilage.

Nous savons depuis l'affaire « *Cambridge Analytica*[31] » que certaines des données personnelles non identifiantes peuvent être utilisées dans un autre but qu'une identification intempestive. Le passage des éléments d'identité (l'identité « pivot ») aux attributs d'identification, voire à des éléments de caractérisation, recèle une nouvelle menace pour l'individu. Ces données ne seront plus uniquement utilisées dans le but de l'identifier mais dans le but de cerner sa personnalité d'une façon plus intrusive que sa simple dénomination ou « individualisation ».

Le terme de profilage, issu du *marketing* commercial, désigne la capacité de caractériser une personne à partir d'un faisceau de données personnelles révélatrices de ses goûts, opinions et habitudes (les traces numériques laissées volontairement ou non, sur internet par la personne) dans un but de conditionnement, voire de manipulation. Comme l'individualisation, cette attaque ne passe pas nécessairement par l'identification de la personne, c'est-à-dire par la capacité de la nommer. Si un tel conditionnement est parfaitement admis dans un domaine commercial où la volonté de l'expéditeur qui fait la publicité d'un bien est suffisamment apparente pour être déjouée, et où l'enjeu consiste seulement à créer des besoins matériels, il n'en est pas de même dans le domaine politique où les intentions de l'émetteur portent sur l'altération du jugement du destinataire. D'autant que ces actions de manipulations sont diligentées dans le plus grand secret, à l'insu de la personne concernée.

On passe donc de la violation du « droit d'être laissé tranquille », à l'atteinte portée à la capacité de l'individu à participer de manière autonome à la vie politique, sociale...

Conscient du risque, le législateur européen définit dans le RGPD le « profilage » comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique… [32]». Le terme « profil » n'est pas défini par la loi : on peut néanmoins facilement le définir comme le résultat de calculs statistiques traités par des algorithmes dont le but est d'anticiper les réactions et de susciter des besoins et des réactions. Il restitue une représentation probabiliste de la personne.

Le profilage, qui porte en lui les menaces d'une atteinte à l'autonomie des individus, passe souvent par l'inscription dans un fichier ; c'est ainsi que prospèrent les géants du numérique (GAFAMI américains et BHATX chinois) qui font des données personnelles de leurs clients la base de leur modèle économique, au grand dam de la CNIL et de ses homologues européens.

Les innovations technologiques récentes, le *big data*, l'intelligence artificielle, ayant démultiplié les utilisations possibles de ces fichiers en facilitant leur interconnexion, il devient de plus en plus important de se prémunir contre leur multiplication entre de mauvaises mains, et contre leur utilisation

[29] Entreprises géantes du numérique américaines : Google, Apple, Facebook, Amazon, Microsoft, IBM.
[30] Entreprises géantes du numérique chinoises : Baidu, Huawei, Alibaba, Tencent, Xiaomi.
31 *https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica*
[32] Article 4 du RGPD.

pour des motifs illégitimes. Le législateur de 1978 avait déjà identifié le problème des fichiers en des temps de technologie numérique balbutiante.

3.4.3. De l'usurpation d'identité au risque de tromperie généralisée

Mais la connaissance de certains de ces éléments d'identification, y compris de certaines des données procédurales qui encadrent la délivrance de titres, peuvent aussi servir à l'usurpation d'identité. La reconnaissance d'une identité légale étant le fondement de la capacité juridique de la personne, usurper l'identité d'une personne revient à la priver de tout ou partie de ses droits. Commence alors pour la malheureuse victime un parcours du combattant pour être réintégré dans son identité et dans ses droits.

En effet, l'utilisation à distance de l'identité numérique, la multiplication des usages numériques et la nécessité de partager ses données dans des contextes variés nous a fait prendre conscience de la grande vulnérabilité des données personnelles numérisées, confirmant la justesse de l'intuition du législateur du 27 mars 2012.

Jadis cantonnées au vol de papiers d'identité, à leur altération, leur falsification, et à la fabrication de faux papiers, le recours désormais croissant aux identifications / authentification en ligne a multiplié les occurrences des usurpations d'identité et amplifié la gravité de leurs conséquences par la constitution illégale de fichiers dans un but d'utilisation illicite ou de revente. L'article L226-4-1 du code pénal précité redéfinit l'usurpation de l'identité pour tenir compte de la nouvelle situation créée par la prolifération des données personnelles. Comme le précise opportunément la circulaire du 28 juillet 2011 également précitée, le délit est étendu à l'usurpation de « toute donnée permettant de l'identifier », y compris un pseudonyme.

Par ailleurs, la manipulation malveillante et illicite par autrui de données personnelles ne conduit pas uniquement à l'incrimination d'usurpation d'identité dans le but de s'approprier les droits de son détenteur. Les tribunaux doivent aussi protéger la collectivité contre la volonté « gratuite » de nuire. Ainsi, la Cour d'appel de Dijon a-t-elle condamné en 2017 l'action d'un délinquant qui s'était rendu coupable de la création d'un « profil internet » en accolant une photographie à des propos qui n'avaient jamais été tenus par la personne représentée.

Pour résumer, la numérisation de l'identité et des données personnelles multiplie les possibilités d'atteintes à la personne en accroissant les possibilités d'acteurs malfaisants dans le domaine de l'espionnage, de l'usurpation d'identité et d'atteinte à la réputation. De plus en plus, la demande sociale se tourne vers l'Etat pour lui demander de lutter efficacement contre les usurpations d'identité en ligne, de protéger les citoyens contre ces différentes atteintes à leurs droits et de créer une identité numérique résiliente aux malversations

La numérisation des données personnelles biométriques pourrait servir à la limiter ces atteintes à l'identité et aux droits afférents.

De plus, l'usurpation d'identité ne se fait pas exclusivement à l'insu du détenteur légitime de l'identité. L'administration et les tribunaux doivent également lutter contre des « prêts d'identité » que les juristes appellent la « fraude comportementale » et qui n'est pas traitée par le règlement européen eIDAS.

A l'heure du partage généralisé des données et de la multiplication des services en ligne, il devient d'autant plus nécessaire de récréer la confiance.

Le besoin de confiance dans une réalité dont l'Etat est le garant ne passe pas seulement par la confiance dans les identités numériques produites sur Internet. C'est la sécurité juridique dans son ensemble qu'il a pour mission de préserver sur Internet. Cette mission de protection s'étend également à l'utilisation qui est faite des différentes allégations qu'il importe d'authentifier et de certifier à l'égal d'une justification d'identité telle l'allégation de la détention d'un diplôme.

3.5. Nouveaux besoins, nouveaux défis pour l'identité et les données personnelles

3.5.1. L'émergence de nouveaux droits numériques

A la lecture de ce qui précède, on comprend mieux ce qui est attendu de l'identité numérique.

Actuellement, le ressortissant et le résident français disposent d'un système de mutualisation des authentifications mis en place par l'Etat dans un contexte administratif, FranceConnect, qui repose sur la distinction entre des fournisseurs d'identité et des fournisseurs de service.

Les titres d'identité sécurisés électroniquement permettent d'identifier leur détenteur :

- dans le monde physique grâce à une lecture numérique,
- en ligne dans un contexte numérique.

Pour autant, la demande sociale va au-delà de ces usages tenant à l'identification par le codage des données constitutives d'identité sur un titre.

Pour récapituler, la numérisation des données d'identité devrait aussi répondre aux quatre demandes sociales exprimées ci-après.

- 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 ;
- 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 » ;
- Droit à la résilience de l'identité légale numérisée en cas d'attaque ;
- 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'Etat et d'autres acteurs clés de la vie du citoyen (banques, assurances, établissement de formations diplômants...).

Il appartient aux différents Etats régaliens de mettre en place les textes et les procédures nécessaires à la réalisation de ce nouvel équilibre social, ainsi que les institutions nécessaires. Mais les textes et les procédures administratives ne peuvent pas tout. La réalisation d'un tel univers de confiance passe aussi par des processus et des innovations techniques.

Ces objectifs, en grande partie contenus dans le concept de *privacy by design* ou *by default,* consistent à instaurer d'emblée « un paramètre basé sur le plus haut niveau de protection des données personnelles ».

3.5.2. Vers des orientations techniques

Déclinés en spécifications, les objectifs politico-juridiques énoncés ci-dessus, peuvent être traduits par les orientations techniques suivantes :

- Permettre la **minimisation** des informations communiquées (exemple de la preuve de majorité requise pour un achat en ligne sans communication de son identité, ou même de sa date de naissance) ; la recherche de la minimisation doit s'apprécier dans un contexte plus général de dissociation de l'identification et de l'authentification (dans le monde physique, pour prendre le métro, il n'est pas nécessaire de décliner son identité)[33]. Cette dissociation devrait aller jusqu'à l'utilisation de pseudonymes, comme dans certains domaines de la vie courante[34]. La recherche de la minimisation des données personnelles communiquées s'apparente au principe de proportionnalité dégagé par la CNIL, selon lequel seules les données « utiles » pour l'accès au service doivent être communiquées. Ce principe est aussi parfois nommé « distributivité sélective ».
- Dans le même temps, il paraît de plus en plus nécessaire **d'ancrer** toutes les données dans un univers de confiance : toute identification doit reposer sur l'identité juridique préservée comme référent unique, incontournable, gage de la sécurité juridique indispensable à la vie civile, économique, et à la préservation de l'ordre public. Assurer la résilience de l'identité en cas d'usurpation, implique de s'arrimer à l'identité régalienne. La défense contre l'usurpation des données personnelles permet de réaffirmer le rôle de l'Etat comme garant des données d'identité, de leur caractère incontestable et vérifiable, un peu à la façon d'un tiers de confiance ultime.
- Un système comparable doit être mis en place pour l'**authentification** de certaines des données produites par des fournisseurs d'attributs. Car le besoin de restaurer la confiance implique également de pouvoir se fier à la revendication de qualité par autrui[35]. Mais dans ce cas, le tiers de confiance chargé de garantir la véracité de la donnée ne sera plus nécessairement l'Etat mais pourra être une autre institution, publique ou privée, même si l'Etat demeure le garant ultime d'une réalité sécurisée.
- La mise en place du principe de *privacy by design* implique aussi de permettre à l'individu d'accéder aux données qui le concernent, voire de manifester son consentement avant de recueillir les informations qui le concernent. Non seulement il est important de l'informer et de recueillir son avis, mais il serait aussi nécessaire de lui permettre en tout temps de faire valoir ses droits : rectification, effacement, portabilité, retrait du consentement. Ces diverses capacités participent à ce que l'on appelle généralement ***l'empowerment*** de l'individu, soit en français, son « **encapacitation** » ou l'accroissement de sa responsabilité, en lui offrant la possibilité de contrôler l'usage de ses données personnelles et, même, de contribuer à la gestion de ses propres données. L'objectif est de lui offrir la possibilité de décider lui-même du périmètre des données communiquées en fonction de l'usage en ligne qui est recherché.
- La réalisation de cette gestion par l'individu de ses propres données personnelles serait un apport décisif, surtout si l'on parvient à conserver l'ancrage des données sur l'identité régalienne. Une réflexion plus approfondie révèle que le danger est celui de « l'associabilité » qui consiste à pouvoir relier les actions effectuées par l'utilisateur dans des contextes différents. En première analyse, le cloisonnement des données semble pouvoir être préconisé,

[33] Il a été reproché à FranceConnect le recueil par le fournisseur de service d'un trop grand nombre de données d'identité, sans égard à leur caractère utile.
[34] L'usage des pseudonymes est par exemple courant pour les artistes, les romanciers et chez les altesses.
[35] Les usurpations constantes du titre d'ingénieur ou de docteur sont un bon exemple du besoin de contrôle.

et pourrait aller jusqu'à la détention d'un support individuel des données personnelles par la personne intéressée. En résumé, la mise en place d'une **architecture fédérative et décentralisée d'identification** doit être favorisée, sauf en ce qui concerne l'identité légale sur laquelle repose tout cet édifice. Cette architecture pourrait utilement compléter le schéma actuel d'identification construit autour de FranceConnect (qui pour l'instant se fonde sur des moyens d'identifications électroniques ne fonctionnant pas à partir de titres électroniques) et des moyens d'identification électronique à venir fonctionnant à partir de titres d'identité électroniques grâce à une nouvelle version d'Alicem.

- Il faut préserver la possibilité pour les forces de sécurité de mettre à profit les ressources de traçabilité pour faciliter la recherche de délinquants et de terroristes dans les conditions d'un Etat de droit sous le contrôle du juge. L'identité doit être constamment accessible pour permettre une vérification de l'identité juridique de l'administré.

Ces six enjeux principaux assignés au monde numérique dans ses relations à l'identité se ramènent tous à un maître mot : **la confiance**.

Confiance grâce à **l'ancrage de l'identité numérique** dans l'identité régalienne. L'identité des individus est garantie par l'Etat et l'identité numérique doit continuer à se fonder sur cette identité régalienne, nonobstant la possibilité d'agir sous un pseudonyme. Il est important que la victime d'une usurpation d'identité, puisse disposer d'un recours étatique ultime.

Confiance dans l'usage fait par le service en ligne des seules données identifiant ou authentifiant un utilisateur grâce à la **minimisation** et au cloisonnement des données transmises qui deviendra la règle Cette minimisation sera de nature à décourager et à limiter la portée de toute utilisation frauduleuse des données.

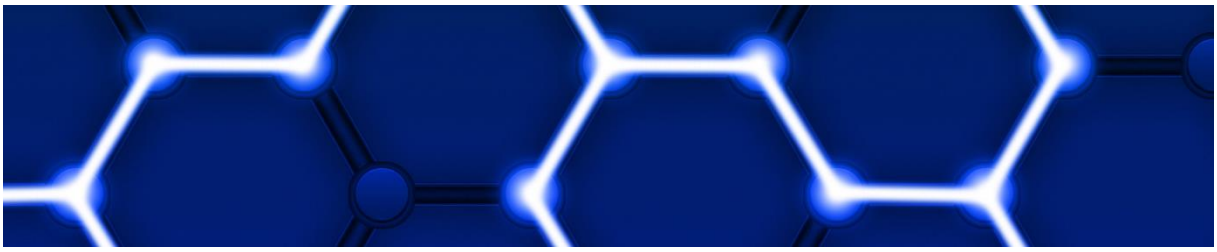
Confiance dans les allégations produites sur Internet relatives à la détention d'une qualité par une **certification appropriée** ; par exemple, les usurpations de diplômes sont certainement plus répandues, moins sanctionnées, mais tout aussi nocives pour un bon fonctionnement de la société que les usurpations d'identité.

Confiance enfin, grâce à la possibilité donnée à **chacun de s'identifier ou de s'authentifier** grâce aux données de son choix, autant pour lutter contre la crainte d'un *big brother* omniscient que celle, plus concrète, du profilage.

Confiance dans la traçabilité des actions qui pourront être mises au jour par les forces de l'ordre dans un contexte de lutte contre la criminalité et le terrorisme.

Certains que ces objectifs peuvent paraitre difficiles à concilier ; de surcroît, certains ne sont pas uniquement du ressort de l'Etat. Il importe cependant de déterminer dans quelle mesure et à quelles conditions l'utilisation de *blockchains* peut aider à les atteindre.

La section suivante présente des cas d'usage collectés au regard de ces enjeux.



4. Que peut apporter la *blockchain* à la problématique de l'identité ?

Le chapitre précédent a précisé ce que l'on entend par identité numérique et par identité pivot ainsi que les nouveaux défis associés. Afin de concrétiser les nouvelles opportunités offertes par la *blockchain*, la démarche suivie a consisté à collecter des cas d'usage proposés par les participants au groupe de travail BCID, « *blockchain* et identité».

4.1 Quelques cas d'utilisation

Voici le résultat de nos échanges portant sur la protection des données d'identité grâce à la *blockchain,* illustré de différents cas d'usage présentés par les membres du groupe de travail.

Comme on le verra, la notion d'identité s'apprécie de façon très différente selon les cas d'usage.

1-DEC : Documents d'état civil non falsifiables

Description

La fraude au passeport, à la carte nationale d'identité, à d'autres titres ou actes divers délivrés par la puissance publique ainsi qu'à certaines prestations sociales, ont conduit la commission européenne à initier un projet de norme pour sécuriser les documents sources, notamment les extraits d'acte de naissance, les attestations de mariage et les certificats de décès, mais aussi les livrets de famille et les permis de conduire [17][18].

Les solutions retenues à ce jour dans la norme en cours d'élaboration au comité CEN / TC224 WG19, sont :

- l'impression d'un sceau digital (c'est-à-dire « numérique ») visible (format éventuellement dérivé de l'OACI) sur les documents papiers, non-électroniques,
- l'impression d'un « tag » RFID sur ces documents papier,
- la mise en place d'un système de vérification à distance par interrogation de serveurs nationaux, selon le modèle du projet Européen FIDELITY[36] .

La *blockchain* mérite d'être considérée également comme une possibilité pour sécuriser les documents sources, assurer leur intégrité lors des transferts, permettre la traçabilité des demandes d'accès, des copies, des mises à jour ou des renouvellements. En effet, actuellement, lors du transfert d'actes d'état civil entre institutions, d'une mairie à une autre, il n'est pas impossible que certains éléments soient altérés. L'usage de *smart contracts* permet aussi d'envisager d'automatiser les procédures.

L'apport de la *blockchain*

La *blockchain* offre un système numérique transparent et auditable, qui assure l'intégrité des documents, actes ou titres échangés, ainsi que l'horodatage et l'ordonnancement de toutes les transactions les concernant. Lors de la rédaction d'un acte de naissance, la mairie pourrait enregistrer une attestation de l'acte rédigé sur la *blockchain,* assurant ainsi son intégrité tout au long de la vie du sujet (et au-delà). Un transfert d'actes entre mairies ne pourrait être opéré qu'après vérification de l'intégrité du document et de son authenticité : la falsification d'un document source serait immédiatement décelée par la *blockchain* et l'émetteur serait sommé de fournir la version originale.
Mieux encore, on pourrait imaginer que l'utilisation de la *blockchain* permette d'harmoniser au niveau européen la vérification des documents sources, en simplifiant les procédures rendues actuellement complexes et onéreuses par la diversité des régimes juridiques des Etats membres.

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

Les empreintes des documents sources seraient enregistrées sous la forme d'assertions vérifiables, prouvant l'intégrité du document source (y compris sa date d'émission précisément enregistrée). Un vérificateur disposant des autorisations requises pour satisfaire au contrôle d'accès serait en mesure de s'assurer que les documents présentés par une personne sont exacts et valides.

Une empreinte unique serait générée à chaque rédaction d'un acte de naissance. L'enregistrement serait horodaté, puis enregistré sur la *blockchain* (aucune modification ultérieure ne serait possible). Le transfert d'une mairie vers une autre mairie ferait l'objet d'une transaction authentifiée, préservant l'intégrité des données échangées, et donc vérifiables par le destinataire.

Les seules personnes susceptibles de disposer d'un contrôle d'accès pour écrire sur la *blockchain* seraient les agents des services d'état civil des mairies et des greffes de tribunaux habilités pour intervenir dans cette procédure.

[36] https://cordis.europa.eu/project/id/284862

2-HCV : La *blockchain* pour gérer vos documents d'habilitation à conduire un véhicule

Description

Le permis de conduire entre actuellement en phase de numérisation, en lien avec un projet de normalisation présenté sous l'égide du comité ISO SC17 WG10 (ISO/IEC 18013-5) portant sur la mise à disposition du document sur un dispositif mobile, en particulier sur *smartphone*.
Or, cette norme concerne exclusivement le permis de conduire et non les documents généralement contrôlés simultanément, qui se rapportent au véhicule comme l'attestation d'assurance, la carte grise, la fiche de contrôle technique à jour et les vignettes, lesquelles restent sous format papier. Il serait pourtant utile de permettre à l'utilisateur de disposer de tous les documents relatifs, d'une part à l'habilitation à conduire un véhicule, et d'autre part, au véhicule conduit, sous une forme numérique authentifiée, consultables sur le *smartphone* ou depuis d'autres dispositifs personnels.
Il en résulterait plus de transparence, de sécurité et de simplification pour les différentes parties prenantes, y compris pour les forces de l'ordre chargées du contrôle.
Le conducteur pourrait produire facilement la preuve de son habilitation à conduire, du bon état technique du véhicule (grâce à l'attestation délivrée pour deux ans), du contrôle de son « empreinte écologique » par la vignette « Crit'Air » et de l'attestation d'assurance.
Le contrôle de l'authenticité de ces éléments produits par les forces de l'ordre serait aussi facilité.
En cas de location de véhicule, les loueurs de voitures seraient aussi à même de contrôler rapidement l'habilitation à conduire de leur client.

L'apport de la *blockchain*

Tout un écosystème d'acteurs interagit à travers les différents documents nécessaires à la conduite d'un véhicule. La *blockchain* semble tout particulièrement adaptée au caractère décentralisé de cette architecture, où chacun des organismes habilités à délivrer une attestation pourrait l'enregistrer sur la *blockchain* sous forme d'empreintes certifiées. L'utilisation d'une *blockchain* permettrait d'enregistrer toutes ces preuves à disposition des vérificateurs, et aux utilisateurs d'accéder à leurs données certifiées, ce qui aurait pour effet de développer un écosystème de confiance en réduisant la fraude.

Seul le conducteur détiendrait sous forme numérique les documents sources relatifs à l'habilitation à conduire et au véhicule, documents qu'il pourrait consulter à tout moment, sur *smartphone* par exemple. Lors d'un contrôle ou pour tout autre usage, le conducteur serait en mesure de produire les preuves d'authenticité, d'intégrité, d'origine, de validité des documents enregistrées, lesquels seraient consultables sur la *blockchain.*

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

Dans la *blockchain*, pourraient être enregistrées par les organismes habilités, les attestations prouvant l'authenticité et la validité des documents suivants :

- permis de conduire et mise à jour du nombre de points,
- carte grise du véhicule,
- carte verte (assurance du véhicule),
- contrôle technique,
- vignette « Crit'Air ».

3-GCV : Covoiturage de confiance

Description

Il existe aujourd'hui de nombreuses plateformes de mise en relation de particulier à particulier, notamment pour les services de covoiturage. Les plateformes *web* se positionnent comme intermédiaire de confiance.
Mais de quelle confiance s'agit-il ? Ces sites assurent le service de mise en relation de personnes, mais sans fournir aucune garantie quant aux personnes ainsi mises en relation, sur la validité du permis de conduire du conducteur, de son assurance ou la date du dernier contrôle technique du véhicule. Le site procède bien à une collecte massive de ces données à caractère personnel, mais sans en effectuer la vérification. Ainsi, les utilisateurs prennent-ils contact dans le monde virtuel via des pseudonymes sur la plateforme, puis se rencontrent physiquement pour la première fois lors de l'exécution du service.
Une *blockchain* pourrait héberger les preuves de possession, d'intégrité, de validité des différents documents apportant la preuve des habilitations du conducteur et du bon état du véhicule, et ceci sans que l'intégralité des documents ne soit transmise à la plateforme.

Le covoiturage est actuellement mis en œuvre par des plateformes d'intermédiation qui fournissent ce service à de nombreux utilisateurs. Ces plateformes servent d'intermédiaire pour le paiement et éventuellement pour la gestion des litiges. Elles sont appréciées pour leur facilité d'usage et leur faible coût. Mais, non seulement la gestion par leur soin des données personnelles, ne fait pas l'objet de vérification ou de garantie, mais de surcroît cette gestion n'est pas toujours conforme au RGPD. Une analyse de ce cas d'usage, d'un point de vue technologique aussi bien que d'un point de vue juridique, est détaillée dans le Livre Blanc « Comprendre la *blockchain* à travers l'étude d'un cas d'usage : le covoiturage, *blockcar* » [19].

L'apport de la *blockchain*

La *blockchain* pourrait offrir un niveau de confiance plus élevé, en apportant la garantie de la capacité du conducteur et du bon état du véhicule, et en résolvant la problématique de l'identification des personnes qui ont pris contact par pseudonymes dans un monde « virtuel ».

Les attestations relatives à l'authentification du conducteur ou du véhicule, certifiées par les organismes qui les ont délivrées, pourraient être enregistrées sur la *blockchain*. Lors de la conclusion d'un contrat de service de covoiturage entre deux personnes, chacune aurait accès aux preuves de l'autre partie, la vérification de la preuve pouvant être effectuée lors de la rencontre physique et avant que le service ne soit conclu. Le « service fait » serait enregistré conjointement via le *smart contract*, avec la preuve de la présentation des documents en face-à-face.

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

Les données enregistrées dans la *blockchain* doivent permettre d'authentifier les parties tout en protégeant leur identité et leurs données personnelles. Une phase d'enrôlement des personnes leur permet d'obtenir un identifiant protégeant leur identité sur le système numérique décentralisé. Seules les preuves certifiées des documents d'identité sont enregistrées sur la *blockchain*. Elles sont rendues accessibles au destinataire lors de la contractualisation d'un service (de covoiturage) via un *smart contract*.

4-AUB : Achat anonymisé d'un billet électronique

Description

De nombreux biens et services sont achetés sur internet sous forme numérique. C'est le cas de titres de transport, de billets de spectacle ou de billets pour assister à des événements sportifs. Le billet numérique émis donne généralement droit à une place nominative. L'acquisition de cette place conduit à transmettre au tiers fournisseur du e-billet des éléments de notre identité. La règlementation RGPD contraint ce fournisseur à protéger nos données d'identité. Mais qu'en est-il réellement ? Qu'en sera-t-il dans le temps ? Comment la sécurité est-elle mise en œuvre chez ce fournisseur ? L'actualité récente illustre les limites des garanties offertes par les textes juridiques.

Lors de l'utilisation du billet électronique, un contrôle est effectué, généralement en face-à-face. Ce contrôle porte sur la validité du billet, et peut aussi porter sur l'identité du titulaire, ou sur un attribut de son identité, par exemple son âge, ou la possession d'une carte d'abonnement pour justifier d'un tarif préférentiel.

L'apport de la *blockchain*

L'usage d'une *blockchain* permettrait d'acquérir le billet grâce à un identifiant anonymisé, éventuellement géré de façon décentralisée. Ainsi, aucun élément d'identité n'est transmis au fournisseur de billets qui reçoit néanmoins l'assurance de la véracité des informations transmises par l'acheteur. Le lien entre l'identifiant anonymisé et l'identité physique serait enregistré sous la forme d'une preuve certifiée ou d'une attestation sur le registre de la *blockchain*, consultable par un tiers habilité. Lors d'un contrôle en face-à-face, l'attestation consultée sur la *blockchain* par le contrôleur établirait l'existence du lien entre le billet et le document d'identité présenté lors de l'achat.

Ainsi, aucune collecte de données à caractère personnel ne serait effectuée par les fournisseurs de biens et services numériques distants, lesquels ne seraient plus tentés d'exploiter les données personnelles des consommateurs à leur insu pour d'autres usages mercantiles.

Quelles sont les données à valeur « probante » enregistrées sur la *blockchain* ?

Il est nécessaire de passer par une phase d'enrôlement pour générer un identifiant anonymisé utilisable sur le système numérique. Seraient enregistrés sur la *blockchain*, la preuve d'émission du e-billet et la preuve de sa détention par l'utilisateur, lequel doit également être en mesure de prouver en face à face que son identifiant anonymisé est bien lié à certains attributs de son identité régalienne.

5-ECJ : La *blockchain* pour exécution automatique de clauses juridiques

Description

Le projet de recherche « *Smart contracts*[37] » soutenu par le Ministère de la Justice, via la mission Droit et Justice, pour une durée de deux ans (2018-2020) vise à créer une librairie de *smart contracts* mis à disposition des professionnels du droit et de la justice. Ces derniers pourront disposer d'un code informatique générique déposé sur la *blockchain* qui exécutera certaines clauses financières si les conditions requises sont remplies. Par exemple, cela pourrait concerner la mise en recouvrement des pénalités financières si un prestataire ne respecte pas les termes d'un contrat, ou encore la restitution du montant de la garantie en fonction de l'état des lieux de sortie d'un local dans une relation bailleur-locataire.

Le projet ne consiste pas à créer une librairie de données numériques identifiantes. Toutefois, dans la mesure où les *smart contracts* ont vocation à s'appliquer à des personnes publiques ou privées, morales ou physiques, les parties devront nécessairement être identifiées préalablement à l'exécution du *smart contract*.

L'apport de la *blockchain*

Le rôle des *smart contracts* consiste seulement à exécuter les clauses conditionnelles d'un acte juridique, contrat ou mise en demeure. Toutefois, étant implémentés sur une *blockchain*, ils héritent de ses caractéristiques, à savoir l'immutabilité, la sécurité, la traçabilité l'horodatage et l'intégrité.

Le groupe de recherche évalue les différents langages de programmation en fonction des critères d'expressivité, de sécurité, et de pérennité, tout en prenant en compte les performances des différentes sortes de *blockchains*.

C'est une *blockchain* publique qui convient le mieux à ce type d'usage, le caractère *permissioned* ou *permissionless* restant à apprécier au regard de la sécurité relative au mécanisme de consensus choisi, (ainsi qu'en fonction de l'empreinte énergétique).

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

Les données numériques indispensables sont celles relatives aux parties prenantes des *smart contracts*. Il n'est pas nécessairement fait mention de leur état civil; tout dépend de la clause qui est implémentée. Mais le *smart contract* doit impérativement renvoyer à des données d'identification bancaires pseudonymisées (Avis de la CNIL 2018). Un exemple de clause implémentée avec le langage *Solidity* dans le cadre du projet « *Smart Contracts* », est disponible sur GitHub[38].

Les professionnels du droit qui utiliseront les *smart contracts* de la librairie seront considérés comme des responsables de traitement au sens du RGDP. Les concepteurs de l'algorithme ou de la plateforme ne seront considérés que comme des fournisseurs de solution.
Ce qui signifie que c'est au professionnel du droit qu'incombera de justifier le recours à la « *smart contractualisation* ».

[37] https://smart-contracts.univ-grenoble-alpes.fr/
[38] https://github.com/abdou77124/clausier/tree/master

6-CEC : Création de crypto-actifs pour une économie circulaire

Description

Depuis 80 ans dans la région de Bâle en Suisse, de nombreuses entreprises utilisent le franc WIR[39]. Cette monnaie complémentaire est née en 1934 de la volonté de 15 entrepreneurs de créer une monnaie privée pour échanger entre eux dans le contexte de la grande dépression de 1929, à une époque où les banques rechignaient à consentir des prêts. Sa masse monétaire est actuellement estimée autour de 60 000 PME suisses. Quand les membres veulent commercer à l'extérieur du réseau, ils recourent au franc suisse, au dollar et à l'euro. C'est la banque WIR qui crée cette monnaie (à très bas coût, via des intérêts minimes sur les crédits). Le franc WIR n'est accessible qu'aux entrepreneurs, dans un schéma d'affaires en B2B. Son principal avantage : apporter aux entreprises participantes une forme de résilience économique en cas de crise, en créant une digue intermédiaire pour atténuer les fluctuations monétaires globales.

Une autre expérience intéressante a lieu en Angleterre, à Bristol, où une monnaie locale est en train de se développer. Dans cet écosystème, n'importe qui peut créer de l'argent, à condition que la création porte sur un montant suffisamment élevé. L'objectif est que le plus grand nombre de consommateurs possible puisse acquérir grâce à ce système monétaire les biens et les services essentiels : nourriture, électricité, transport.... Cet écosystème, qui procède de la défiance à l'égard d'un système financier international soupçonné d'être inféodé à de grandes entreprises indifférentes aux enjeux locaux, doit permettre de créer une réserve de monnaie locale au bénéfice de la communauté et favoriser ainsi le développement des entreprises locales. L'économie qui repose sur ce type de création monétaire se veut plus locale, plus écologique et résiliente en cas de crise. A la différence du franc WIR, cette monnaie locale s'adresse aux consommateurs selon un schéma B2C[40].

Ces deux exemples illustrent que des formes de (crypto) monnaies locales, ou de monnaies réservées à certains types d'activités, garantissent une certaine résilience face aux crises économiques, aident à soutenir l'économie locale et à sauvegarder des emplois. Tandis que le premier exemple en B2B nécessite d'identifier la personne morale (entreprise) à l'origine d'un paiement vers ses partenaires, le second exemple en B2C impose d'identifier le compte des consommateurs / utilisateurs. L'extension de l'usage d'une monnaie locale, aussi vertueuse soit-elle, est basée sur la confiance. La gageure consiste à garantir cette confiance.

L'apport de la *blockchain*

Ces deux types de système financiers pourraient être mis en œuvre avec des crypto-actifs adaptés aux micro modèles économiques, fondés sur des *smart contracts* qui prévoient un échange de jetons (*tokens)* grâce à une *blockchain* régulée par une gouvernance maitrisée. Chaque *token* serait échangé contre de la crypto-monnaie, et la crypto-monnaie pourrait être changée en euro ou en toute autre monnaie.

L'infrastructure fournirait et maintiendrait la sécurité du registre partagé et répliqué grâce à un mécanisme de consensus à déterminer, et supportant le crypto-actif dédié.

La *blockchain* et les *smart contracts* apporteraient de la souplesse à l'économie locale en fonction des opportunités entrepreneuriales en B2C, si toutefois la réglementation autorise les crypto-actifs à figurer dans la comptabilité commerciale. L'objectif est de soutenir des formes d'économie collaboratives entre entreprises partenaires souhaitant créer un écosystème.

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

Chaque écosystème disposerait de son livre de comptes associé à son crypto-actif sous la forme d'un *smart contract* émetteur de jetons consultable sur la *blockchain*. L'usage de crypto-actifs nécessite un enrôlement dans une économie réelle, ce qui implique la responsabilisation des acteurs, règlement des litiges et toute une régulation adaptée. Pour cela, l'identification des personnes morales (entreprises) est requise dans le monde physique, ce qui nécessite une procédure de type KYC (Know Your Customer ou Connaissance du client). Dans le cas de commerces, il peut y avoir besoin d'identifier les clients, par exemple pour le suivi de la garantie d'un bien.

[39] Cette appellation WIR vient de « *Wirtschaft* » mot allemand qui signifie « économie », mais l'abréviation « *wir* » signifie « nous » dans cette langue, ce qui renvoie à l'ancrage local du crypto-actif.

[40] *Business to consumer*, soit entre entreprise et consommateur.

7-ACE : Autoconsommation d'énergie en copropriété

Description

Depuis 2017, la réglementation française encadre l'autoconsommation collective d'électricité (décret du 30 avril 2017 n°2017-676 [16] autorisant l'autoconsommation collective d'électricité). Au sein d'une copropriété ou d'un « îlot énergétique » disposant de ses propres sources d'énergie verte (panneaux photovoltaïques, géothermie…), les habitants peuvent se fédérer pour gagner en autonomie. Chacun pouvant devenir un « consom'acteur »[41] d'énergie.
La mise en œuvre d'un tel système implique une gestion fine des flux d'énergie dont la production est collective et la consommation individuelle.
Doivent être pris en compte :

- la gestion de la demande en fonction de la quantité d'énergie produite,
- l'équité de la répartition susceptible de donner lieu à un intéressement financier ou en nature (notion d'*incentive*),
- la gestion des surplus : stockage ou revente de la production excédentaire collective (par une borne de recharge par exemple),
- la répartition de la facturation (pour la maintenance des installations).

L'énergie produite étant un bien collectif, celles des données personnelles qui sont associées à la production sont consultables par tous les occupants. En revanche, chaque habitant pourrait garder le contrôle et la gestion de ses données personnelles de consommation, données relatives à son logement et à son identité. L'intéressement et la facturation seraient individualisés, ce qui nécessiterait seulement le partage de certaines données personnelles avec un tiers. Ci-dessous, une vue simplifiée du système.

L'apport de la *blockchain*

- L'usage de *smart contracts* opérés par une *blockchain* permettrait d'apporter aux « consom'acteurs » la transparence de la gestion des flux d'énergie dont la collectivité est bénéficiaire.
- Chacun aurait le contrôle de ses données, stockées dans un espace personnel.
- Les droits d'accès et les autorisations pourraient être gérés par des *smart contracts*, ainsi que les preuves de divulgation des données à un tiers.

Quelques verrous technologiques restent à lever :
- pour transmettre à des tiers en toute confidentialité des données à caractère personnel nécessaires aux opérations de facturation,
- pour certifier et tracer la source de l'énergie,
- pour garantir le respect de la vie privée des « consom'acteurs » sur le système numérique tout en permettant leur identification au sein de la copropriété.

Quelles sont les données à valeur « probante » à enregistrer dans une *blockchain* ?

L'adhésion des « consom'acteurs » au règlement commun de partage de l'énergie pourrait être enregistrée dans la *blockchain* via un *smart contract*. La *blockchain* permettrait de tracer en temps réel toutes les données de la partie collective du projet : production d'énergie, stockage, consommation globale, transfert sur le réseau électrique national, tout en préservant la confidentialité des données de consommation individuelle.

[41] Terme désignant un acteur ayant un double rôle de consommateur et de producteur.

4.2. Analyse des cas d'usage

Les cas d'usage présentés à la section 3.1 illustrent des besoins liés à l'usage de l'identité numérique ou à certaines données personnelles dans les domaines de l'énergie (7-ACE), de la mobilité (2-HCV, 3-GCV), de l'état civil (1-DEC, 2-HCV, 4-AUB), de services administratifs de l'Etat ou de l'autorité judiciaire (1-DEC, 2-HCV, 5-ECJ), de la finance, du commerce et de l'économie (4-AUB, 6-CEC, 7-ACE). Bien entendu, ces exemples ne sont pas limitatifs. Des besoins analogues peuvent être observés dans d'autres domaines comme, par exemple, la santé.

4.2.1 Vers un bon usage de la *blockchain* pour l'identification

L'identité numérique est au cœur des enjeux de l'économie numérique : on sait que la détention des données personnelles des utilisateurs constitue l'une des bases du modèle économique des géants du numérique et de quelques autres acteurs du système. Pour l'instant, les écosystèmes d'identité existants sont assez peu adaptés aux nouveaux défis tels que la protection de la vie privée (RGPD), la mise en conformité avec les nouvelles régulations anti-fraude, ou encore avec la prévention du vol d'identité.

Or, si on se réfère à la section 3 qui porte sur l'analyse juridique du sujet de l'identité des personnes, le principal besoin identifié porte sur la protection de la vie privée. La *privacy* englobe aussi bien ce qui touche à la protection de son identité, que ce qui concerne la protection des données personnelles dans leur ensemble.

Dans le monde numérique, cette notion de *privacy* fait apparaitre une tension entre le besoin d'être anonyme sur les systèmes numériques ou sur internet, et le besoin d'assurer la sûreté et la sécurité dans l'espace social, de permettre la résolution des litiges et l'exercice de la justice.

La **souveraineté** de l'Etat, qui s'est toujours affirmée à travers la maîtrise de l'état civil et qui y trouve matière à se renouveler grâce au numérique, se confronte à cette tension, internet étant devenu un monde à part et presque sans frontière ; il est difficile pour les Etats souverains d'y faire respecter leur législation sur les données de leurs ressortissants et de leurs résidents. Aussi devient-il urgent de poursuivre le développement de solutions respectueuses de nos valeurs et de notre culture, qui protègent l'identité des individus et évitent son usurpation et sa marchandisation.

Reste à démontrer que la *blockchain* est capable d'aider l'Etat à concilier la démarche en faveur de la protection de la vie privée avec la sécurité et le respect de l'ordre public, également dans l'espace numérique.

Or dans tous les cas d'usage présentés à la section 4.1, il est question d'**identification ou d'authentification**. L'identification nécessite généralement une phase initiale d'enrôlement qui consiste à attribuer à une personne un identifiant associé à des moyens d'identification, qui peuvent être variés comme un login/mot de passe, de la biométrie (empreinte digitale, reconnaissance faciale, son de la voix), un code PIN, une adresse IP… Quel que soit le moyen d'identification, l'identifiant attribué à un individu est unique.

C'est parfois l'identification qui permet au sujet de s'authentifier, c'est-à-dire de se faire reconnaitre comme détenteur d'un droit ou titre. En pratique, l'authentification ne passe pas nécessairement par l'identification (la faculté de nommer une personne). Mais dans de nombreux contextes, l'**authentification** est subordonnée à la capacité d'apporter la preuve de son identité. Cette preuve est liée à la façon dont le sujet est repéré sur le système et peut s'opérer différemment selon que l'authentification/identification a lieu à distance ou bien en face-à-face.

Nous avons vu dans la section 3 que la numérisation des échanges expose à de nouveaux périls d'identification intempestive du fait du partage des données de plus en plus fréquent dans les opérations courantes de la vie quotidienne. Ce faisant, elle expose aussi à une augmentation des risques d'usurpation d'identité, soit dans le but de disposer à notre place de nos biens et s'arroger nos droits, soit simplement dans une volonté de nuire à notre réputation. Indépendamment du risque d'identification non souhaitée, la simple « individualisation », sans mise au jour de nos noms et prénoms, peut se révéler aussi dommageable pour la victime, sans parler des effets « liberticides » du profilage. Tous ces dangers sont démultipliés par les possibilités nouvelles ouvertes par l'intelligence artificielle qui permet de porter l'industrialisation de la malveillance à des niveaux d'efficacité jusqu'alors insoupçonnés.

Une authentification sans identification sur les réseaux s'avère beaucoup plus protectrice de nos données personnelles par la minimisation des données communiquées qu'elle permet : l'exposition à la malveillance et aux attaques de toute nature est beaucoup plus réduite.

Pour autant, dans de nombreux cas d'usage**, il est fondamental de pouvoir recourir à la sécurité offerte par la garantie étatique de l'identité juridique** (forme de certification) qui procède de l'état civil régalien. Les différents schémas ou solutions d'identification sont encadrées par les autorités nationales, responsables de la sureté des citoyens et de leurs biens, du contrôle aux frontières, du respect des règlementations nationales et européennes telles que eIDAS et le RGPD. Tous les cas d'usage présentés dans la section 4.1 requièrent l'enregistrement de preuves vérifiables pour protéger ou renforcer la protection de la vie privée dans un contexte décentralisé où les données sont sous le contrôle de l'utilisateur, et fondées sur une identité régalienne protégée par l'Etat. Dans les cas les moins sensibles, la certification de l'identité peut être assurée par un tiers de confiance privé habilité.

4.2.2 Fonctions administratives en lien avec l'identité

Le cas d'usage relatif à l'échange d'actes d'état civil (1-DEC) illustre le besoin d'assurer l'intégrité des actes d'état civil tout au long de la vie (et au-delà…). Dans ce cas, l'*empowerment* concerne les services de l'administration devenue ainsi plus résiliente et mieux armée face à la fraude. Ce type d'architecture sur *blockchain* pourrait notamment être utilisée par les services pour mutualiser entre services répertoriés une information confidentielle et sensible.

L'administration gagnerait aussi à la mise en place du projet relatif au portfolio de documents habilitant à la conduite et au véhicule considéré (2-HCV) ; l'utilisation de la *blockchain* est un outil qui faciliterait le contrôle opéré par les forces de l'ordre. De façon générale, les vérificateurs et responsables d'audit, tous secteurs confondus, sont très favorables à la *blockchain* qu'ils considèrent comme un outil qui simplifierait leur travail.

Le cas d'usage relatif à l'automatisation des transferts financiers développés par l'autorité judiciaire (5-ECJ) ouvre des perspectives. Ce sont plutôt les fonctionnalités d'automatisation des *smart contracts* qui sont recherchées dans ce cas, leur exécution sur une *blockchain* conférant à l'application résilience, traçabilité et transparence.

Les services liés à l'état civil (1-DEC, 2-HCV) requièrent la vérification de l'identité pivot, c'est-à-dire des données essentielles qui constituent l'identité juridique régalienne. La règlementation européenne eIDAS crée un niveau d'identification élevé. On pourrait imaginer de créer ce même niveau d'exigence pour qualifier l'exécution de clauses juridiques (5-ECJ).

4.2.2 La protection des données personnelles : l'authentification sans identification

L'emploi d'une *blockchain* mise en œuvre en complément d'autres infrastructures dans un système complexe pourrait aider à dissocier identification et authentification. Par l'usage du numérique, il s'agirait de conférer des droits aux individus sans qu'ils aient besoin de justifier de leur identité, tout du moins tant qu'ils ne sont pas sujets à un contrôle (contrôle aux frontières, contrôle routier…) par une autorité habilitée (2-HCV).

Tandis que l'usage d'un crypto-actif requiert la connaissance du titulaire du compte (selon les pratiques de KYC « *Know Your Customer* ») pour des activités de commerce (6-CEC), il n'est pas souhaitable qu'un site en ligne distant proposant des biens ou des services marchands ait connaissance de l'identité du consommateur (4-AUB). De même, dans l'application de covoiturage (3-GCV), les partenaires, passager et conducteur, n'ont pas besoin de s'identifier, c'est-à-dire de décliner leur nom et prénom, mais seulement de se reconnaitre comme étant les co-contractants en ligne. La *blockchain* peut fournir un moyen d'authentification, doublé de l'assurance pour le passager que le conducteur possède toutes les habilitations requises par la loi.

Pour d'autres cas d'usage, comme 2-HCV ou 7-ACE, il s'agit de prouver qu'on est bien le possesseur d'un document ou d'une donnée personnelle (de consommation par exemple). Dans l'exemple 4-AUB, seuls certains attributs d'identité peuvent être divulgués pour justifier d'un avantage tarifaire par exemple.

4.2.3 Souplesse d'une architecture permettant un accès différencié et sélectif à l'information

La capacité de la *blockchain* à s'adapter à la complexité d'un écosystème d'acteurs disposant de droits différenciés d'accès aux données, est illustrée par le cas d'usage relatif à l'autoconsommation d'énergie (7-ACE). Certaines données de copropriété sont accessibles à tous les acteurs, tandis que d'autres restent confidentielles.

Cette capacité de permettre la sélection des attributs d'identité à divulguer en fonction du service sollicité fait de la *blockchain* un outil particulièrement utile à l'heure du partage des données sur internet.

Et parmi ces données partagées figurent en tout premier lieu les données bancaires. C'est sans doute, pour cette raison que le système bancaire, en France et ailleurs, s'est très vite emparé de la *blockchain*.

4.2.4 Adaptation à un système complexe pour « encapacitation » de l'utilisateur

L'analyse des cas d'usage fait apparaitre des besoins liés à la gestion de l'identité numérique qui correspondent partiellement aux caractéristiques des systèmes permettant aux personnes morales et physiques d'héberger leur propre identité sur leur dispositif personnel et de ne fournir à ce service, que les attributs d'identité nécessaires à l'usage, éventuellement en s'appuyant sur des tiers de confiance habilités à valider l'identité. Pour correspondre plus complètement aux besoins des cas d'usage, le recours à la certification par l'Etat est un complément nécessaire pour créer une infrastructure de **confiance**.

Le concept de *Self-Sovereign Identity*, qui peut être traduit en français par l'auto-détermination informationnelle, est issu du droit allemand. La loi fédérale du 20 décembre 1990 sur la protection des données, modifiée ultérieurement, a remplacé la loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données. Avec la loi fédérale de 1977, l'Allemagne avait été le premier pays à se doter d'un texte général sur la

protection des données personnelles. L'abrogation de la loi de 1977 fut notamment la conséquence de l'arrêt rendu par la Cour constitutionnelle en 1983 sur la loi relative au recensement de la population. La Cour constitutionnelle dégagea en effet à cette occasion un nouveau droit constitutionnel : le droit à l'autodétermination informationnelle, c'est-à-dire le droit pour chaque individu de décider lui-même de la communication et de l'emploi des informations le concernant.

Ce système qui place l'utilisateur au centre du dispositif met en œuvre un système décentralisé orchestrant plusieurs rôles (cf. Figure 5) :

- Les utilisateurs qui opèrent depuis un dispositif personnel
- Les prestataires de service
- Les fournisseurs d'identité numérique
- Les certificateurs d'attributs d'identité et/ou de documents source (organismes habilités)
- Les vérificateurs

Le **prestataire de service** peut déléguer à un vérificateur la tâche de contrôle des éléments d'identité fournis avant d'autoriser l'utilisateur à bénéficier du service.

Un rôle d'auditeur indépendant, mandaté en cas de litige, peut être ajouté. Ce rôle est indispensable dans un contexte régalien pour défendre les intérêts de citoyens et/ou des intérêts économiques.

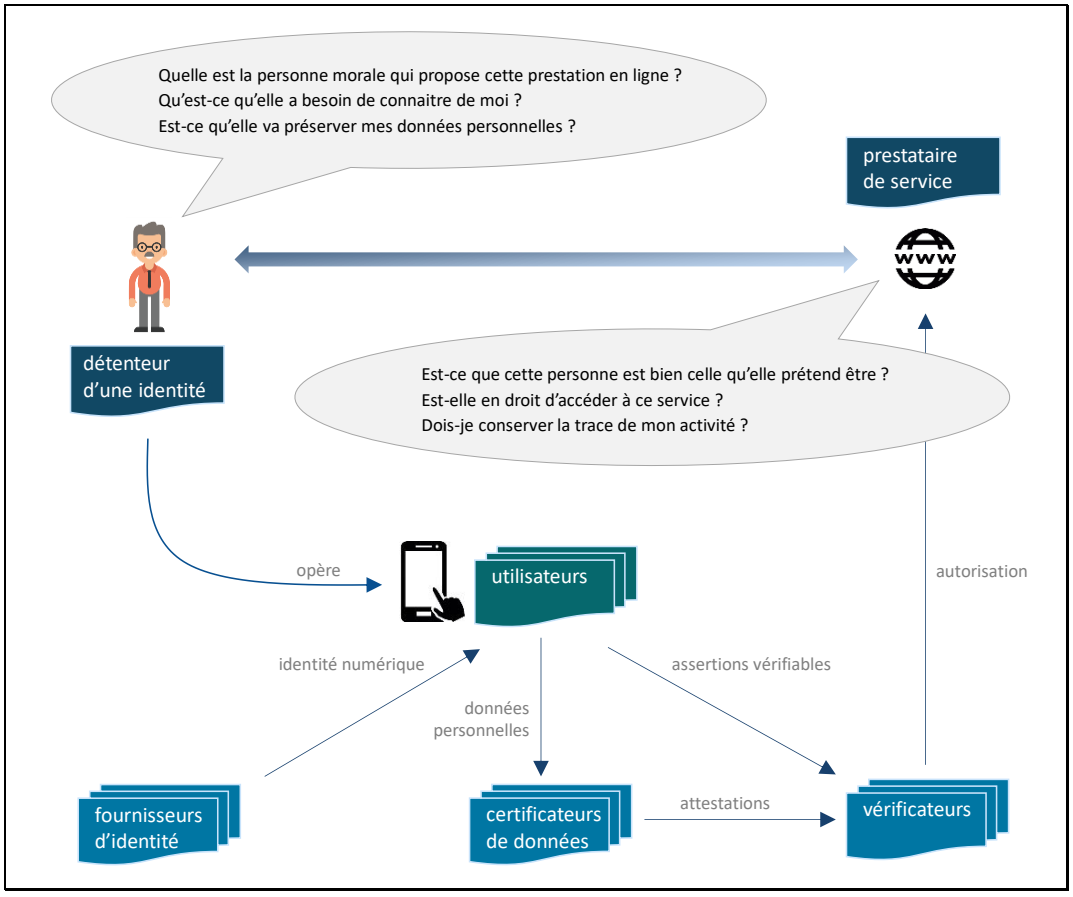


Figure 5 : liens entre les différents rôles dans un système de SSI

La présence de plusieurs acteurs ou organismes, qui incarnent chacun de ces rôles dans une architecture décentralisée, justifie d'orchestrer l'ensemble des acteurs et utilisateurs, ainsi que le flux d'information autour des *smart contracts*. Ceux-ci peuvent s'exécuter sur une *blockchain*. A ce stade, l'écosystème mis en œuvre autour d'une *blockchain* pourrait s'inscrire dans une solution fédérative de

type FranceConnect, ouverte aux services privés et permettant, par la minimisation des éléments communiqués, de remplacer une identification maximaliste par une authentification sélective, orientée sur le service dont l'usage est sollicité.

4.2.5. Vocation discriminante fonctionnelle et locale de la *blockchain*

Enfin, une autre caractéristique de la *blockchain* apparait à la lecture des différents cas d'usage. C'est son caractère sélectif et discriminant dans le choix des ayants droit.

En contradiction avec le succès planétaire rencontré par la *blockchain* publique et *permissionless* du *Bitcoin*, la plupart des cas d'usage évoqués concernent des *blockchains* privées, *permissionned* (n'y contribue pas qui veut).

Comme il a été dit plus haut, cette sélectivité des membres la rend particulièrement opérationnelle pour des usages administratifs comme ceux relatifs à l'état civil ou à l'automatisation des contrats, condamnation ou pénalités imposés par l'autorité judiciaire ou directement par le pouvoir administratif. Dans ce cas, seules les personnes compétentes fonctionnellement, « ayant à en connaître » disposeront des droits d'accès, conformément à la pratique administrative actuelle : mairie, notaires, greffes de tribunaux, policiers.

Mais, en vertu de sa sélectivité, la *blockchain* est aussi particulièrement appropriée à un usage local comme en témoignent les cas d'usages sur l'autoconsommation d'énergie (7-ACE), la création de monnaie locale (6-CEC) ou le covoiturage (3-GCV) qui a vocation à être mis en place par des collectivités locales ou des établissements de regroupements intercommunaux.

La *blockchain* crée entre ses membres une confiance qui peut venir redoubler la proximité géographique et qui en fait une technologie candidate pour toutes les initiatives locales. Elle peut venir en support d'une politique de décentralisation et de déconcentration politico-administrative.

4.3. Quelle justification majeure pour employer ces technologies émergentes ?

4.3.1 Qu'apporte une *blockchain* en plus de l'existant ?

L'énumération des avantages portés par la *blockchain*, comme système centré sur l'utilisateur et ainsi sur son dispositif mobile (voir section 5.3), ne suffit désormais pas à répondre à la question récurrente « Pourquoi un système de vérification centralisé et sous l'autorité d'une seule instance publique ou privée ne suffirait-il pas à réaliser globalement le même objectif ? »

S'il n'y avait qu'une seule instance en charge du rôle de vérificateur et/ou une seule instance habilitée à enregistrer les données (écrire et certifier les transactions dans la *blockchain*), un système centralisé client/serveur pourrait tout aussi bien en assurer la vérification.

L'emploi de la technologie *blockchain* est pertinent lorsqu'il est question d'interconnecter vérificateurs et fournisseurs d'attributs au bénéfice des utilisateurs, en particulier lorsque les conditions figurant ci-dessous sont réunies :

- Existence de plusieurs fournisseurs de données indépendants les uns des autres (fournisseurs d'identité numérique, ou d'attributs d'identité, fournisseurs de documents certifiés, fournisseurs d'attestations…) censés enregistrer et maintenir les données propres à leur activité respective en lien avec le cas d'usage.
- Existence de plusieurs vérificateurs indépendants les uns des autres mais concernés par le cas d'usage devant vérifier la conformité des assertions numériques et des preuves délivrées

par les utilisateurs afin de leur autoriser l'accès physique ou numérique et l'obtention d'un droit.

- Pluralité des acteurs impliqués dans le cas d'usage, qu'ils soient fournisseurs, utilisateurs ou vérificateurs, indépendants les uns des autres.

Ces critères permettent d'apprécier la pertinence de la *blockchain*, face à des systèmes centralisés fédératifs.

Cette analyse est corroborée par l'étude du *World Economic Forum* [23] qui décrit les systèmes d'identité distribués comme les plus appropriés pour répondre au besoin de cas d'usage incorporant un grand nombre de fournisseurs d'identité et de prestataires de service, pour offrir à l'utilisateur du confort, le contrôle sur ses données et la protection de sa vie privée en ligne.

Un système centralisé pourrait également répondre à ces exigences, la différentiation entre système centralisé, système décentralisé et *blockchain* se situant essentiellement du côté des exigences de transparence et d'« encapacitation » de l'utilisateur.

Les services rendus par la *blockchain* peuvent être résumés comme suit : une solution distribuée facilitant et améliorant la procédure de vérification - identification et authentification - par l'utilisateur ou par une personne morale, pour l'accès et l'obtention de services ou pour la fourniture de preuves numériques [20] à toutes fins utiles (telles que la preuve de notarisation, la preuve d'antériorité, la preuve d'intégrité, la preuve de propriété, la preuve d'authenticité, la preuve d'un droit…).

La *blockchain* apparaît ainsi comme une brique technologique venant compléter les fonctionnalités des systèmes existants, y compris des systèmes centralisés, en offrant une technologie efficace pour l'échange de transactions, l'échange de preuves authentifiées ou encore d'attestations. Le processus de vérification peut s'appuyer avantageusement sur une *blockchain*, tout en garantissant à l'utilisateur confidentialité et moyen de se réapproprier l'usage des attributs d'identité ou données personnelles.

4.3.2 Quel intérêt pour une solution de *Self-Sovereign Identity* ?

Le concept de *Self-Sovereign Identity* (SSI) cherche à ouvrir l'identité numérique à plusieurs autorités émettrices d'attestations différentes dans un même système. Afin que cette nouvelle forme d'identité soit vérifiable et à valeur probante, les différents acteurs du système (fournisseurs de services, autorités certificatrices et utilisateurs) doivent se faire mutuellement confiance. Mais, au contraire de la fédération d'identité, il n'existe pas dans le concept de SSI d'acteur central naturel pouvant apporter cette confiance. La *blockchain* étant une technologie qui a été créée pour résoudre ce type de problème, c'est un candidat naturel pour une implémentation de SSI.

Dans une étude récente [21], les auteurs présentent un travail conséquent qui consiste à recenser les solutions de management de l'identité basées sur la *Self-Sovereign Identity,* et de les évaluer selon des critères de performance, d'implémentation, et des propriétés requises pour la gestion de l'identité (les dix propriétés décrites par Christopher Allen [22] et le support d'assertion vérifiable). Cette étude conclut que bien que la technologie *blockchain* ne soit pas indispensable pour la mise en œuvre d'une solution de *Self-Sovereign Identity*, elle apparait comme une excellente fondation pour construire un système décentralisé, de par les multiples avantages et propriétés qu'elle fournit.

La section suivante présente le concept de *Self-Sovereign Identity*, les notions associées, les solutions existantes, ainsi que les choix d'implémentation.

5. La *Self-Sovereign Identity*

L'identité auto-souveraine ou « autodétermination informationnelle » (*Self Sovereign Identity*, SSI) est l'expression utilisée pour évoquer la faculté pour un individu de détenir et de contrôler la numérisation de son identité sans l'intervention d'une entreprise centralisant les données[42] ou d'une autorité administrative. Cette configuration n'exclut nullement le fait que l'identité juridique demeure garantie par l'Etat : elle permet seulement à l'individu de rester maître de la communication de ses données personnelles dans un contexte autre qu'administratif et régalien, y compris en usant d'un pseudonyme. Ce schéma offre aux individus la possibilité d'interagir dans le monde numérique avec la même liberté et la même confiance que dans le monde physique.

Dans le monde physique, les informations relatives aux individus (date de naissance, nationalité, diplômes universitaires, droits de propriétés intellectuelles…) sont présentées sous forme de titres ou de certificats détenus par le titulaire de l'identité dans son portefeuille ou dans un endroit sûr, et sont présentés lorsque la personne doit décliner son identité ou rapporter la preuve de la détention d'un attribut ou d'une qualité en rapport avec cette identité.

Le concept de *Self Sovereign Identity* désigne la faculté de bénéficier des mêmes facilités et des mêmes garanties d'autonomie personnelle sur Internet que dans le monde physique, grâce à un système de gestion sûr et fiable de l'identité. Cela signifie que l'individu (ou l'organisation) gère les éléments qui composent son identité et contrôle l'accès à ses informations d'identification numérisées. Avec la *Self Sovereign Identity*, le pouvoir de contrôler les données personnelles appartient bien à l'individu, grâce à l'intervention d'un tiers habilité requis pour apporter sa garantie, à la façon d'un tiers de confiance.

Plus concrètement, cette « encapacitation » (ou *empowerment*) repose sur la possibilité d'utiliser un portefeuille numérique et d'authentifier sa propre identité à l'aide d'informations d'identification (ou attributs, ou données personnelles) délivrées par des institutions diverses. Sous réserve d'une mise en œuvre adaptée, il n'est plus nécessaire d'abandonner le contrôle de ses informations personnelles à des dizaines de bases de données chaque fois que l'on souhaite accéder à de nouveaux biens et services, avec le risque d'utilisation non contrôlée ou même de vol d'identité que cela implique.

Selon ce schéma, chaque personne peut désormais contrôler l'usage de son identité. L'existence numérique d'une personne peut désormais s'affirmer indépendamment de toute organisation, l'organisation étatique demeurant cependant le garant ultime de cette identité.

5.1. Présentation de la *Self-Sovereign Identity*

Il existe actuellement plusieurs catégories d'identité numérisée :

- Identité régalienne, attribuée par l'État,
- Identité institutionnelle (celle utilisée par la banque et les différentes institutions, étatiques ou non, qui doivent renvoyer à l'identité régalienne),

[42] de type GAFAMI ou BHATX.

- Identité déclarative auto-déterminée par un utilisateur, un groupe, un consortium ou une fédération, utilisée pour accéder à un service privé ou propre à un domaine d'activité,
- Identité sociale (les traces laissées sur les réseaux sociaux), et plus généralement les traces numériques résultant de l'utilisation de services en ligne.

Il résulte de ces catégories d'usages de l'identité (qui ne sont pas placées sur le même plan), de nombreuses duplications, un gros risque de perte des données lorsqu'une des bases de données est attaquée, et un problème de confiance entre les différents acteurs qui détiennent des éléments identifiants. Depuis plusieurs années, on a constaté une évolution de la gestion des données d'identification numérisées, passant d'une identité numérique centralisée propre à un seul opérateur, à un identifiant fédéré, voire parfois distribué, fourni par un unique **fournisseur d'identité** tel que Google, Facebook...

A cela s'ajoutent les évolutions des usages et des technologies disponibles pour assurer un niveau de confiance suffisant. On assiste actuellement à l'émergence de nombreuses architectures reposant sur le concept de **fédération d'identités**. Ce concept repose sur la compatibilité entre une identité et des moyens d'identification et d'authentification mis en commun par différents services et organisations. Il est principalement mis en œuvre par l'interconnexion de systèmes séparés via l'utilisation d'un protocole commun pour l'authentification et/ou par les autorisations liées à une identité, en utilisant par exemple un login/mot de passe créé pour un service donné dans le but d'accéder à un autre service. Le recours croissant au système de fédération d'identités a favorisé la collecte de données par les différents acteurs fournisseurs de services selon un modèle « *data-centric* »[43]. Depuis quelques années, d'autres approches sont envisagées pour préserver le respect de la vie privée grâce à une meilleure séparation entre fournisseurs d'identités et consommateurs d'identités. Des mécanismes d'anonymisation sont progressivement introduits et une décentralisation plus forte via les technologies *blockchain* combinées à une approche « *user-centric* » permettent d'envisager une architecture décentralisée, voire distribuée, de la gestion de l'identité compatible avec le principe de « *privacy-by-design* ».

5.1.1. Les évolutions et les enjeux des systèmes

L'identité numérique est au cœur des enjeux de l'économie numérique : on sait que la détention des données personnelles des utilisateurs constitue l'une des bases du modèle économique des géants du numérique et de quelques autres acteurs du système. Pour l'instant, les écosystèmes d'identité existants sont assez peu adaptés aux nouveaux défis tels que la protection de la vie privée (RGPD), la mise en conformité avec les nouvelles régulations anti-fraude, ou encore avec la prévention du vol d'identité.

Historiquement, les architectures des systèmes de gestion de l'identité numérique sont passées par les étapes suivantes (Figure 6) :

- Des **architectures centralisées** « *data-centric* » s'appuyant sur une autorité centrale, par exemple des services d'annuaire (*Active Directory*, LDAP_*Lightweight Directory Access Protocol*…) ou sur une infrastructure à clés publiques (PKI) avec des autorités de certification et de vérification gérant le cycle de vie de l'identité.
- Puis, des **architectures fédératives** « *data-centric* » interconnectant les systèmes centralisés avec des interfaces pointant sur les différents silos d'identification. Pour cela, des concepts comme l'authentification unique (SSO) et l'identité de fédération ont été inventés en

[43] FranceConnect fonctionne par exemple actuellement comme une fédération d'identités.

s'appuyant sur des protocoles tels que Kerberos, Radius, SAML (*Security Assertion Markup Language*), *OpenID Connect*, *OpenID*, *OAuth*…

- Plus récemment, une troisième génération d'architectures de gestion d'identité est apparue, les **architectures décentralisées** « *user-centric* », qui offrent aux utilisateurs la possibilité de gérer par eux-mêmes leurs données personnelles et de ne transmettre que des jetons ou des références sur leurs données vers une base de données centrale. Le protocole DESIRE[44] [53] est un exemple de ce type d'architecture exploitant la notion de « *differential privacy* »[45].
- Les **architectures distribuées** se sont fait connaitre ces dernières années avec notamment la *blockchain* mettant en œuvre un registre de comptes ou de données répliqué et partagé entre les nœuds du réseau, mais surtout étant consultable de façon transparente par tous les acteurs du système. Ce qui distingue les architectures décentralisées et distribuées, c'est la gouvernance du *back-end*[46], du ressort d'une autorité dans le cas décentralisé et relevant généralement d'un consortium dans le cas distribué.

La technologie des registres distribués (*Distributed Ledger Technology*, DLT) se distingue de la technologie *blockchain* par la gouvernance du *ledger*. Celle-ci est partagée par différents acteurs, en principe indépendants, qui assurent la disponibilité du système et maintiennent l'état du *ledger* au cours du temps dans le cas des *blockchains*. C'est le cas des *blockchains permissionless* BitCoin et Ethereum mises en œuvre selon une architecture distribuée. En revanche, les DLTs sont mis en œuvre selon une architecture décentralisée déléguant à un seul acteur positionné comme tiers de confiance, le maintien du *ledger*. C'est notamment le cas d'Hyperledger Fabric[47].

La nouveauté essentielle introduite par les architectures centrées sur l'utilisateur (*user-centric*) tient au fait qu'au lieu de céder « gratuitement » (et quasi automatiquement) leurs droits sur toutes leurs données personnelles en échange d'un service, les utilisateurs peuvent, grâce aux identifiants décentralisés, sélectionner les données, attributs et assertions qu'ils acceptent de divulguer. Cette évolution redonne aux utilisateurs le contrôle sur l'exploitation de leurs données personnelles, et se révèle adaptée au RGPD. Elle apparaît comme un moyen de s'y conformer, même s'il reste encore des questions à résoudre telle que le droit à l'oubli. Toutefois, seules les références aux données anonymisées, et non les données elles-mêmes, sont stockées sur la *blockchain*, aucune information personnelle n'y figurant. Il convient tout de même de rester vigilant sur le droit à l'oubli, car les moyens d'analyse de données sont de plus en plus performants avec notamment l'utilisation de l'intelligence artificielle. Associés à des attaques de cryptanalyse, également de plus en plus performantes, pouvant cibler des données anonymisées, l'identification d'utilisateurs ou leur traçabilité pourrait être facilitées dans un avenir proche.

[44] *https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE*
https://hal.inria.fr/hal-02568730/document

[45] *https://en.wikipedia.org/wiki/Differential_privacy* (confidentialité différentielle)

[46] Serveurs et bases de données effectuant un service de type « *cloud* », distant de l'utilisateur.

[47] Hyperledger Fabric est géré par IBM, et il n'est pas exclu que le *ledger* ne soit répliqué que dans le *cloud*, voire dans le *data center*, propriétaire.

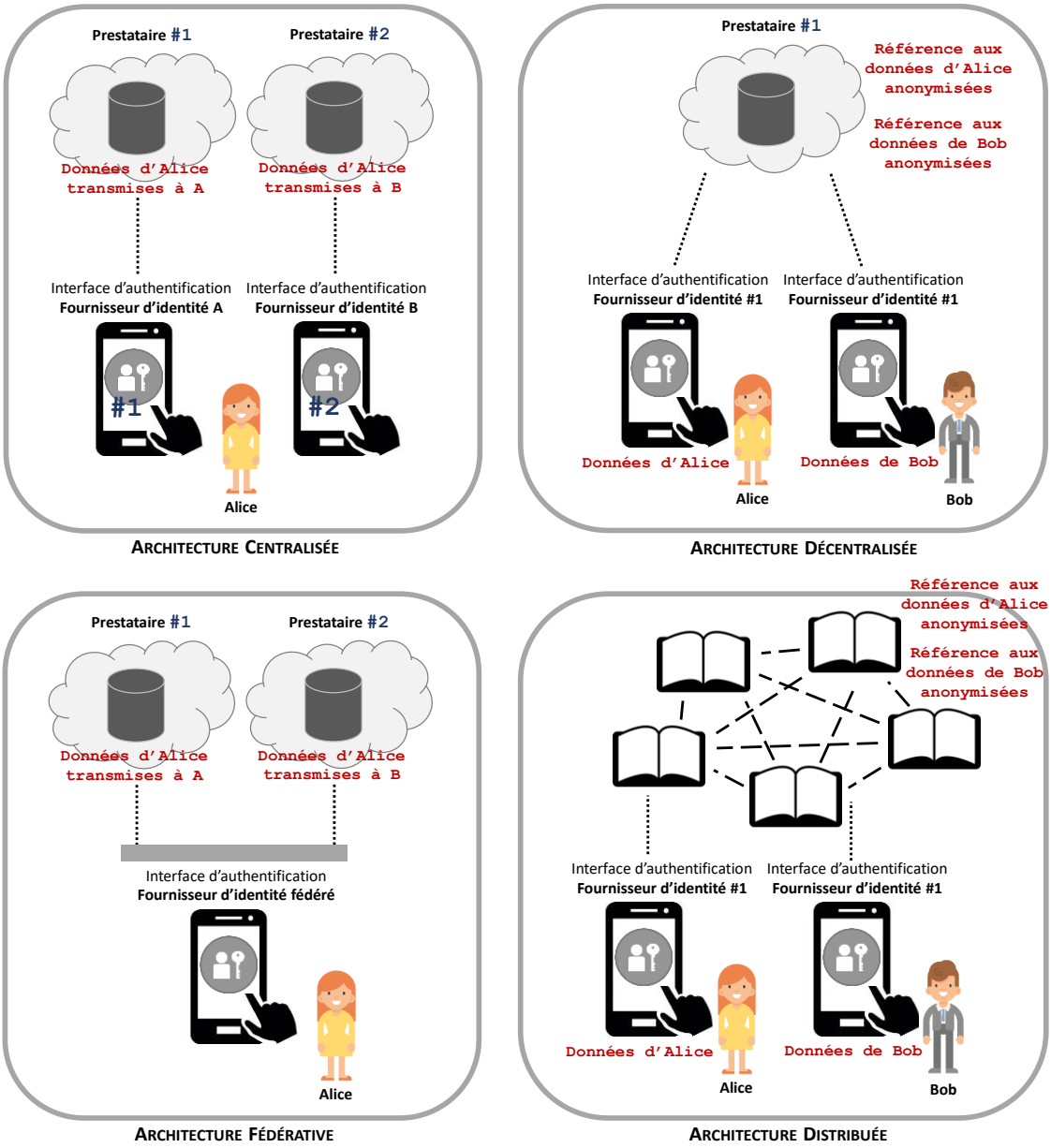


Figure 6 : architectures des différents systèmes d'information

Le W3C a fourni un modèle de données destiné à être utilisé comme *Verifiable Presentation,* c'est à dire comme assertions sujettes à la vérification d'un acteur appelé « vérificateur », ainsi qu'un modèle de conditions déclaratives limitant l'usage des assertions « pour servir et valoir ce que de droit », qui figurent, codées sur le *Verifiable Presentation* dans la section dite « *Terms of Use* » [26].

Grâce à ces éléments associés à la cryptographie dite de divulgation sélective ou encore à la cryptographie dite « *Zero-Knowledge Proof*[48] » (ZKP), il est possible à l'utilisateur de prouver l'authenticité d'un document en sa possession, certifié par un organisme habilité (par exemple, une attestation de diplôme), ou encore d'attester la véracité d'attributs de son identité (par exemple, avoir plus de 18 ans ou être majeur).

[48] https://en.wikipedia.org/wiki/Zero-knowledge_proof

L'implémentation d'une solution de *Self-Sovereign Identity* avec une *blockchain* exploite principalement deux techniques visant à minimiser les données sources transmises et à effectuer les vérifications nécessaires quant à leur intégrité et authenticité :

1. **la divulgation sélective d'attributs d'identité** qui consiste à minimiser les données transmises à son interlocuteur. Par exemple, pour s'inscrire dans un club de sport il suffit de fournir un certificat médical valide. Le document transmis est accompagné d'une preuve d'authenticité sous la forme d'un élément cryptographique émis par une autorité ou un organisme reconnu, certifiant que les données, documents ou attributs d'identité sont exacts et authentiques. La preuve d'authenticité est normalisée par le standard ISO/IEC DIS 18013-5 sous l'appellation "*Mobile Security Object*" [53] qui a fait le choix d'utiliser une méthode de divulgation sélective. Il faut noter que le principe de divulgation sélective peut être implémenté de différentes manières.
2. **les assertions vérifiables** qui sont présentées tout en préservant la confidentialité de certaines informations par l'utilisation de preuves de connaissance à divulgation nulle (ZKP) sont des déclarations de type « je suis majeur(e) », dont la justification est garantie par des éléments cryptographiques. Une assertion vérifiable est formée d'un ensemble de métadonnées infalsifiables et d'éléments cryptographiques permettant d'authentifier l'émetteur.

5.1.2 Le modèle *Self-Sovereign Identity* dans un contexte de souveraineté

En pratique, on observe que pour la plupart des solutions de SSI, les trois éléments sur lesquels s'appuie l'implémentation de la *Self-Sovereign Identity* sont :

- des clés et fonctions cryptographiques,
- des identifiants décentralisés (*Decentralized IDentifiers*, DID),
- des assertions vérifiables.

Schématiquement, les trois étapes fondamentales sont :

1. l'utilisateur acquiert ou crée une identité numérique unique, génère ses identifiants décentralisés et y relie ses documents ou attributs certifiés[49],
2. l'utilisateur fait usage de son **identifiant décentralisé** en ligne pour obtenir un bien ou avoir accès à un service. Il déclare être « celui qu'il est », et prouve qu'il possède les attributs nécessaires à l'accès au service à travers des assertions vérifiables portant sur des attributs de son identité et/ou des documents authentiques.
3. Le vérificateur contrôle les attestations et preuves fournies avant d'autoriser l'accès au service.

Par commodité, l'utilisateur préférera sans doute opérer depuis son téléphone mobile. Cela fait de ce dispositif un appareil particulièrement sensible en termes de sécurité matérielle et de protection des données personnelles et d'identité hébergées.

Pour les usages qui se cantonnent à la sphère du numérique, les utilisateurs peuvent employer une solution de *Self-Sovereign Identity* leur permettant de générer leurs propres identifiants décentralisés utilisables pour s'authentifier sur le système numérique, sans pour autant s'identifier. Il n'est pas systématiquement requis d'établir un lien entre l'élément personnel décentralisé utilisé pour avoir accès au service et l'identité juridique tant que l'usage demeure dans le monde virtuel et/ou que

[49] En fonction des applications, et des usages, ils peuvent être certifiés par une autorité, un tiers de confiance, un autre utilisateur ou « auto-certifiés ».

l'identité de l'utilisateur n'a pas besoin d'être contrôlée. C'est le cas par exemple de l'usage de crypto-monnaies telles que Bitcoin. Tant que l'utilisateur échange des bitcoins avec d'autres utilisateurs via la *blockchain* Bitcoin, en procédant à une forme de troc, il s'authentifie avec une adresse de compte de portefeuille qui joue le rôle d'un pseudonyme sur le réseau Bitcoin. En revanche, dès lors qu'il souhaite revenir dans le monde physique, par exemple en échangeant ses bitcoins en monnaies fiduciaires comme des euros, l'utilisateur doit s'identifier en ouvrant un compte en banque sur lequel il recevra des unités monétaires. C'est le principe du « *Know Your Customer* » (KYC).

Dans cette étude, les auteurs se sont intéressés aux usages impliquant l'identité réelle de l'utilisateur. Ici, par le terme « réel », il est entendu l'identité juridique, ou des attributs physique ou biométrique permettant d'identifier une personne de façon univoque. La certification de cette identité provient d'un tiers habilité, qui agit en tant qu'autorité, pour certifier ou attester de leur authenticité. On voit apparaître ici une double notion de « souveraineté » au sens anglais du terme :

- D'une part, la souveraineté / autonomie de l'utilisateur faisant usage de son identité sous une forme numérique ou numérisée pour bénéficier d'un droit,
- D'autre part, la souveraineté de l'autorité qui atteste de l'authenticité d'un titre d'identité, d'un attribut de l'identité, d'un document source ou encore d'une caractéristique biométrique.

Sur la base de ce paradigme, deux niveaux de vérification sont requis :

- Le premier vise à répondre aux questions : « Est-ce que ce document, cet attribut d'identité, est suffisant pour authentifier son détenteur et lui ouvrir l'accès à un droit ? Et par quel organisme habilité cet attribut est-il délivré ? »
- Le second vise à répondre aux questions : « L'émetteur de la requête est-il le détenteur légitime de cette identité ou de ce document ? »

L'utilisateur présentant une assertion vérifiable attestée par un certificateur d'attributs doit être en mesure de prouver son identité selon le niveau de sécurité requis pour le service demandé. Faute de quoi, il se verra refuser l'accès au service sollicité si le vérificateur estime que le niveau de confiance requis n'est pas atteint.

Tel est précisément l'objet du réglement eIDAS (Règlement (EU) n°910/2014)., Si une *blockchain*, conçue comme décrit ci-dessus, venait à être notifiée comme un service public de confiance, le vérificateur exerçant dans un autre Etat Membre devrait satisfaire aux conditions du règlement d'exécution n°2015/1502 du 8 septembre 2015 pour accéder au service de vérification offert par cette *blockchain*. En retour, une telle *blockchain* devrait faire l'objet d'un audit d'accréditation selon le règlement n°765/2008 du 9 juillet 2008.

La soumission au règlement eIDAS aurait pour vocation essentielle de faciliter la construction de *blockchains* vertueuses, susceptibles de jouer un rôle moteur dans l'économie européenne dont le développement nécessite des services d'identification numérique fiables.

5.2. Etat de l'art de solutions de *Self-Sovereign Identity*

Dans certains pays du monde, les naissances ne sont pas systématiquement enregistrées par l'état civil. La promesse d'une identité numérique pour chacun peut donner lieu à des initiatives vertueuses. Ainsi, le groupe de la Banque mondiale a-t-il créé l'initiative « Identification pour le développement » ID4D[50],

[50] https://id4d.worldbank.org

qui se compose d'unités travaillant sur le développement numérique, la protection sociale, la santé, l'inclusion financière, la gouvernance, le genre et les questions juridiques. L'initiative se concentre également sur l'intégration des systèmes d'identification numérique avec l'état civil (documenter les événements de la vie tels que la naissance, le mariage, l'adoption, le décès…).

Le consortium SIA (*Secure Identity Alliance*) a réalisé, à travers son projet de durabilité OSIA[51], un ensemble d'interfaces libres (API) en *Open Standard* pour l'interopérabilité des opérations sur les registres civils, d'identité et administratifs, offrant ainsi un moyen évolutif vers la *Self-Sovereign Identity*. La gestion et l'implémentation du *back-end* sont laissées à la discrétion des intégrateurs selon le modèle choisi par l'autorité publique en charge des registres.

L'Alliance ID2020[52] est un partenariat public-privé dédié à la résolution des défis liés à l'identité par le biais de la technologie. Cette alliance vise à financer des projets mettant en œuvre des solutions de certificats numériques sécurisés, à établir des normes pour faciliter l'interopérabilité et à permettre une collaboration multi-acteurs. Dans le cadre de l'Alliance, Microsoft a collaboré récemment avec Accenture et Avanade pour créer un prototype d'identité basé sur une *blockchain* sur Microsoft Azure[53]. Ce prototype a été conçu pour être interopérable avec les systèmes d'identité existants afin que les informations personnelles identifiables puissent résider hors *blockchain* (*off-chain*).

Pour rappel, Christopher Allen a introduit en 2016 (voir par exemple [22]), dix propriétés pour l'identité numérique décentralisée. Les auteurs de l'étude [30] les ont classées comme suit :

Tableau 1 : propriétés de l'identité numérique décentralisée

Sécurité	Contrôle	Cycle de vie
1) Protection des données à caractère personnel 2) Persistance de l'identité numérique 3) Minimalisation des données divulguées	4) Absence de collision d'identifiants, existence propre et indépendante 5) Contrôle par l'utilisateur 6) Consentement de l'utilisateur	7) Interopérabilité 8) Transparence et code ouvert 9) Accessibilité 10) Portabilité

Christopher Allen réserve l'appellation de *Self-Sovereign Identity* au choix d'implémentation couvrant plusieurs de ces propriétés et mettant en œuvre les trois rôles de fournisseur, utilisateur et vérificateur autour d'un système décentralisé.

L'intérêt de la combinaison des concepts d'identité décentralisée avec la *blockchain* est traité par la littérature scientifico-technique depuis environ 5 ans, voir notamment les publications [28] et [29]. Le document [40] décrit en détail la combinaison des concepts de *Self-Sovereign Identity* avec des technologies *blockchain* (ou DLT) et leur articulation aux architectures de gestion d'identité plus traditionnelles.

Cette combinaison s'appuie généralement sur plusieurs fournisseurs d'identité, et peut suivre partiellement ou complètement les spécifications et recommandations développées par des acteurs tels que W3C [24][25] ou DIF[54]. Elle peut être mise en œuvre autour de *smart contracts*, on parle alors d'application distribuée (*dApp)*. Une solution de *Self-Sovereign Identity* comprend aussi des « agents »,

[51] https://secureidentityalliance.org/osia
[52] https://id2020.org
[53] https://www.technologyrecord.com/Article/accenture-avanade-and-microsoft-create-blockchain-solution-for-id2020-59042
[54] https://identity.foundation/

comme l'application client fournie à l'utilisateur à partir de laquelle il accède et opère sur le système de *Self-Sovereign Identity*. Le vérificateur dispose également d'un agent lui permettant d'accéder à la *blockchain* et comportant les algorithmes de vérifications des preuves, attestations et/ou assertions. Chaque solution doit faire le choix d'un ou plusieurs fournisseurs d'identité numérique et éventuellement de certificateurs de documents ou d'attributs. Pour cela, un format de données est défini pour échanger l'information. La *blockchain* fait partie des acteurs de l'écosystème. Elle peut être choisie selon sa gouvernance ou son caractère *permissioned* versus *permissionless*, ainsi que publique versus privée.

Le concept de *Self-Sovereign Identity* est étudié de façon intensive depuis 2016 et donne lieu à de nombreux projets, preuves de concept et réalisations.

5.2.1 Approche fonctionnelle

Le rapport [23] du Forum économique mondial (*WEF - World Economic Forum*) présente le sujet de l'identité numérique en 6 couches fonctionnelles. Selon ce schéma, le WEF a rédigé un guide pour l'usage de l'identité numérique au service du développement durable lors du *Sustainable Development Impact Summit*[55] de 2018. Nous y avons ajouté une 7ème couche, celle de l'identité numérique décentralisée (cf. Figure 7), qui peut être organisée selon diverses modalités, et qui doit être durable, protégée contre le vol ou l'usurpation et pouvoir être retrouvée en cas de perte.

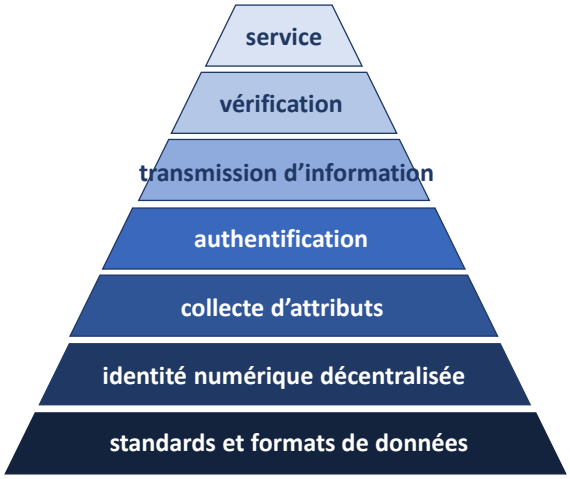


Figure 7 : couches fonctionnelles associées à l'usage d'une identité numérique décentralisée

1) Standards et formats de données : élaborer des normes pour régir le fonctionnement du système et permettre les interactions entre les acteurs de l'écosystème

2) Identité numérique décentralisée : générer et/ou fournir un identifiant numérique unique pour s'authentifier sur le système numérique

3) Collecte des attributs : recueillir des attestations des attributs d'identité ou de documents sources auprès d'organismes habilités

4) Authentification : utiliser l'identifiant numérique pour accéder à un service en ligne

[55] https://www.weforum.org/events/sustainable-development-impact-summit

5) Transmission d'information : donner accès aux données sources et/ou aux preuves et justificatifs requis pour bénéficier du service en ligne

6) Vérification : vérifier des preuves et justificatifs fournis pour être autorisé à bénéficier du service

7) Service : enregistrer la réalisation du service, de type « notarisation », dans la *blockchain,* assurant la traçabilité des transactions et permettant l'audit

5.2.2 Etat de l'art

L'approche formelle par couches fonctionnelles a donné lieu aux travaux suivants.

Standards et formats d'identité

L'une des missions des instances de normalisation consiste à spécifier des formats de données et des procédures permettant l'interopérabilité des fonctionnalités entre les acteurs de l'écosystème, et à favoriser la portabilité de l'identité d'une solution à une autre.

La *Decentralized Identity Foundation*[56] est une organisation qui travaille sur la création d'un écosystème d'identité décentralisée. La DIF produit des spécifications assurant l'interopérabilité entre les acteurs de l'écosystème, ainsi qu'avec les solutions de gestion d'identité et d'authentification déjà déployées, telles que OpenID Connect[57]. La DIF réunit un éventail diversifié de membres allant de l'Enterprise *Ethereum Alliance* et Hyperledger à IBM et Mastercard.

La mission du groupe de travail DID (*Decentralized Identifier*)[58] du W3C consiste à introduire des spécifications communes pour contribuer à l'utilisation d'identités numériques décentralisées pour les applications *web*. Ce groupe élabore en particulier les spécifications *Decentralized Identifiers* (DIDs) [24], se fondant notamment sur les documents de la DIF qui sont utilisées par de nombreuses solutions de *Self Sovereign Identity*[59]. Ces travaux sont aussi en lien avec les travaux sur les assertions vérifiables du W3C[60] (*Verifiable Credentials*) lesquelles sont parfaitement compatibles avec un schéma de DID. Si, par exemple, l'utilisateur délivre ses assertions sous forme de *Verifiable Credentials* alors le vérificateur devra connaitre le DID de l'utilisateur pour vérifier leur intégrité et leur authenticité. Les *Verifiable Credentials* sont rassemblés dans une *Verifiable Presentation* signée par l'utilisateur et comportant les termes d'usages. Ces termes, limitant l'usage des assertions pour servir et valoir ce que de droit, figurent dans les *Verifiable Presentations* dans l'objet dit "*Terms of Use*"[25]. Associés avec les techniques cryptographiques dites « *Zero-Knowledge Proof* », il est possible pour l'utilisateur de prouver qu'il détient légitimement certains documents certifiés par un organisme habilité, ou encore qu'il est le légitime détenteur de données ou d'attributs d'identité, sans en révéler le contenu afin d'en préserver la confidentialité.

Plusieurs comités de normalisation dépendant de l'ISO (*International Organization for Standardization*) travaillent aussi sur l'application de ces techniques ou de principes similaires, par exemple :

- ISO/IEC JTC 1/SC 17 *Cards and security devices for personal identification* développe une norme ISO/IEC 18013-5 *Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application,* et une série de spécifications ISO/IEC AWI 23220 *Card and security*

[56] https://identity.foundation/
[57] https://identity.foundation/did-siop/
[58] https://www.w3.org/2019/did-wg/
[59] https://w3c-ccg.github.io/did-method-registry/
[60] https://www.w3.org/2017/vc/WG/

devices for personal identification - Building blocks for identity management on mobile devices, reprenant des concepts proches des *verifiable credentials*.

- ISO/TC 307 *Blockchain and distributed ledger technologies* dispose de groupes de travail dont le périmètre inclut la gestion d'identité et la *Self Sovereign Identity*. Un document « *Overview of existing DLT systems for identity management* » est notamment en cours de développement.
- ISO/IEC JTC 1/SC 27 *Information security, cybersecurity and privacy protection*, qui est un des acteurs principaux pour le développement de normes sur la gestion d'identité et de cadre d'authentification de confiance (*e.g.* ISO/IEC 29115), développe la norme ISO/IEC 27551 *Information technology — Requirements for attribute-based unlinkable entity authentication* couvrant plusieurs principes avancés tels que les *attribute-based credentials* qui sont des *verifiable credentials* construits à l'aide de techniques ZKP.

D'autres organismes importants sont actifs sur le sujet. On notera le comité technique récemment créé JTC19 « *Blockchain and Distributed Ledger Technologies* »[61] du CEN/CENELEC (organismes de normalisation européen) travaillant sur des aspects spécifiques au marché européen comparé à l'ISO/TC 307 ; l'OACI (à travers son groupe TRIP NTWG[62]) s'intéressant aux documents d'identité dématérialisés ; et les groupes IEEE P2418.

Identité numérique décentralisée

L'acquisition d'une identité numérique décentralisée doit garantir à chaque individu l'unicité de son identifiant. Pour acquérir cet identifiant, deux techniques se distinguent :

- Soit l'utilisateur déclare son identité numérique de son propre chef (système « auto déclaratif »). Dans ce cas, il génère lui-même son identifiant à partir d'un générateur de nombres aléatoires assurant que l'identifiant en sortie comporte une très forte entropie et un taux de collision nul à l'échelle temporelle de plusieurs générations.
- Soit un fournisseur d'identité fournit à l'utilisateur un identifiant unique, l'unicité étant garantie par l'usage d'un serveur central[63].

La *blockchain* introduit une solution médiane entre ces deux extrêmes en jouant le rôle d'intermédiaire pour l'enregistrement des identités numériques décentralisées, et remplaçant ainsi le serveur d'enregistrement utilisé dans les systèmes centralisés.

Pour permettre l'identification par le vérificateur, il est requis d'effectuer une phase d'enrôlement, visant à relier l'identifiant décentralisé (numérique) avec l'identité juridique de la personne.

Par exemple, Sovrin [31], ou Hyperledger Indy, permet à un utilisateur de générer autant d'identifiants anonymisés qu'il le souhaite. Les identifiants ne sont pas liés entre eux, et sont gérés par l'utilisateur qui en est le seul détenteur, ou bien par une forme de gouvernance[64]. Quant à uPort [32], il fournit une solution permettant à chacun de générer une identité décentralisée et de faire usage de cet identifiant décentralisé pour accéder à des services via des *smart contracts*. Un *smart contract* « contrôleur » relié au compte d'émission du détenteur sert de point d'entrée. Accessible depuis un téléphone mobile, Sora [33] fournit une solution japonaise de *Self-Sovereign Identity* permettant à l'utilisateur de générer

[61] https://www.cencenelec.eu/news/brief_news/Pages/TN-2019-049.aspx
[62] https://www.icao.int/Security/FAL/TRIP/Pages/rfi.aspx
[63] L'utilisateur est en mesure de faire usage de son identifiant de façon décentralisée, y compris si l'identifiant a été généré de façon centralisée (cf. Alicem).
[64] Un fournisseur d'identité peut être considéré comme une gouvernance, comme par exemple l'ANTS dans le cas d'Alicem.

autant d'identifiants qu'il le souhaite afin d'éviter d'être tracé en ligne. Les données personnelles hébergées sur le dispositif mobile sont chiffrées. La *blockchain* sert à enregistrer les transactions. Cependant, toutes ces solutions ne permettent pas d'effectuer l'identification de l'utilisateur lors de la phase de vérification.

D'autres solutions, comme par exemple ShoCard [35], fournissent une identité de confiance permettant l'identification, en tirant parti de la *blockchain* pour lier à un identifiant d'utilisateur un *credential* de confiance existant comme un passeport, un permis de conduire ou une carte d'identité, ou encore d'autres attributs d'identité. Dans le cas de ShoCard, ce lien est réalisé via un haché cryptographique enregistré dans la *blockchain* : la *blockchain* est alors utilisée comme un service d'horodatage pour signer les empreintes cryptographiques des informations d'identité d'un utilisateur, et un serveur centralisé sert d'intermédiaire lors de l'échange d'information d'identité chiffrée entre un utilisateur émetteur et un destinataire ; le schéma repose sur trois phases : l'initialisation, la certification et la validation.

Dans un schéma décentralisé, en l'absence de serveur central, la sauvegarde de l'identifiant décentralisé de l'utilisateur pour pouvoir le récupérer en cas de perte, constitue un véritable défi. Différents mécanismes existent, comme l'usage d'un moyen mnémotechnique (matérialisé par une série de mots) dans la communauté *blockchain*, ou encore le partage de secrets consistant à distribuer à plusieurs amis (indépendants) des morceaux du secret sur lequel l'identifiant est basé. Plusieurs pièces du secret sont nécessaires pour récupérer l'identifiant en cas de perte. Plusieurs acteurs, en particulier uPort, utilisent un *smart contract,* servant de *proxy*[65] à l'identité, lié à un service de récupération (*recovery)* de l'identifiant décentralisé, qui permet de déléguer la gestion à un tiers.

Collection d'attributs

La collecte d'attributs d'identité implique différents tiers ou organismes habilités à délivrer des documents ou des attributs d'identité et de les certifier ; en particulier dans le cadre de l'identité décentralisée, il faut pouvoir solliciter les différents services susceptibles de certifier les attributs. L'article [29] présente une façon de procéder à partir de la *blockchain*. L'attestation est transmise à l'intéressé sous forme numérique, signée par l'autorité qualifiée. Celle-ci peut également transmettre à l'intéressé une attestation qui lui permettra de prouver l'authenticité dudit document en vue de sa vérification.

Dans le monde physique, le Cachet Electronique Visible (CEV)[66] joue ce rôle de certificateur du document sur lequel il est apposé ; c'est une signature numérique. C'est le cas notamment de la vignette « Crit'Air ». Un CEV est apposé sur chaque pastille certifiant son contenu : l'immatriculation du véhicule et la cotation comprise entre 0 et 5. L'autorité, organisme habilité à délivrer les vignettes, signe chaque CEV avec la même clé privée. Il suffit ainsi de disposer de la clé publique associée pour vérifier l'authenticité de chaque pastille, en vérifiant la signature numérique inscrite sur le CEV. Le CEV est la transposition sur un support physique d'une attestation numérique.

Le formatage des attributs selon un modèle spécifique est essentiel pour garantir l'interopérabilité entre les différents acteurs et les différents rôles.

La collecte des attributs d'identité soulève la question du stockage de ces données à caractère personnel qui doivent être protégées conformément à la règlementation RGPD. Pour des raisons de

[65] Serveur jouant le rôle d'intermédiaire.
[66] https://aigcev.org/

confidentialité, les données ne sont généralement pas stockées « en clair » sur le *ledger* (« ***on-chain*** »). Si, pour les besoins d'un cas d'usage, des données doivent être enregistrées directement sur la *blockchain*, il est indispensable de les chiffrer avec un algorithme de chiffrement offrant une sécurité de niveau élevé, ou d'utiliser un mécanisme cryptographique. De tels mécanismes impliquent de gérer des clés secrètes pour permettre au destinataire de déchiffrer ou d'en vérifier le contenu. Elles sont de préférence stockées hors *blockchain* (« ***off-chain*** »), soit localement sur le dispositif de l'utilisateur dans une zone sécurisée, soit dans un espace personnel situé dans un *cloud*, sous le contrôle de l'utilisateur. Dans ce dernier cas, l'adresse web (URL) indiquant l'endroit où sont stockées les données, des valeurs de contrôle d'intégrité ainsi que la gestion des droits d'accès et des autorisations peut être enregistrée dans le *ledger* (« *on-chain* ») ou via un *smart contract*.

On distingue ici deux types de données :

1) Les données brutes, à caractère personnel, conservées dans un espace de stockage sécurisé et sous contrôle de l'utilisateur, telles que les attributs d'identité donnant lieu à une divulgation sélective comme l'âge ou la couleur des yeux, les assertions vérifiables comme la déclaration « je suis majeur(e) », les documents authentiques comme un permis de conduire.

2) Les éléments cryptographiques faisant référence aux données brutes, tels que les attestations, les preuves d'authenticité, les preuves à connaissance nulle de divulgation (ZKP).

Cette distinction donne lieu à deux formats différents de registres spécifiés par le consortium W3C.

D'une part, le registre des identifiants (« *Identifier Registry Model » [24]*) décentralisés, dans lequel les éléments d'identification numériques et les données personnelles sont stockés sur le dispositif sécurisé sous contrôle de l'utilisateur (par exemple son téléphone mobile), qui sont donc non seulement hors *blockchain* (« *off-chain* ») pour des raisons de confidentialité, mais également hors *cloud* pour que l'utilisateur conserve le contrôle de son identité. Il apparaît dans ce modèle que la *blockchain* pourrait agir comme une sorte de DNS (*Domain Name System*). Concrètement, on peut lier logiquement une identité juridique vérifiée par un schéma eIDAS notifié à partir d'un identifiant décentralisé (ou DID).

D'autre part le registre d'assertions (« *Claim Registry Model »* [25]) décentralisées qui sert à conserver les empreintes numériques cryptographiques de toutes les assertions d'identité émises.

Par exemple, uPort utilise ces deux types de registres, basés respectivement sur l'emploi de deux *smart contracts,* l'un pour enregistrer les identifiants décentralisés (DID) dans le *ledger*, et l'autre de type ERC780[67], standardisé par la communauté Ethereum, pour stocker/enregistrer des assertions (« *claim* ») dans le *ledger* (« *on chain* »). Le *ledger* peut alors référencer des données ou attributs stockés à l'extérieur de la *blockchain*.

Ce choix d'implémentation basé sur les modèles de registres d'identifiants et d'assertions conserve la topologie distribuée en ce qui concerne le stockage des données.

En revanche, dans le projet Blockstack [34], les données brutes à caractère personnel sont centralisées dans le *cloud* et hébergées chez des fournisseurs classiques du *cloud*. Seul le lien référençant leur emplacement est enregistré sur la *blockchain*.

Centrée sur l'utilisateur et opérant sur sa propre infrastructure, la solution EverID (ou Evrest) [38] héberge l'identité numérique des utilisateurs dans le *cloud*. Ceux-ci peuvent effectuer des transactions

[67] https://github.com/ethereum/EIPs/issues/780

depuis n'importe quel dispositif connecté. Leur données d'identité pivot et biométrique sont sur un serveur EverID, éventuellement sécurisé conformément à la RGPD, mais à la merci d'une attaque cyber.

Authentification

L'authentification repose sur l'usage de l'identifiant décentralisé pour accéder à un service en ligne. L'authentification relie l'utilisateur ou son dispositif à son activité numérique. Non répudiable, elle doit fournir un niveau de sécurité plus ou moins élevé.

La Figure 3 et la Figure 4 présentent des mécanismes basés sur la signature numérique qui peuvent être utilisés pour l'authentification. La signature numérique repose sur la cryptographie asymétrique utilisant une paire de clés, la clé privée doit être conservée secrète par son possesseur car elle sert à construire la signature numérique d'une donnée ou d'un document, tandis que la clé publique est communiquée au destinataire et sert à authentifier l'émetteur et à vérifier l'intégrité des données transmises. La signature numérique permet à l'utilisateur de prouver qu'il est en possession de la clé privée. Lorsqu'on peut vérifier les données pointées par le DID à partir de la clé publique, cela prouve que la signature a bien été calculée à partir de la clé privée correspondante. Ce mécanisme, propre aux *blockchains*, authentifie le compte émetteur au sein d'une transaction, qui, une fois enregistrée dans le *ledger*, devient non-répudiable.

Mise en œuvre depuis un dispositif mobile, une authentification forte ou une authentification multi-facteurs renforce la sécurité, *a contrario* d'une authentification uniquement par login/mot de passe. L'alliance FIDO propose pour cela diverses techniques comme le protocole UAF (« *Universal Authentication Framework* ») compatible avec les dispositifs mobiles (et permettant de combiner l'authentification à distance à une authentification locale avec PIN ou avec biométrie). Il en est de même pour le protocole U2F[68] (« *Universal Second Factor* ») qui intègre notamment la possibilité d'utiliser un composant de sécurité. Les portefeuilles de comptes « Nano Ledger » commercialisés par la société Ledger[69] sont compatibles avec ce mécanisme. Plusieurs autres techniques d'authentification forte utilisent des moyens biométriques tels que la lecture d'empreintes digitales, la reconnaissance faciale ou vocale.

Le projet Digi-ID [36] s'intéresse au processus de KYC (*Know Your Customer*) et à l'authentification unique basée sur la capture de l'empreinte digitale. Associé à un moyen de paiement, il permet une identification rapide de l'utilisateur. Egalement positionné sur la garantie du KYC, IDchainZ[70] introduit une preuve de concept quant à la certification de documents source basée sur les travaux de Morris [37].

En dehors de tout cadre régulateur, LifeID [39] propose une solution de *Self-Sovereign Identity* basée sur la biométrie depuis un téléphone mobile. Chacun peut générer une identité numérique auto-proclamée, liée avec ses données biométriques. La sécurité de cette solution repose sur l'éventuelle difficulté à reproduire les données biométriques d'un autre, et sur la qualité de l'implémentation des algorithmes de reconnaissance.

Les organismes habilités à délivrer des documents authentiques et/ou à délivrer des attestations doivent fournir aux vérificateurs les éléments (cryptographiques) prouvant leur légitimité. Ce processus, appelé « *root-of-trust* » en sécurité, doit être traité dans le contexte d'une solution impliquant une *blockchain*.

[68] https://fidoalliance.org/specifications/
[69] Société française
[70] https://www.chainzy.com/products/

Transmission d'information

La transmission des données doit garantir de bout-en-bout la sécurité et la confidentialité des données. Celles-ci ne doivent pas pouvoir être interceptées, ni déchiffrées par un tiers. De plus, les protocoles mis en œuvre doivent protéger l'identité des utilisateurs et leur laisser le contrôle sur leurs données. Cela soulève la question du choix et de la minimalisation des données à transmettre, des attestations et/ou des preuves à produire pour être autorisé à bénéficier du service souhaité, ainsi que les mécanismes de préservation d'anonymat. Ces problématiques sont fortement liées au concept de *Self Sovereign Identity*, ainsi qu'à l'utilisation d'assertions vérifiables protégées par des mécanismes de divulgation sélective, ZKP ou d'autres techniques cryptographiques.

De nombreux choix d'implémentations sont envisageables, en particulier le choix des éléments à enregistrer sur le *ledger* (« *on-chain* ») et des données à transférer hors *blockchain* (« *off-chain* »). Un format de données doit aussi être choisi en concertation avec les acteurs de l'écosystème pour assurer l'interopérabilité. Comme écrit dans les précédentes sections, c'est l'un des enjeux des groupes de spécification ou normalisation.

Le sujet de la transmission sécurisée d'attributs est déjà traité dans les protocoles modernes de gestion d'identité et d'authentification ou autorisation, tels que OpenID Connect, SAML et OAuth 2.0.

Vérification

L'étape de vérification consiste à valider les preuves et attestations fournies avant d'autoriser l'utilisateur à bénéficier du service demandé. On distingue trois types de vérification distincts :

- Celle qui porte sur l'authenticité des attributs d'identité et/ou des documents,
- Celle qui porte sur l'authentification de l'émetteur,
- Celle qui porte sur l'identification.

Authenticité des attributs d'identité et/ou des documents

Cette étape consiste pour le vérificateur à s'assurer de l'authenticité des attributs d'identité et des documents présentés. Ce contrôle est rendu possible par la vérification des preuves et des attestations fournies, délivrées par des entités habilitées (ou « de confiance » du point de vue du vérificateur).

La notion d'accréditation suppose la présence d'un cadre régulateur. La certification d'un document ou d'une donnée s'appuie sur une *root-of-trust*, visant à délivrer une attestation à l'utilisateur. Libre ensuite à celui-ci d'en faire usage « pour faire valoir ce que de droit ». Le vérificateur doit être en mesure de disposer des éléments cryptographiques, clés publiques et certificats, susceptibles d'établir l'authenticité des données certifiées.

Authentification de l'émetteur

Authentifier l'émetteur d'une transaction ou d'un message est la base de toute solution de *Self Sovereign Identity*. La distinction entre les différentes solutions réside dans l'implémentation de la fonction qui doit garantir la sécurité de bout-en-bout. Par ailleurs, dans un système complexe mêlant des messages (données) envoyés hors *blockchain* (« *off-chain* ») et des transactions (justificatifs) inscrites dans le *ledger* (« *on-chain* »), envoyés via des canaux de communication différents, il est

nécessaire que l'utilisateur soit authentifié de la même façon (ou via des méthodes proches) lors de la présentation de données et lors de la présentation de l'attestation correspondante.

On garantit la cohérence de l'authentification en employant la même clé privée pour signer le message incluant les données chiffrées et pour signer la transaction prouvant leur intégrité.

Identification

L'identification concerne une personne physique ou morale, à l'origine des données authentifiées transmises à un tiers. L'identification vise à répondre à la question : « Est-ce que la personne authentifiée, qui fait emploi de cet identifiant numérique, est bien la personne qu'elle prétend être ? ».

L'identification peut relever de différents niveaux de sécurité, le niveau le plus élevé, selon la règlementation eIDAS, consistant à apporter la preuve de son identité juridique.

Un utilisateur souhaitant accéder à un service qui requiert un niveau d'identification élevé, devra employer une solution d'identité numérique, ou passer par un fournisseur d'identité offrant le niveau élevé, et fournir les preuves de son identité juridique.

La vérification peut être effectuée à distance (en ligne) ou bien en face-à-face selon les usages. Pour un même niveau de sécurité, les données qui sont présentées en face-à-face, et qui restent sous le contrôle de l'utilisateur, peuvent être transmises pour une vérification à distance. Dans ce dernier cas, même si l'utilisateur consent à la transmission de ses données, il doit être en mesure de s'assurer de l'identité du vérificateur. Dans un contexte de souveraineté, il est souhaitable que l'Etat joue le rôle de tiers de confiance pour certifier l'identité juridique de ses ressortissants et résidants vis-à-vis d'un prestataire de service privé, dans le but de minimiser les données d'identité transmises.

La solution ShoCard [35] introduit une technique permettant à un utilisateur de prouver, via la *blockchain,* qu'il détient le titre d'identité associée à son identité numérique. Cependant, en l'absence d'attestation et/ou de preuve du vivant, un faux titre d'identité ou un document volé peuvent être utilisés. L'application sur téléphone mobile Alicem, introduite par la France, offre une solution d'identité numérique de niveau élevé conformément à la règlementation eIDAS, incluant à la fois la certification des données d'identité et l'usage d'une preuve du vivant (biométrie).

Service

Une fois l'identité de l'utilisateur vérifiée avec le niveau de sécurité requis, selon le service demandé, l'utilisateur est autorisé à accéder au service. Celui-ci peut donner lieu à un échange de données qui peut être notarisé dans le *ledger*. La notarisation consiste à enregistrer via une transaction l'exécution du service. La propriété de transparence de la *blockchain* permet à chaque partie de voir cette information qui devient alors opposable et traçable, et facilite le travail d'audit.

5.2.3. Architecture de solutions de *Self-Sovereign Identity*

Pour chacune des couches fonctionnelles de la Figure 7, plusieurs choix d'implémentation sont envisageables. Ces choix dépendent de l'architecture globale du système, et des compromis effectués entre l'usage de serveurs centralisés et la mise en œuvre de solutions distribuées. Les choix d'architecture soulèvent la question de l'hébergement et du transfert des données à caractère personnel, mais aussi la question de la protection des secrets, de la gestion des clés cryptographiques, de la génération et de l'échange des preuves, de l'accessibilité et de la transparence.

Par exemple, ShoCard met en œuvre une architecture permettant l'identification aussi bien en face-à-face qu'à distance, en faisant du titre d'identité physique la racine de l'identité. Une autre solution consiste à utiliser le coffre-fort numérique, qui centralise l'information sur un serveur géré par un tiers de confiance. C'est le choix d'implémentation de Sovrin : l'utilisateur n'a pas complètement le contrôle de son identité et de ses données personnelles qui sont hébergées dans un coffre-fort situé sur un dispositif intermédiaire détenu et géré par un tiers. En pratique, cela revient à confier ses données à un acteur privé sur un serveur *cloud* centralisé. En hébergeant les données sur le dispositif de l'utilisateur, Shocard et uPort proposent à l'utilisateur de garder le contrôle via une application sur téléphone mobile qui embarque le DID et les données à caractère personnel.

Pour le contrôle de l'authenticité des données à caractère personnel, ShoCard repose sur un serveur centralisé, tandis que uPort utilise un registre distribué (« *claim registry model* ») implémenté via un *smart contract* ERC780 sur Ethereum. Le choix d'une implémentation distribuée fournit la transparence aux acteurs de l'écosystème, et *in fine* crée de la confiance, chacun étant en mesure de contrôler la légitimité des organismes habilités. La corruption est plus difficilement envisageable et plus facilement décelable sur ce type de système.

Le document [42] compare l'architecture des trois solutions de *Self Sovereign Identity* citées précédemment : uPort, Sovrin et ShoCard. Il met en évidence qu'aucune des implémentations ne satisfait l'ensemble des « lois de l'identité » introduites en 2005 par Kim Cameron [43]. Celui-ci, constatant que sur internet il n'y a pas d'approche cohérente et compréhensible permettant aux utilisateurs d'évaluer la sécurité offerte par les sites qu'ils visitent, et qu'ils ne disposent pas de moyens fiables de savoir s'ils ne communiquent pas leurs données à caractère personnel à des destinataires frauduleux, a publié dans le document [43] ses idées sur la façon dont une couche d'identité pour l'Internet pourrait être ajoutée. Actuellement, ces couches sont au nombre de sept et nous en donnons ci-dessous notre interprétation :

1) ***Privacy* de bout-en-bout** : l'identité numérique, les attributs d'identité et les données personnelles restent sous le contrôle de l'utilisateur. Elles peuvent par exemple être hébergées sur son dispositif personnel (téléphone mobile), d'où sont émis les messages et les transactions signés à destination du vérificateur. Les éléments intermédiaires (passerelles, routeurs, serveurs…) ne doivent pas être en mesure de déchiffrer les données à caractère personnel, ni d'identifier l'émetteur.

2) **Minimisation des données** : le prestataire de service ne doit connaitre que le strict minimum des données à caractère personnel ou des attributs d'identité de l'émetteur, nécessaires à la fourniture du service. L'identification, l'authentification de l'émetteur, ainsi que la vérification de l'authenticité des données fournies doivent être déléguées à un tiers de confiance.

3) **Légitimité** : chaque acteur doit être en mesure de décliner son identité physique ou morale, son rôle dans l'écosystème et sa légitimité à accéder au service demandé.

4) **Identifiant public versus privé :** les identifiants décentralisés (DID) des acteurs publics (prestataire de service, tiers de confiance, autorités) doivent être invariants, connus, accessibles à tous et doivent permettre de les identifier. En revanche, les identifiants (DID) des utilisateurs sont privés et ne doivent pas permettre de les identifier en ligne.

5) **Pluralisme des acteurs :** le système doit être ouvert à de nouveaux acteurs, reposer sur des normes et des spécifications connues, et/ou des protocoles de communication et des technologies ouvertes.

6) **Génération de multiples identifiants décentralisés indépendants** : chaque utilisateur doit être en mesure de générer autant d'identifiants décentralisés qu'il le souhaite, indépendants les uns des autres, pour éviter qu'un auditeur externe ne puisse tracer son activité.

7) ***Privacy* en ligne et Audit** : les acteurs et utilisateurs de l'écosystème ne doivent pas être en mesure de tracer l'activité d'un utilisateur. En cas de nécessité, un tiers de confiance indépendant (type huissier de justice) mandaté, appelé auditeur, doit pouvoir identifier et auditer les utilisateurs et les acteurs impliqués à partir des informations publiques enregistrées sur le système numérique.

Pour respecter l'ensemble de ces objectifs, il est nécessaire que les fonctions de génération de l'identité numérique, de certification des attributs d'identité et/ou documents authentiques, de vérification et d'audit soient effectuées par des acteurs strictement indépendants. Cela implique que les rôles de :

- fournisseurs d'identité numérique,
- organismes habilités à délivrer des attestations,
- vérificateurs ou contrôleurs,
- auditeurs

soient indépendants les uns des autres, mais également que chacun des acteurs qui assument le même rôle soit indépendant de ses confrères.

La Figure 8 met en évidence les liens logiques qui apparaissent dans une architecture qui respecte la distinction des rôles et l'indépendance des acteurs.

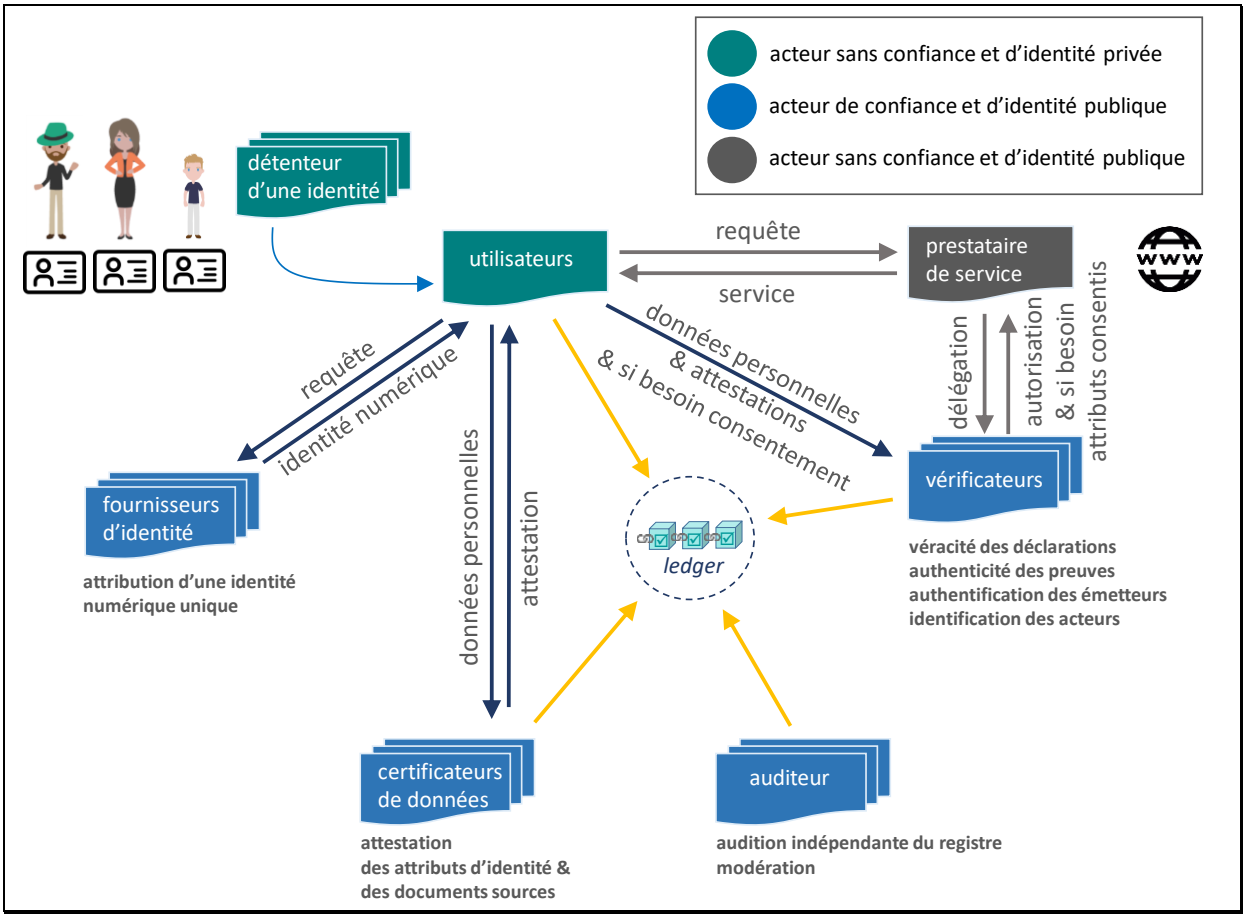


Figure 8 : organisation schématique d'un système de SSI

Ici, l'utilisateur d'une identité numérique n'est pas nécessairement à la fois propriétaire et détenteur des données associées, puisque des mécanismes de délégation peuvent être mis en œuvre, sur des supports amovibles (téléphone, carte sans contact…) ou dans des services distants (serveur dédié, *smart contract* autonome distribuant les données seulement si certains critères sont satisfaits…).

Plusieurs initiatives, comme [44] [45], sont en cours pour identifier les briques de base nécessaires à la réalisation de cette architecture dans un contexte européen en prenant en compte les contraintes RGPD et eIDAS.

5.2.4 La *Self-Sovereign Identity* opérée avec une *blockchain*

Un schéma de *Self-Sovereign Identity* n'est pas nécessairement implémenté par une *blockchain*. Toutefois, l'étude réalisée par les auteurs de [21] fait apparaitre qu'environ 90% des solutions de *Self-Sovereign Identity* actuellement existantes sont implémentées sur *blockchain*. Les avantages induits par son usage dans la mise en œuvre d'architectures de tels systèmes complexes sont nombreux.

En assurant l'immuabilité et la traçabilité des données qu'elle préserve, la *blockchain* devient la garante de leur intégrité, horodatage et authenticité, rendant ainsi l'écosystème moins dépendant des fournisseurs de dispositifs et des applications. La *blockchain* se prête bien à la conservation des attestations, des preuves sur des assertions certifiées, ainsi qu'à la gestion des certificats numériques émanant d'acteurs d'identité publique (acteurs étatiques souverains), ou encore à la traçabilité des services rendus. Elle fournit au vérificateur, de façon décentralisée, une preuve permettant de vérifier la validité, l'authenticité et l'intégrité des données. Le prestataire de service peut se passer de l'intermédiaire de vérification et peut endosser directement ce rôle en accédant à la *blockchain*. Tout certificateur d'attributs ou de documents authentiques, a la possibilité d'enregistrer les preuves et attestations sur la *blockchain*, ce fournisseur d'attributs pouvant indifféremment être une université, une école, une banque, une administration ou un service public, une association, ou tout autre entité connaissant l'utilisateur et se portant garant de ses attributs identitaires ou de l'authenticité de ses documents.

Le directoire de gouvernance de la *blockchain* fait autorité pour délivrer une autorisation à tout certificateur de documents authentiques et/ou d'attributs désirant faire partie de l'écosystème d'acteurs.

La *blockchain* rend visible aux yeux de tous la probité et la transparence du processus de vérification.

Les données ne sont dévoilées qu'avec le consentement de l'utilisateur, la *blockchain* contenant les moyens cryptographiques de fournir une preuve de l'intégrité, l'horodatage, l'authenticité et l'authentification de ces données. Les fournisseurs de services ont la possibilité d'articuler autour de la *blockchain* leurs fonctions respectives, tout en permettant à l'utilisateur de réaliser sa transaction avec le prestataire de services depuis le dispositif de son choix. Les tâches peuvent être automatisées par le biais du *smart contract* qui n'est pas un contrat au sens juridique du terme.

Il est possible d'utiliser son dispositif personnel comme un simple intermédiaire de collecte d'éléments d'informations recueillis depuis un composant sécurisé externe (carte plastique, CNIe, ou autre), et mettant en œuvre des techniques de KYC (*Know Your Customer*). Le contrôle de l'utilisateur sur ses données personnelles à consentir à la délivrance de tout ou partie des attributs ou assertions vérifiables requis pour accéder au service sollicité.

5.3. Mise en œuvre avec des dispositifs mobiles

Dans la perspective du développement de services accessibles depuis des dispositifs personnels connectés (ex. smartphone, tablette, objet connecté, voire véhicule), une solution d'identité numérique centrée sur l'utilisateur se positionne en considérant les besoins suivants :

- les données personnelles des utilisateurs doivent être organisées sur leur dispositif de sorte à en limiter l'exposition à des usages malveillants,
- les dispositifs mobiles n'endossent pas de responsabilité sur ces données. En théorie, la responsabilité de la vérification des données délivrées par un dispositif mobile devrait être imputée au fournisseur du système d'exploitation embarqué sur le dispositif, ou encore au fabricant du dispositif ou du composant sécuritaire embarqué, ainsi qu'à l'émetteur ayant provisionné les données personnelles sur le dispositif. La responsabilité des données communiquées n'est pas une question simple, d'autant que l'utilisateur peut aussi endosser une part de cette responsabilité s'il expose ses données sans précaution. Le consentement de l'utilisateur peut parfois conduire à des expositions à son détriment et, parfois, à son insu.
- Selon la nature du composant sécuritaire embarqué sur le dispositif (eSE, SoC SPU, TEE, WBC), les niveaux de certifications et de confiance peuvent varier.
- Les liens logiques associant l'utilisateur aux données qu'il détient peuvent être de natures diverses (ex. physique, biométrique, par connaissance d'un mot de passe, par propriété d'un titre, d'une attestation). L'absence de lien fort entre les données et l'utilisateur produit une autre forme de risque comme l'attaque par substitution du lien entre données et utilisateurs.
- Il est essentiel de fournir à l'utilisateur une interface conviviale et facile à utiliser.
- La présence de données sur un dispositif personnel doit impérativement prendre en compte la protection des données en cas de perte, de vol ou de destruction du dispositif.

Face à ces besoins, il apparait que le niveau de confiance va dépendre globalement d'au moins trois aspects concomitants :

1) la nature du composant matériel sécurisant le dispositif,
2) la confiance dans le ou les rôles qui portent la responsabilité des données,
3) le lien entre les données et l'utilisateur.

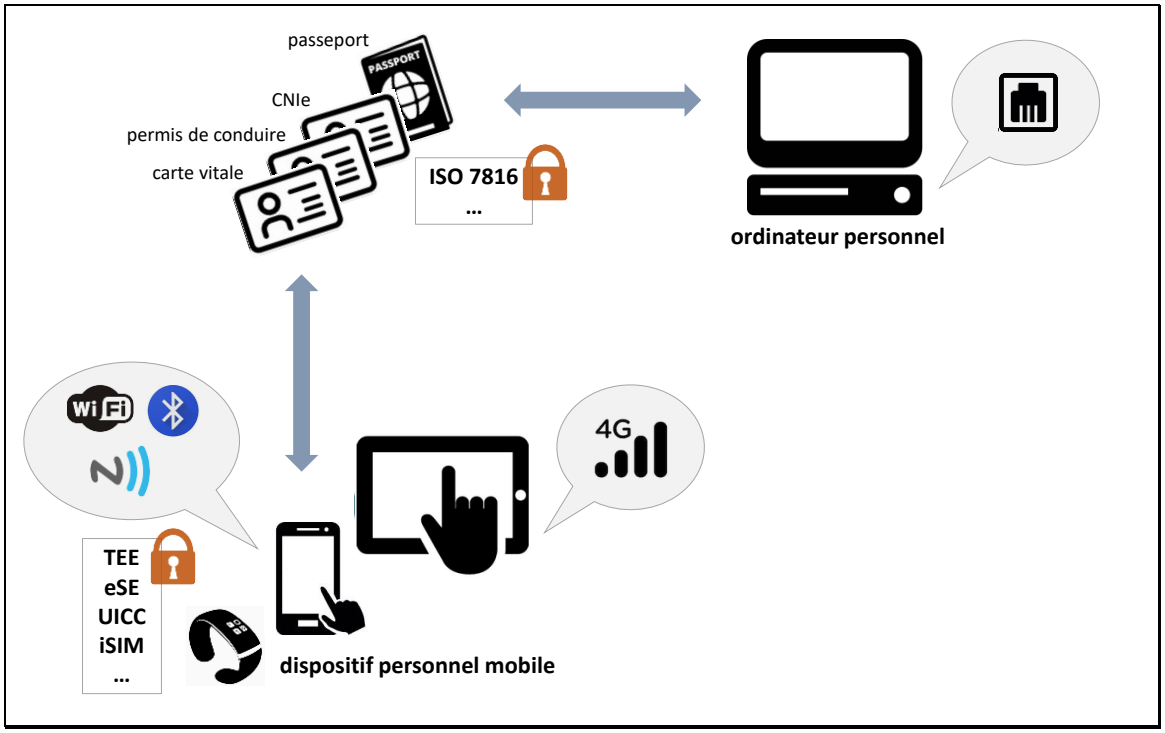


Figure 9 : dispositifs personnels d'accès aux services d'identification

La première solution d'identité numérique française compatible avec eIDAS, Alicem (Authentification en LIgne CErtifiée sur Mobile), est actuellement en cours de qualification par l'ANSSI. Dans la suite d'Alicem, la Carte Nationale d'Identité électronique (CNIe) sera bientôt déployée en France. Alicem est une application pour téléphone mobile aspirant à un niveau de sécurité élevé. Une phase d'enrôlement, basée sur un processus d'authentification faciale, vise à créer une identité vérifiée et à générer un identifiant anonymisé dont l'utilisateur fait usage pour accéder à des services en ligne. Ces éléments d'identité sont hébergés dans le téléphone mobile de l'utilisateur. L'Agence Nationale des Titres Sécurisés (ANTS) agit en tant que tiers de confiance vérificateur.

La connexion à Alicem s'effectue via FranceConnect (agrégation de fournisseur d'identité). Si un service demande un niveau substantiel d'identification, seules les solutions d'identité garantissant un niveau substantiel peuvent être employées.

Dans le cadre de l'application du règlement européen qui oblige tous les états membres à déployer une carte nationale d'identité sécurisée conforme au standard ICAO, le projet de Carte Nationale d'Identité électronique (CNIe) prévoit de proposer, comme moyen d'authentification de l'utilisateur, un processus alternatif à la reconnaissance faciale.

Au travers de FranceConnect, les six attributs d'identité constituant l'identité « pivot » FranceConnect (nom, prénom, date de naissance, sexe, lieu de naissance, pays de naissance) sont transmis au prestataire de service avec le consentement de l'utilisateur. Celui-ci n'a pas la possibilité de rester anonyme vis-à-vis du prestataire de service, ni de sélectionner de façon sélective les attributs de son identité qu'il souhaite/doit dévoiler. L'introduction d'une *blockchain* dans le système, par exemple selon l'architecture présentée en Figure 8, permettrait de remédier à cet inconvénient en apportant davantage de flexibilité à l'utilisateur et en améliorant la protection de ses données d'identité.

La Figure 9 illustre les liens entre le dispositif personnel (mobile, tablette, PC…) utilisé par l'utilisateur et les services chargés de son identification. Par l'intermédiaire d'une *blockchain*, l'utilisateur présente

des assertions vérifiables signées par l'organisme certifiant ces attributs d'identité, et signées par une fonction de signature numérique exécutée sur son dispositif personnel avec une clé secrète protégée.

Via son dispositif personnel, l'utilisateur peut prouver son identité en apportant la preuve de :

- qui il est, par l'usage de la biométrie
- ce qu'il possède, comme des titres d'identité ou des documents authentiques
- ce qu'il sait, par exemple un mot de passe ou un code PIN

Bien entendu, chacun de ces moyens d'authentification doit être implémenté de façon très sécurisée, en reposant sur les composants matériels de sécurité embarqués dans le dispositif personnel.

Un des défis à relever concerne le lien entre l'identité de l'utilisateur et son authentification par les acteurs tiers sur le système numérique, et la possibilité de procéder à tout moment à la vérification de ce lien. Le dispositif personnel de l'utilisateur constituent la passerelle entre le monde réel et le monde numérique. Ainsi, c'est à lui que revient la charge d'héberger les secrets certifiant le lien entre l'identité de l'utilisateur et son identifiant anonyme (ou DID).

6. Comment la blockchain peut-elle s'intégrer dans l'écosystème national et européen actuel ?

Ce chapitre invite à réfléchir sur la façon dont la *blockchain* pourrait s'intégrer dans les réglementations nationales et européennes pour renouveler les pratiques liées à l'identification numérique.

Dans le cadre juridique français et européen, l'utilisation de la technologie de la *blockchain* est possible pour les services offert par le privé ou pour ceux des services publics dont l'objet central n'est pas la gestion de l'identité, comme en témoignent les cas d'usages évoqués au chapitre 4.

Pour aller plus loin, et notamment pour pouvoir l'utiliser pour la gestion des titres d'identité et de voyage, une évolution du cadre juridique national et européen est nécessaire.

6.1. La *blockchain* face au cadre régulateur RGPD

L'article 5 du Règlement Général de Protection des Données à caractère personnel (RGPD) [9] présente les principes à mettre en œuvre dans le traitement des données. Il précise notamment que les données doivent être :

1) traitées de façon loyale et transparente conformément à la Loi,
2) collectées pour une finalité déterminée et ne pas être utilisées à d'autres fins, et surtout ne doivent pas être utilisées à l'insu de l'utilisateur,
3) minimalisées et réduites au strict nécessaire pour l'accès au service demandé,
4) exactes et tenues à jour,
5) conservées sous une forme permettant l'identification des personnes concernées pendant une durée limitée,
6) protégées sous le double aspect de l'intégrité et de la confidentialité.

Le responsable du traitement doit pouvoir démontrer que ces principes sont bien respectés.

Par construction, la *blockchain* garantit la transparence en traçant les flux et accès aux données. Elle protège l'intégrité des données horodatées, mais n'en assure pas la confidentialité. La *Self-Sovereign Identity* assure le principe de minimalisation des données transmises, via un schéma centré sur l'utilisateur, lui garantissant le plein contrôle des données qu'il souhaite divulguer, ainsi que l'exactitude des données conservées et transmises à travers le mécanisme de vérification.

Nous avons déjà relevé que pour assurer la confidentialité des données, il est préférable de les héberger « *off-chain* ». Si la CNIL, soucieuse de la conformité à la RGPD peut tolérer dans ses premiers éléments d'analyse sur la *blockchain* [9] [27] que des données personnelles puissent éventuellement être conservées sur la *blockchain* à condition d'être chiffrées, il n'en reste pas moins que l'idéal est de ne stocker sur la *blockchain* que les références utiles à la réalisation de la preuve de vérification.

La vérification doit permettre de garantir l'exactitude des données présentées. Pour cela, l'usage d'attestations délivrées par des organismes publics habilités est requis. Une personne qui auto-déclarerait un attribut de son identité, son âge par exemple, devrait en fournir la preuve en présentant un document source (titre d'identité).

La question de la conservation des données pendant une durée limitée, de leur mise à jour et du droit à l'oubli, s'avère délicate. Les informations enregistrées sur la *blockchain* sont, par nature, non modifiables. Toutefois, les données à caractère personnel n'ayant pas vocation à être enregistrées sur la *blockchain*, seuls des preuves et/ou des liens vers ces données y figurent : il est alors tout à fait possible de mettre à jour ces données conservées « *off-chain* », de les supprimer ou de les remplacer. Si de surcroît, ces données sont hébergées dans le dispositif de l'utilisateur, c'est lui qui en assure le contrôle.

Le document [27] publié par l'observatoire européen sur la *blockchain* insiste sur la nécessité d'utiliser des fonctions de cryptographie robustes pour éviter que les preuves et/ou les liens enregistrés sur la *blockchain* ne permettent de remonter à l'identification des personnes par traçage, ou encore de remonter aux données brutes.

Aussi, pour que la *Self-Sovereign Identity* contribue à une identification fiable, il faut prouver que l'identifiant anonymisé figurant sur la *blockchain* est bien associé à une identité juridique. Dans une implémentation centrée sur l'utilisateur, seule la personne concernée est en mesure d'en fournir la preuve, via tout dispositif personnel connecté.

Il faut noter au surplus que la vision centralisée du RGDP qui fait porter la responsabilité de la gestion des données personnelles sur les contrôleurs qui gèrent des silos de données ne correspondra plus aux modèles DID transformant les individus en maîtres de leurs données qu'ils pourront eux-mêmes copier, renouveler, partager, déplacer et supprimer.

6.2. Comment le règlement eIDAS peut-il réguler la *blockchain ?*

Cette section propose d'étudier la conformité de la *blockchain* au règlement eIDAS et de déterminer comment et en fonction de quelles exigences une *blockchain* pourrait se voir appliquer les qualifications eIDAS.

En effet, la mise à disposition au niveau international de briques logicielles et de plateformes de *blockchain* (Hyperledger, Corda R3, Ethereum), et l'engouement d'une génération de développeurs pour cette technologie à travers le monde, portent à croire que le foisonnement des initiatives privées va bien au-delà d'un effet de mode et que les initiatives de création de *blockchains* vont continuer à se multiplier.

Ce succès risque de créer une confusion chez le public non-expert et auprès des décideurs potentiels. Il est donc important de pouvoir compter sur un référentiel pour mettre un peu d'ordre dans ce paysage en qualifiant les *blockchains* en fonction du niveau de confiance qu'elles peuvent légitimement inspirer. L'assainissement du marché passe par l'établissement de ce référentiel comparatif commun, particulièrement utile pour les usages qui requièrent un niveau élevé de confiance.

Pour l'instant, en l'absence de tout référentiel dédié à la technologie *blockchain* au niveau international, la qualification de la *blockchain* au regard des exigences eIDAS pourrait offrir une approche intéressante dans un cadre européen, d'autant que la *blockchain* pourrait très bien, dès

maintenant, servir d'appoint technique à l'architecture eIDAS, tout en respectant le RGPD, protecteur des données.

Mais comment apprécier la conformité d'une *blockchain* aux exigences d'un référentiel établi pour l'identification électronique et/ou pour les services de confiance électroniques ?

6.2.1 Intérêt du règlement eIDAS

L'objectif du règlement eIDAS adopté le 23 juillet 2014 par le Parlement européen et le Conseil de l'Union européenne, est d'établir un cadre d'interopérabilité pour les différents systèmes mis en place au sein des Etats membres afin de promouvoir le développement d'un marché de la confiance numérique. Il fournit ainsi, dans une première partie, un socle commun à l'identification numérique des citoyens et des résidents européens et, dans une deuxième partie, des critères communs pour apprécier la fiabilité des services électroniques dits « de confiance ».

La reconnaissance mutuelle entre Etats membres des identifications électroniques et des services de confiance pris en compte dans le règlement ne concerne que les organismes du secteur public qui nécessitent, pour l'accès à l'un de leurs services en ligne, la mise en œuvre d'un moyen d'identification électronique notifié : le règlement eIDAS s'applique uniquement aux échanges entre l'administration et le public (citoyens, entreprises).

Cette reconnaissance mutuelle procède par l'attribution d'un niveau de qualification des identités et des services selon une échelle de confiance à trois niveaux : bas, substantiel ou élevé.

Dans ce contexte, pour être accessible à un autre Etat membre, un service public en ligne utilisant une *blockchain* devrait répondre aux exigences du règlement eIDAS et se voir attribuer un des trois niveaux de confiance.

Il n'existe pas pour l'instant dans eIDAS de corrélation entre les procédures d'identification numérique et celles relatives à la fiabilité des services de confiance, d'où le caractère dual de notre étude qui examine la *blockchain* en la rapportant à chacune de ces deux catégories, d'abord aux moyens d'identification, ensuite aux services de confiance accessibles en ligne.

La Figure 10 montre schématiquement comment la *blockchain* peut s'intégrer dans une architecture eIDAS.

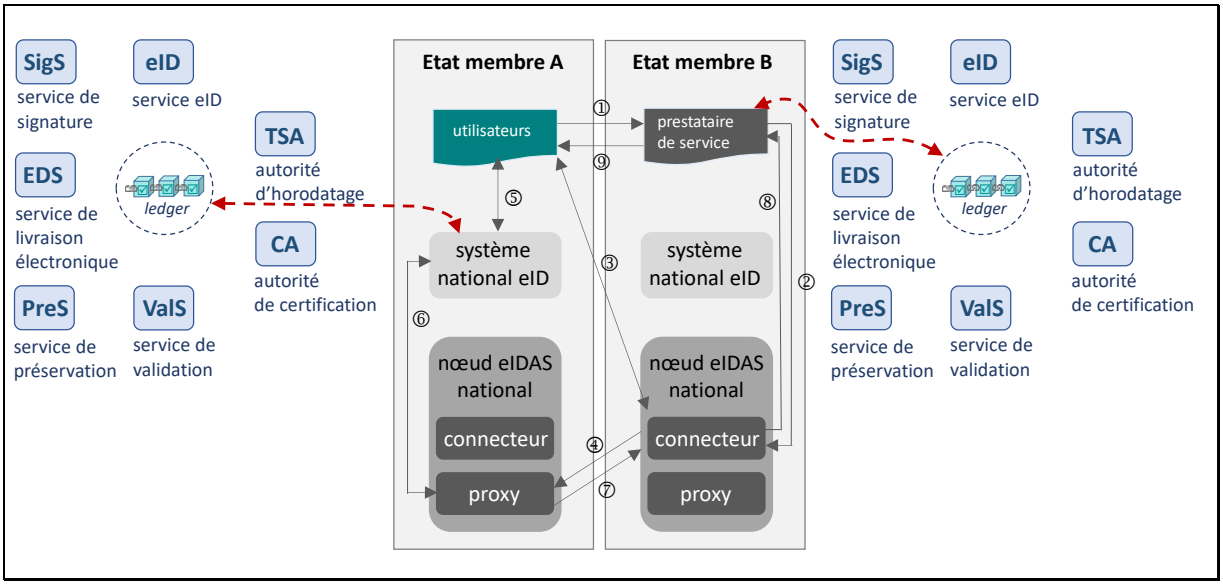


Figure 10 : options pour une blockchain dans un cadre eIDAS

6.2.2. Identification électronique

Si on rapporte la *blockchain* à la partie du règlement eIDAS relative à l'identification électronique, conformément à la suggestion de certains officiels de la DG CNECT de la Commission Européenne, il ressort rapidement que 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 :

- ni la minimisation des données et la divulgation sélective d'attributs,
- ni l'utilisation de références anonymisées comme par exemple les assertions vérifiables certifiées (*Verifiable Credentials*) basées sur le modèle de données du W3C,
- ni la communication d'attributs connexes d'identification, autres que les « données pivot » (qui, renvoyant à l'identité juridique, servent à identifier la personne),
- ni des services en ligne offerts par le privé, (le règlement traite uniquement de l'action des administrations publiques),
- ni l'hébergement des données personnelles sur un dispositif personnel mobile de façon sécurisée.

Pour l'identification électronique, les exigences applicables aux différents niveaux de garantie qui sont prévus par le règlement eIDAS sont détaillées dans le règlement d'exécution n°2015/1502 du 8 septembre 2015. L'article 8 du règlement (UE) 910/2014 permet d'apprécier le niveau de garantie ou *Level of Assurance* (LoA) de cette identité qui repose sur deux types caractéristiques :

- la qualité des données d'identité en elles-mêmes,
- la qualité des moyens d'identification.

On peut observer que le règlement eIDAS mélange ces deux catégories d'éléments de fiabilité, alors que la perspective du traitement sur une *blockchain* conduit à les distinguer. La Figure 11 indique schématiquement la manière d'aborder la *blockchain* sous l'angle d'évaluation eIDAS.

La *blockchain* a vocation à vérifier des assertions vérifiables concernant les attributs d'identité certifiés au sens large, ce qui va au-delà du jeu de données obligatoires ou optionnelles définies par eIDAS (voir à ce sujet le règlement d'exécution (UE) 2015/1501 de la commission du 8 septembre 2015, Annexe sur les exigences relatives à l'ensemble minimal de données d'identification personnelle représentant de manière univoque une personne physique ou morale, visé à l'article 11).

D'une manière générale, une *blockchain* dédiée à la vérification d'identité numérique au sens large, peut comporter parmi ses données enregistrées, des attestations d'attributs de personnes physiques ou morales, des attestations de documents, des assertions vérifiables sur de tels attributs certifiés comportant les liens vers les données personnelles hébergées en dehors de la *blockchain*, ou encore des chemins certifiés de clés publiques permettant la vérification de la chaîne de confiance ayant certifiée ces données. Ces éléments dépassent donc le cadre restreint délimité par l'Annexe de l'Acte d'Exécution 2015/1501 qui définit un ensemble minimal de données respectivement pour une personne physique ou morale, pour les besoins d'interopérabilité entre Etats membres.

Comme évoqué ci-dessus, la *blockchain* peut aussi fonctionner comme dispositif de vérification qui enregistre et maintient la chaîne de confiance des certificats numériques des acteurs dont l'identité est publique. Cela permet aux vérificateurs de procéder à la validation des signatures apposées sur les attributs et/ou sur les documents certifiés présentées par l'utilisateur pour demander l'accès à un service ou la reconnaissance d'un droit. La *blockchain* peut ainsi offrir une sorte de PKI décentralisée.

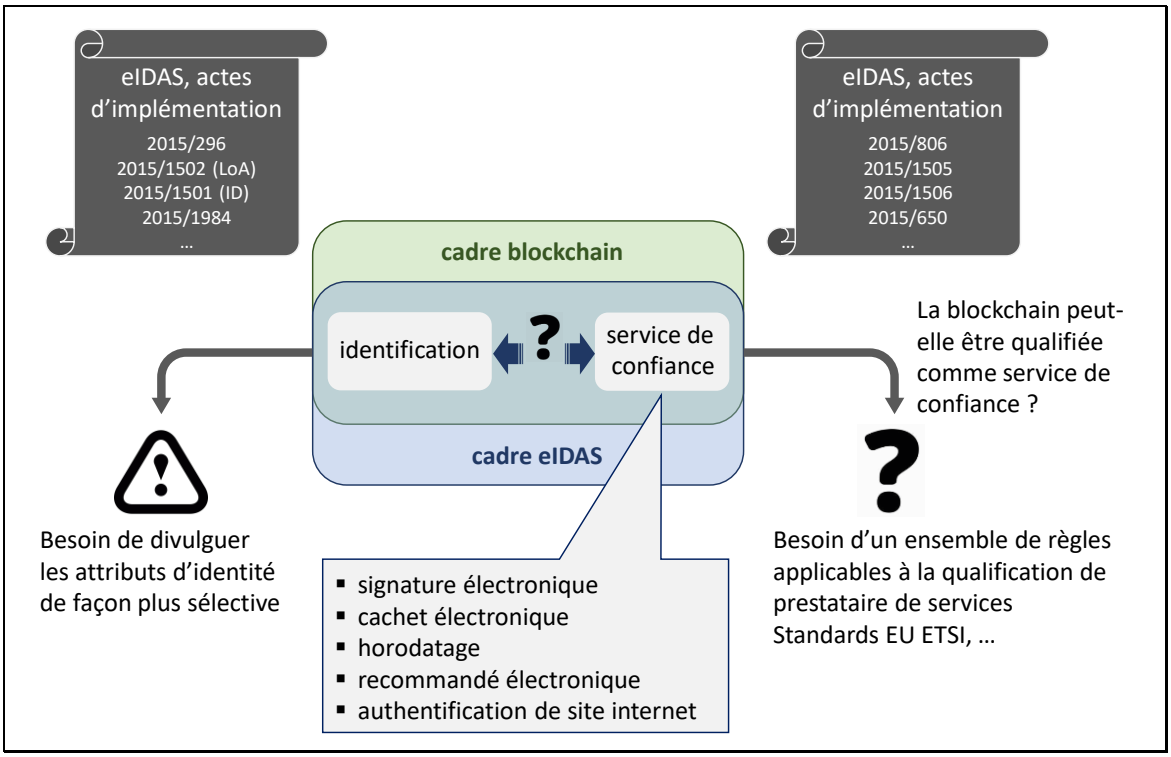


Figure 11 : réflexion sur l'angle d'évaluation de la blockchain au regard d'eIDAS

Si la fonction d'identification est réalisée par une application exécutée sur une *blockchain*, il n'est pas recommandé de conserver les attributs d'identification en clair sur la *blockchain* car cela les exposerait à tous les utilisateurs de la *blockchain*, utilisateurs et nœuds du réseau qui détiennent une réplique du *ledger*. Le fait de contrôler l'accès en consultation à la *blockchain* grâce à des autorisations comme le permet une *blockchain permissioned* ne dispense pas pour autant de préserver les données à caractère personnel par des moyens cryptographiques tels que le chiffrement et le hachage. Il apparaît donc essentiel de faire figurer sur la *blockchain,* non pas les attributs d'identification en clair, mais

uniquement les assertions vérifiables pointant sur les attributs certifiés ou/et les racines et chaînes de confiance des certificats des organismes habilités d'identité publique, tandis que les attributs d'identité et les données à caractère personnel sont préservés sur des dispositifs sécurisés aux mains des utilisateurs.

Dans le cas où une application d'identification s'exécutant sur une *blockchain* voudrait se conformer aux exigences applicables aux différents niveaux de garantie qui sont prévus par le règlement eIDAS, les Actes d'exécution n°2015/1502 du 8 septembre 2015 [46] détaillent les fonctionnalités exigées d'une telle application. Le tableau présenté en annexe A, donne quelques éléments d'équivalence entre les fonctions *blockchain* et certaines exigences du règlement.

6.2.3. Les services de confiance

Le volet « service de confiance du règlement » permet-il une approche plus pertinente de la *blockchain* ? Comment les services de confiance sur *blockchain* peuvent-ils satisfaire aux exigences d'eIDAS et de ses actes d'exécution actuellement publiés ?

Une infrastructure sécurisée fonctionnant sur *blockchain* pourrait gagner en crédibilité grâce à une qualification au titre des services de confiance selon eIDAS. Dans cette optique, il est nécessaire de vérifier si un projet de *blockchain* européen endossé par les autorités publiques des Etats membres peut constituer un service de confiance et pourrait être rattaché à eIDAS lors d'une révision du règlement.

La question de la minimisation des données (RGPD) peut constituer un point d'entrée intéressant pour la mise en avant du service *blockchain* envisagé (conformément aux orientations de la CNIL et de la DG CNECT). Il convient donc d'examiner les exigences qui figurent dans le Référentiel ANSSI pour eIDAS [14] afin d'apprécier dans quelle mesure le projet de *blockchain* pour un service de vérification distribué pourrait répondre aux exigences de sécurité et de confiance.

Pour rappel, Les services de confiances sont les suivants: la délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet, la validation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés, la conservation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés, l'horodatage électronique qualifié, et l'envoi de recommandés électronique qualifié.

Devant la perméabilité des frontières numériques et l'influence grandissante des opérateurs, systémiers et intégrateurs couvrant des domaines transverses, la notion de territorialité numérique fait de plus en plus sens. Dans ce contexte, préserver l'usage de l'identification des personnes pour la facilitation de leur accès aux services dématérialisés réclame non seulement de s'appuyer sur des Règlements Européens mais aussi de distinguer les alternatives qui permettraient de faire front contre la dispersion des données sensibles y compris les données biométriques, les logins et mots de passe, et attributs divers (provenant de fournisseurs publics ou privés) en sus les données d'identité pivot. C'est une telle dispersion qui nourrit fondamentalement le fonds de commerce des exploitants et attaquants (hackers). La posture que prend aujourd'hui la « S*elf-Sovereign Identity* » est telle qu'elle représente une offre de service au citoyen considérée de qualité. Elle lui permet de gérer de façon interactive et responsable ses données personnelles. La S*elf-Sovereign Identity* peut ainsi permettre à l'usager d'accéder aux services numériques en mobilité en s'appuyant sur une protection régalienne de ses attributs d'identité, en lui garantissant une protection contre la traçabilité et le vol d'identité.

6.2.4. Critères d'évaluation de la conformité au règlement eIDAS

Cette section s'appuie sur les critères du référentiel ANSSI pour eIDAS, et présente sous forme de tableaux la correspondance entre les exigences du référentiel et les fonctions assurées par les différentes couches organisationnelles de la *blockchain*.

Les exigences spécifiques applicables aux prestataires de services de confiance disposant déjà d'une qualification selon le RGS[71] ne sont pas listées ci-dessous mais peuvent être consultées sur le site de l'ANSSI. A noter que si un service de confiance est déjà qualifié selon le RGS, il peut bénéficier des modalités de transfert de la qualification RGS vers la qualification correspondante règlement eIDAS.

Dans les sections suivantes, seul le service d'horodatage est traité en détail, à titre d'exemple, pour illustrer l'approche adoptée. Les autres services feront l'objet du même traitement qui a fait l'objet d'une contribution française, après validation par AFNOR, au comité européen CEN/CENELEC JTC19 pour son nouvel item sur « *Blockchain* et eIDAS ».

Encart A :

Critères d'évaluation de la conformité au règlement eIDAS aux services d'horodatage électronique qualifiés

Le Tableau 2 présente les critères d'évaluation de la conformité au règlement eIDAS Version 1.1 du 3 janvier 2017 (SGDSN/ANSSI) appliqué à l'article de référence du Règlement eIDAS (UE). Le référentiel de l'ANSSI décrit les exigences relatives à la qualification des services d'horodatage électronique selon le règlement eIDAS (Annexe 2 du référentiel ANSSI).

Tableau 2 : couverture des exigences du règlement pour l'horodatage

Extrait du référentiel ANSSI [47]			
Article	**Exigence du règlement eIDAS**	**Clauses applicables des normes EU**	**Fonctions *blockchain***
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_421] Clauses 7.6.2 et 7.6.3	Voir note 1
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance (7 ans après l'expiration du jeton d'horodatage)	[EN_319_421] Clause 7.12	Voir note 2
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_421] Clause 7.14	Voir note 3
42(1).a	Lien entre date, heure, et données	[EN_319_421] Clauses 7.6.3 et 7.7.1	Voir note 4
42(1).b	Fondation sur une horloge exacte reliée à l'UTC	[EN_319_421] Clauses 7.7.1 et 7.7.2	Voir note 5
42(1).c	Signature ou cachet électronique avancé, ou méthode équivalente	[EN_319_421] Clause 7.7.1	Voir note 6

✓ Note 1

Un service d'horodatage externe fiable peut être mis à la disposition des nœuds du réseau participant à la *blockchain* pour assurer la synchronisation des horloges. Dans ce cas, une unité d'horodatage peut être installée par la gouvernance de la *blockchain* et être identifiée sur une liste de confiance. L'authentification peut se faire par le biais d'un certificat délivré par une autorité de certification reconnue dans la charte de gouvernance de la *blockchain*.

[71] Référentiel Général de Sécurité (RGS)

L'enregistrement du certificat dans le *ledger* s'effectue via un *smart contract,* permettant à tous les acteurs autour de la *blockchain* d'effectuer des vérifications.

✓ Note 2

Par construction, la *blockchain* enregistre et conserve les informations de manière immuable (au-delà des sept années de conservation requises). Un bloc ne peut être modifié sans affecter l'intégralité de toute la chaîne située en aval de ce bloc. La rectification requiert une telle quantité de calcul qu'elle en devient quasiment impossible à réaliser (sauf attaque des 51% ou similaire). Les informations enregistrées dans le *ledger* peuvent être considérées comme stables et pérennes.

Les blocs sont horodatés par construction, estampillant ainsi l'ensemble des données qu'ils contiennent.

Au cas où une *blockchain* est déclassée (en cas de non utilisation, d'attaque, de mise à jour…), la charte de gouvernance doit prévoir le transfert du contenu du *ledger* vers un autre système préservant les données et l'accessibilité. Les nœuds du réseau ayant participé à une *blockchain* peuvent conserver leur copie la plus récente de la chaîne même après son déclassement.

Le caractère distribué de la *blockchain* lui confère une résilience forte, assurant que les enregistrements restent accessibles même au cas où plusieurs nœuds du réseau venaient à s'interrompre.

Le cycle de vie des clés et des certificats utilisés par l'unité d'horodatage doit être tracé, mais pas nécessairement enregistré dans le *ledger* bien que ce soit une option possible.

✓ Note 3

Si l'autorité d'horodatage n'est plus en service, elle doit révoquer toutes ses unités d'horodatages agissant sur la *blockchain*.

L'autorité d'horodatage devra suivre la procédure décrite par les exigences de la norme ETSI EN 319 401, clause 7.12 qui prescrit notamment une feuille de route lors de la mise hors service, des notifications aux abonnés au service (en l'occurrence les nœuds et utilisateurs de la *blockchain*), cessation des autorisations en cours délivrées aux sous-contractants, transfert de responsabilité à un tiers de confiance, destruction des clés privées du fournisseur d'horodatage et révocation des certificats, prévision des réserves financières utiles pour assumer les coûts d'un tel transfert de responsabilité en cas de faillite du prestataire d'horodatage. Toutes ces mesures devront être prévues dans la charte de gouvernance de la *blockchain*.

✓ Note 4

Chaque bloc comporte au moins un identifiant, en particulier le haché de l'ensemble de son contenu, l'adresse de compte du nœud mineur ayant construit le bloc, la signature numérique du nœud mineur, l'horodatage du bloc. Les données formant le contenu du bloc sont ainsi liées de façon immuable à l'horodatage.

✓ Note 5

La *blockchain* utilise un horodatage basé sur l'heure Unix (*Unix Time-stamping*) qui est une convention qui indique le nombre de secondes écoulées depuis le 1er janvier 1970 à 00:00:00 UTC ; elle est supportée par tous les systèmes conformes à la norme POSIX (IEEE 1003) associant un nombre réel à un évènement dans le temps.

Plusieurs nœuds participants concurremment à la validation des blocs, il est indispensable que leurs horloges soient synchronisées pour un horodatage calibré.

Les transactions délivrées au réseau ne sont pas nécessairement assorties d'un horodatage sauf si les données portées par la transaction sont préalablement estampillées. L'inclusion des transactions dans un bloc de la *blockchain* leur associe par construction l'horodatage du bloc, assurant la notarisation des transactions enregistrées, ainsi que leur ordonnancement.

Par exemple, avec Ethereum, l'API `web3.js` permet à l'application cliente de communiquer avec la *blockchain* et les *smart contracts*. La commande `web3.eth.getBlock()` retourne les méta-données d'un bloc, dont l'horodatage avec notamment l'horodatage de la validation du bloc. La fonction d'échange de messages entre nœuds du réseau avec le protocole Whisper offre un service de souscription à un événement. La commande `web3.shh.subscribe()` permet de connaitre l'horodatage d'un message, et la commande `web3.shh.getFilterMessages()` retourne les messages filtrés et horodatés selon un critère donné en paramètre.

✓ Note 6

L'horodatage utilisé par la *blockchain* devra être conforme au profil décrit par la norme ETSI 319 422 : il devra répondre à des critères de qualité vérifiables tels que l'alignement sur un service de métrologie local ou international officiel comme par exemple le Bureau International des Poids et Mesures (BIPM).

La synchronisation de l'horodatage avec l'horloge UTC devra être dans les limites de précision définies par la charte de gouvernance de la *blockchain* ou indiquée dans les données de l'horodatage même, faute de quoi, l'unité d'horodatage ne serait pas en mesure d'effectuer l'horodatage d'un bloc.

La clé privée de signature de l'horodatage devra être exclusivement dédiée à cet usage. L'unité d'horodatage devra impérativement cesser toute émission à partir de cette clé privée dès lors que sa date limite de validité est atteinte et que son certificat est révoqué.

Encart B :

Critères d'évaluation de la conformité au règlement eIDAS aux services de conservation qualifiés des signatures et des cachets électroniques qualifiés

Le Tableau 3 présente les critères d'évaluation de la conformité au règlement eIDAS version 1.0 du 03 janvier 2017 (SGDSN/ANSSI) appliqué à l'article de référence du Règlement eIDAS (UE). Les exigences décrites par l'ANSSI dans son référentiel permettent d'apporter une présomption concernant la fiabilité, au-delà de la période de validité technologique, des signatures électroniques qualifiées et des cachets électroniques qualifiés tels que définis par le règlement eIDAS (Annexe 2 du référentiel ANSSI).

Tableau 3 : Couverture des exigences du règlement pour la conservation des signatures et cachets

Extrait du référentiel ANSSI [48]			
Article	**Exigence du règlement eIDAS**	**Clauses applicables des normes EU**	**Fonction Blockchain**
24(2).e	Utilisation des systèmes et des produits fiables	[EN_319_401] Clauses 7.7	
24(2).h	Conservation des informations délivrées et reçues par le prestataire de services de confiance (7 ans après l'expiration du jeton d'horodatage)	[EN_319_401] Clause 7.10 [NF_Z42_013] V.6 et [GA_Z41-019] (archivage électronique)	
24(2).i	Continuité de service suite à l'arrêt d'activité du prestataire de services de confiance	[EN_319_401] Clause 7.12	
34(1)	Utilisation de procédures et technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées	[NF_Z42-013] et [GA_Z42-019] [EN_319_102-1] Clauses 4.3.5 (extension des signatures et cachets électroniques / capture des informations de validation)	
40	Application *mutatis mutandis* de l'article 34 à la conservation des cachets électroniques qualifiés		

Selon les dernières informations, il semble pour l'instant tout aussi difficile de modifier les actes d'exécutions de eIDAS pour étendre leur application à la *blockchain* sans toucher au règlement, que de reconfigurer le règlement eIDAS lui-même, lequel a déjà fait l'objet d'un consensus déjà difficile à obtenir entre Etats membres.

Pour l'instant, eIDAS semble devoir rester agnostique par rapport à la *blockchain* ou à toute autre solution technique. Il est peu probable qu'une qualification spécifique à la *blockchain* comme service d'identification figure prochainement dans le règlement.

Néanmoins, les agents de la DG CNECT sont conscients de la nécessité de travailler sur l'« encapacitation » (*empowerment*) de l'utilisateur en essayant de développer une *Self Sovereign Identity* éventuellement en relation avec eIDAS. Une analyse juridique est actuellement en cours dans les instances européennes.

Cependant, la question de la création d'un référentiel pour apprécier les niveaux de confiance qu'il est légitime d'accorder à une *blockchain* reste entière et peut être traitée ailleurs que dans le règlement eIDAS ; en tout état de cause, des ajustements seront nécessaires, quel que soit le véhicule « normatif » envisagé, qu'il s'agisse d'une règle juridique ou d'une normalisation plus technique.

6.3. Vers un partenariat européen pour la *blockchain*

Les perspectives offertes par l'utilisation de la *blockchain,* comme technologie d'appoint dans l'écosystème européen reposant sur les règlements eIDAS et RGPD, a suscité l'intérêt de la Commission Européenne sous l'impulsion de la DG CNECT notamment. C'est ainsi qu'à l'heure où le présent Livre Blanc est publié, on voit avancer le projet initié par le partenariat européen pour la *blockchain* (*European Blockchain Partnership*, EBP), co-signé par de nombreux Etats Membres dont la France. L'*European Blockchain Service Infrastructure* (EBSI) qui désigne l'initiative conjointe de l'EBP et de la Commission Européenne pour spécifier le fonctionnement des services publics transfrontaliers à l'échelle de l'UE, en est une des concrétisations.

Il s'agit d'un réseau multi-*blockchains* avec de multiples cas d'utilisation, tels que la notarisation de documents, la certification de diplôme, le partage de données de confiance et l'*European Self-Sovereign Identity Framework* (ESSIF). Figurant au nombre de ces usages, le projet ESSIF, qui désigne le cadre de déploiement européen pour l'identité souveraine réunit des experts de nombreux Etats membres autour de la réalisation d'un cadre commun de déploiement de la *SSI*. Ce nouveau cadre doit être le socle technique incluant interfaces et briques technologiques pour l'interopérabilité autour d'un système distribué, en l'occurrence par *blockchain*, de vérification de l'identité des utilisateurs pour l'accès aux services numériques privés et publics. Ce projet est conçu comme un complément au règlement eIDAS pour y puiser un solide justificatif régalien des assertions vérifiables que l'utilisateur pourra réunir comme autant de preuves de son identité et/ou pour son profil. En d'autres termes, l'utilisateur pourra collecter des assertions estampillées eIDAS, en provenance de fournisseurs d'identité publics. Un prototype appelé « pont eIDAS pour le *Self-Sovereign Identity* »[72] (« SSI *eIDAS bridge* ») est déjà en cours de développement pour offrir une validation d'attributs par eIDAS sur demande des utilisateurs, à distance et de façon synchrone.

Le comité européen CEN/CENELEC JTC19 a démarré officiellement ses travaux le 17 Février 2020 pour entreprendre, au bénéfice de l'ESSIF, un projet de normalisation sur la gestion décentralisée de l'identité en tenant compte de l'environnement eIDAS et RGPD. L'AFNOR est membre actif de ce comité. Une des difficultés que le JTC19 devra résoudre consiste à qualifier des attributs provenant d'émetteurs privés parmi d'autres attributs régaliens. Autrement dit, comment évaluer le niveau de confiance globale accordé à une liste d'attributs d'origines mixte, publique et privée dans un contexte où un des objectifs principaux consiste à fournir aux vérificateurs responsables de l'accès aux services à valeur ajoutée le moyen d'établir en toute confiance le droit d'accès sur la base des assertions vérifiables présentées par les utilisateurs.

Dans le même sens, un comité de l'ISO (ISO SC17 WG4/WG10) s'est attaché depuis 2019 à spécifier une approche méthodique de l'évaluation du niveau de confiance dans les données délivrées depuis un dispositif mobile à un vérificateur pour servir les besoins d'identification depuis un mobile. Ce travail en cours délivrera une Spécification Technique ISO sous le numéro ISO/IEC TS 23220-5 coéditée par la France et les USA.

Tous ces travaux sont très précieux pour aider à la diffusion de l'intérêt que représente l'utilisation des *blockchains* pour la gestion des identités.

[72] *https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about*

6.4. Urbanisation de FranceConnect dans un contexte *blockchain*

L'impact possible des transformations numériques qu'introduit l'usage d'une *blockchain* est discuté dans cette section. Comment une *blockchain* peut-elle venir étoffer une infrastructure préexistante telle que FranceConnect pour les besoins d'un service d'identification, et comment un schéma de *Self-Sovereign Identity* pourrait-il se greffer sur cette infrastructure ?

FranceConnect est la plateforme en ligne de l'Etat, créée en 2016, qui permet aux utilisateurs de se connecter à un nombre croissant de services publics français avec les mêmes identifiants. FranceConnect se positionne comme l'intermédiaire de confiance entre les fournisseurs d'identité et les utilisateurs.

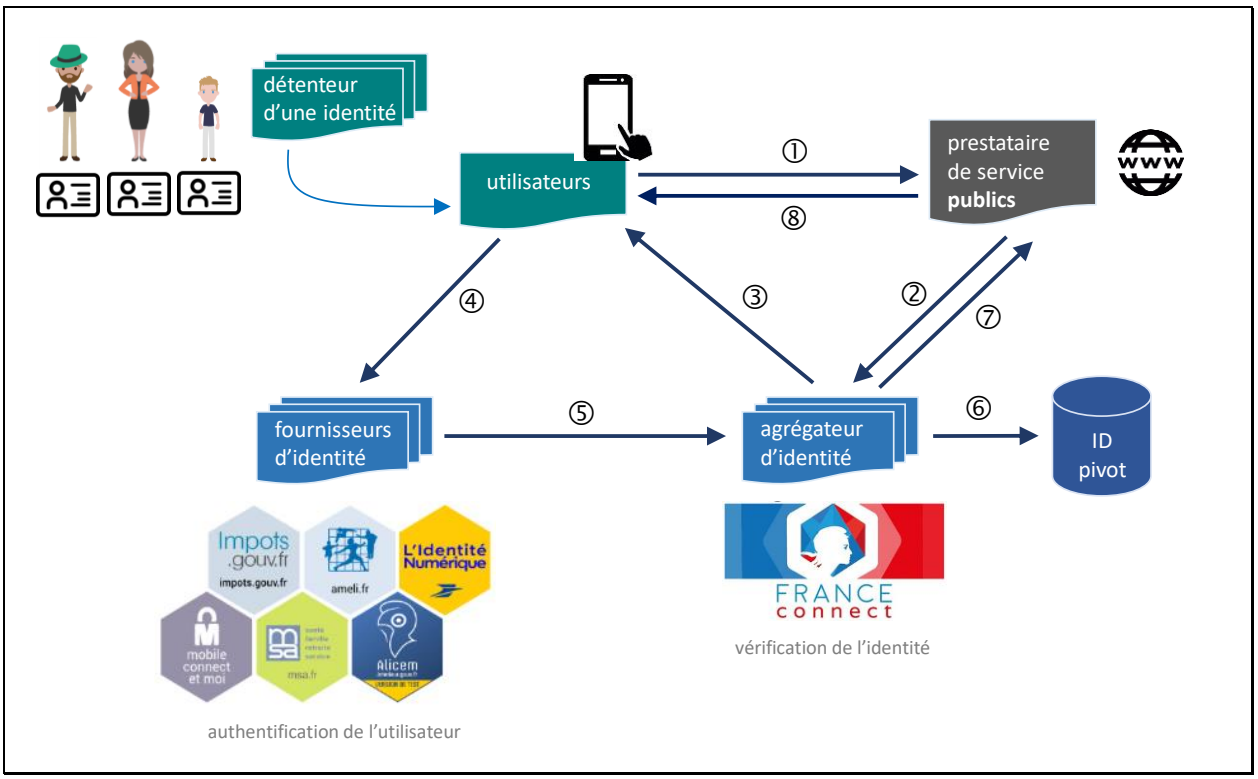


Figure 12 : flux et rôles avec FranceConnect
(les flèches indiquent la séquence des opérations et non pas la continuité de la session)

La séquence des opérations effectuées dans le but d'identifier l'utilisateur avec FranceConnect est présentée sur la Figure 12 et explicitée ci-dessous :

① L'utilisateur se connecte à un service public français
② Le service public redirige l'utilisateur vers FranceConnect
③ FranceConnect redirige vers les fournisseurs d'identité
④ L'utilisateur sélectionne un fournisseur d'identité fournissant un niveau d'assurance suffisant pour le service demandé, puis il s'authentifie avec les informations d'identification appropriées (numéro fiscal, numéro social, email…)
⑤ Le fournisseur d'identité transmet le statut à FranceConnect, ainsi que les attributs d'identité
⑥ FranceConnect vérifie l'identité et la cohérence, par exemple en comparant au référentiel d'identité pivot maintenu par l'état
⑦ FranceConnect notifie le service public
⑧ L'utilisateur accède au service public requis

Parmi les fournisseurs d'identité, seul Alicem, actuellement en cours d'évaluation au moment de la publication de ce Livre Blanc, est prévu fournir un niveau d'assurance élevé au regard du référentiel eIDAS.

La divulgation sélective d'un attribut d'identité, choisi parmi les attributs de « l'identité pivot » ou parmi d'autres attributs, au service demandé, n'est pas envisageable dans le schéma présent. Pour l'instant, FranceConnect donnant seulement accès à des services publics français, la transmission de l'ensemble des attributs d'identité ne saurait être considérée comme critique.

A l'avenir, il est possible que des prestataires de service privés ou encore des services publics d'Etats membres de l'UE, puissent être accessibles via FranceConnect. Le besoin de divulguer de façon sélective les seuls attributs d'identité nécessaires au traitement du service demandé deviendra alors plus pressant.

Un schéma de *Self Sovereign Identity* permettrait de répondre à ces besoins de minimalisation des données transmises, et pourrait aussi permettre à l'utilisateur d'accéder au service d'un prestataire privé sous couvert de l'anonymat. Supporté par une *blockchain*, la *Self Sovereign Identity* amène à redéfinir les rôles de l'infrastructure FranceConnect préexistante selon le schéma de la Figure 13.

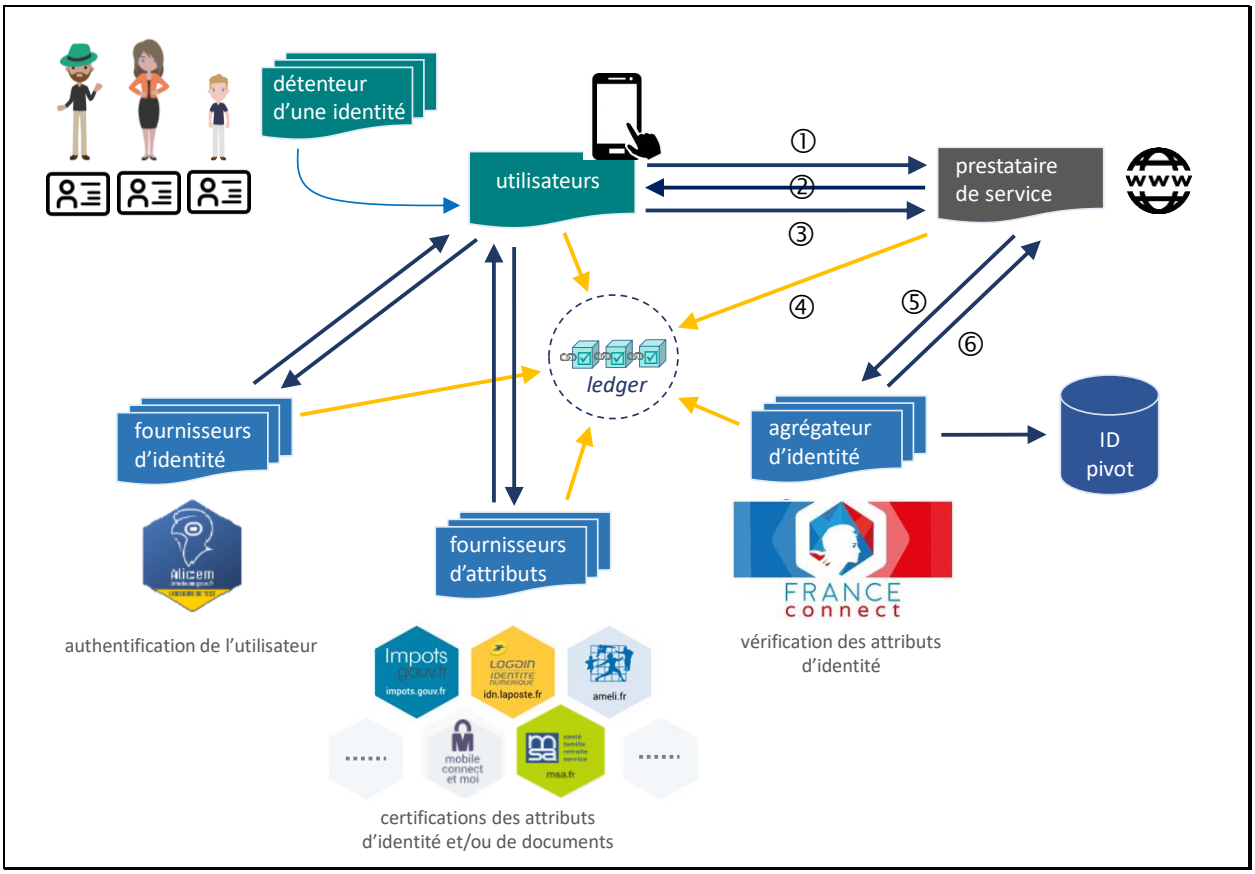


Figure 13 : exemple de Self-Sovereign Identity opérée avec une blockchain dans l'infrastructure FranceConnect

Dans ce schéma, l'utilisateur doit préalablement à toute transaction, s'enrôler auprès d'un fournisseur d'identité afin d'acquérir un identifiant numérique. Dans un second temps, il peut faire appel à des organismes habilités pour certifier ses documents authentiques ou ses attributs d'identité. Il reçoit alors une attestation qu'il pourra présenter au prestataire de service afin de prouver l'authenticité de ses données personnelles. Le prestataire peut déléguer la vérification à un tiers de confiance. Dans l'exemple illustré sur la Figure 13, une utilisation envisageable de FranceConnect lui ferait jouer le rôle

de vérificateur des assertions présentées par l'utilisateur au prestataire de service public (ou privé à l'avenir).

① L'utilisateur se connecte à un service public (ou privé ?)

② Le service demande des attributs d'identité à l'utilisateur

③ L'utilisateur communique de façon sélective certains attributs d'identité

④ Le prestataire de service consulte dans la *blockchain* les références permettant la vérification de ces attributs d'identité

⑤ FranceConnect effectue la vérification des attributs d'identité fournis

⑥ FranceConnect répond au prestataire de service sur la validité des attributs présentés par l'utilisateur

Sur la Figure 13, FranceConnect pourrait jouer le rôle de vérificateur dans un contexte où la *blockchain* orchestrerait un service distribué d'identification. Le rôle d'agrégateur d'identités numériques pourrait être complété par un rôle de vérificateur, au même titre que tout autre vérificateur habilité qui serait mandaté par un prestataire de service public ou privé. L'accréditation des fournisseurs d'identité (Alicem, La Poste, Ameli, impôts.gouv.fr…) est, dans ce cas, vérifiable sur le *ledger* de la *blockchain*. Dans un tel schéma, l'utilisateur gèrerait lui-même ses données personnelles et aucune donnée le concernant ne serait transmise par un tiers sans son consentement, ni même à son insu. Il aurait pleinement le contrôle de ses données d'identité et de ses documents authentiques.

7. Conclusion

Ce Livre Blanc nous a permis de mettre en évidence des concepts émergents tels que les « données pivot », ensemble minimal d'informations permettant d'identifier une personne de façon incontestable, le concept d'« individualisation » qui désigne la reconnaissance d'une personne sans être pour autant capable de l'identifier (au sens de le nommer), concept qui gagnerait à être encadré juridiquement, tant dans une optique d'ordre publique que pour protéger la vie privée. Dans ce cadre protecteur un autre concept émergent appelé à prendre une grande importance est celui de « furtivité », compris comme l'inverse de la traçabilité numérique ; dans certains cas, la furtivité pourra être assurée par une *blockchain*.

Cette réflexion sur la *blockchain* dans ses rapports à l'identité nous a permis de constater qu'il est possible, et même souhaitable dans une optique de protection de la vie privée, de dissocier l'identification d'une personne de l'authentification de ses droits (chapitre 3). Elle nous a permis aussi de constater que la *blockchain*, munie d'une gouvernance adaptée, pourrait être un moyen de concilier la traçabilité avec la protection des données personnelle, de réconcilier en quelque sorte les préoccupations de sûreté et de sécurité avec les exigences des libertés publiques protectrices de l'intimité.

Mieux encore, par son adaptabilité et sa plasticité (chapitre 4), l' « encapacitation » des individus leur donne les moyens de gérer eux-mêmes leurs attributs d'identité et d'être informés de la divulgation des informations les concernant, tout en conservant à l'Etat son rôle de garant ultime des identités juridiques dans un univers de confiance. C'est ce que l'on appelle la *Self Sovreign Identity* décrite au chapitre 5. Un tel système peut avantageusement être opéré sur une *blockchain*.

Comment concrètement mettre à profit les diverses fonctionnalités de la *blockchain* dans la gestion de l'identité ?

1) Proposer des modifications du règlement européen eIDAS de façon à qualifier une gestion de l'identité par *blockchain* et prévoir l'implémentation de cette technologie sur l'architecture du système européen mis en place par eIDAS, en soulignant l'intérêt de prendre en compte le plus tôt possible les services offerts par les entreprises privées, notamment la fourniture d'attributs d'identité venant de prestataires privés,

2) Donner mandat à la représentation française au JTC19 du CEN/CENELEC via la commission de normalisation compétente de l'AFNOR (CN *blockchain*) de participer à la création d'un référentiel des niveaux de confiance d'une *blockchain* et influer dans le même sens et de la même façon sur les travaux de l'ISO au TC307,

3) Constituer une représentation française coordonnée (avec idéalement une représentation de ministères régaliens) dans les instances européennes évoquées au chapitre 6 : *European*

Blockchain Partnership, et *l'European Blockchain Service Infrastructure*, sans oublier l'*European Self-Sovereign Identity Framework*, coordonnée avec les travaux du JTC19,

4) Travailler avec les entreprises privées et les instances publiques sur l'utilisation de la *blockchain* comme vecteur du « compagnon numérique » (passeport dématérialisé) lors des passages frontières pour sécuriser les titres de voyage,

5) Travailler sur les interconnexions du système de fédération d'identités FranceConnect avec des *blockchains*, ainsi que sur l'urbanisation du projet de carte nationale d'identité électronique développé par France Identité Numérique par des *blockchains* en soulignant l'intérêt des deux fonctionnalités suivantes : la possibilité de vérifier des attributs d'identité, et la possibilité de certifier des attributs au profit de prestataire de service,

6) En ce qui concerne les nombreux usages de la *blockchain* pour lesquels l'identification est connexe, il importe de faire connaitre les ressources de la *blockchain* aux différentes filières économiques : l'Afnor serait un espace pour diffuser l'information,

7) Inciter, y compris financièrement, les organismes de recherche à travailler sur des algorithmes de preuve garantissant une confiance élevée et moins consommateurs d'énergie que la preuve par le travail (*Proof of Work*),

8) Ne pas hésiter à mobiliser des moyens pour ancrer la confiance dans les dispositifs personnels, en particulier avec l'emploi de composants matériel de sécurité. On oublie trop souvent que le corollaire de la sophistication des logiciels et des applicatifs est la fiabilité des équipements de sécurité mis à la disposition des usagers, notamment sous la forme de portefeuilles électroniques (*wallets*). Pouvoir disposer d'outils sécurisés est une des conditions de l' « encapacitation » des usagers (*empowerment*) que les auteurs de ce Livre Blanc appellent de leurs vœux.

Le sujet présenté par ce livre Blanc se situe à l'intersection de plusieurs disciplines. Il nécessite un dialogue approfondi entre juristes, ingénieurs, chercheurs et membres d'instances de normalisation.

Annexe A

Le tableau suivant présente quelques éléments d'équivalence entre les fonctions *blockchain* et certaines exigences du règlement eIDAS, Actes d'exécution n°2015/1502 du 8 septembre 2015 [46].

Tableau 4 : quelques équivalences sur les niveaux de garantie du règlement

Exigences eIDAS Références	**Description**	**Application à la *blockchain***
Reconnaissance mutuelle des identifications électroniques	Chaque Etat membre doit reconnaître les moyens d'identification électronique issus des systèmes d'identification électronique des autres Etats membres, à condition que le système en question respecte certaines conditions et ait été notifié à la Commission européenne.	Alors que eIDAS est fédératif, la *blockchain* est distribuée, donc offrant un même système d'identification pour tous les utilisateurs et pour une *blockchain* donnée (même gouvernance et contrôles à travers par exemple les permissions et la/les preuves de validation utilisées) La reconnaissance mutuelle porte donc sur la charte commune de gouvernance de la *blockchain* (qui touche aux *smart contracts*, à la reconnaissance des nœuds de validation, aux résolutions en cas de ***fork*** ou de modification de la preuve en cours de vie de la *blockchain*, à la protection des données personnelles s'il y a lieu, à la confidentialité des transactions...)
Champ d'application : le règlement eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques, élargissant ainsi le champ d'application de la directive 1999/93/CE sur la signature électronique, qu'il abroge.	Le règlement formule des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique ainsi qu'à celle des signatures électroniques, pour les échanges entre les organismes du secteur public et les utilisateurs. Il exclut les échanges internes des administrations sans impact direct sur les tiers ainsi que les actes sous-seing privé. Le règlement eIDAS s'applique aux échanges entre l'administration et le public (citoyens, entreprises) et ne s'applique pas aux « systèmes fermés ».	Les cas d'usages SSI concernés sont ceux impliquant le secteur public et les services à l'utilisateur pour entrer dans le champ d'application eIDAS. Les *blockchain* privées*, ou de consortium, sont en dehors du champ d'application du règlement : le règlement ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés n'ayant pas d'impact direct avec des tiers. Au moins 3 catégories de chaîne sont à considérer au regard de cette exigence selon la terminologie de ISO/IEC WD TS 23635 explicitée dans le glossaire : A. *blockchain « Permissioned/*Privée » → **hors du champ d'application** Seuls les utilisateurs authentifiés et autorisés peuvent soumettre des transactions et consulter le *ledger*. Seuls les nœuds mineurs (ou minteurs), enrôlés peuvent mettre à jour le *ledger* et faire évoluer la charte de gouvernance. B. *blockchain « Permissioned/*Publique » → **dans le champ d'application** Tout le monde peut soumettre des transactions et accéder au *ledger*. Seuls les nœuds mineurs (ou minteurs), enrôlés peuvent mettre à jour le *ledger* et faire évoluer la charte de

Exigences eIDAS Références	Description	Application à la *blockchain*
		gouvernance. La participation au consensus pourrait être ouverte à des nœuds validateurs quelconques. C. <u>*Blockchain* « *Permissionless*/Publique »</u> → **hors du champ d'application** Tout le monde peut soumettre des transactions et accéder au *ledger*. Tout le monde peut déployer un nœud mineur (ou minteur), soumettre un nouveau bloc pouvant compléter le *ledger* et s'impliquer dans la gouvernance de la *blockchain*.
Authentification des sites web, eIDAS Récital (67)	Confiance de l'utilisateur dans un site web qui est authentifié.	
Notification du moyen d'identification électronique (depuis le 29 sept 2015)	Le moyen d'identification électronique doit avoir été délivré conformément à un schéma d'identification électronique notifié par l'Etat membre concerné et figurant sur la liste publiée par la Commission.	Il faudra une démarche de notification du moyen d'identification depuis un dispositif personnel pouvant se connecter à une *blockchain,* pour qu'il apparaisse dans la liste publiée par la Commission.
Niveaux de garantie des schémas d'identifications électroniques définies par l'article 8	L'article 8 du règlement (UE) n° 910/2014 prévoit qu'un schéma d'identification électronique notifié en vertu de l'article 9, paragraphe 1, doit préciser les niveaux de garantie (Faible, Substantiel, Elevé) Le moyen d'identification électronique doit présenter un niveau de garantie égal ou supérieur à celui requis pour accéder au service du secteur public.	Il faut établir la correspondance entre les procédures décrites par l'Annexe du règlement d'exécution (UE) 2015/1502 de la commission et les procédures mises en œuvre pour interagir avec une *blockchain*. Pour chaque procédure identifiée, il faut voir quelles exigences techniques s'imposent notamment pour le niveau « Elevé ». Voir section 2 de l'Annexe qui décrit les spécifications techniques et les procédures servant à déterminer de quelle façon les exigences et les critères de l'article 8 du règlement (UE) n°910/2014 sont appliqués aux moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique. Annexe « Spécifications techniques et procédures pour les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié »
Détail des spécifications techniques et procédures (UE) 2015/1502	2.1 Inscription	
	2.1.1 Demandes et enregistrements	Enrôlement des utilisateurs et des possesseurs, personnes physique ou morale d'identité publique, des nœuds mineurs (ou minteurs).
	2.1.2 Preuve et vérification d'identité (personne physique)	L'enrôlement des utilisateurs doit suivre une procédure, selon un moyen d'identification électronique qualifié, permettant de vérifier l'identité selon le niveau d'assurance Faible, Substantiel ou Elevé.

Exigences eIDAS Références	Description	Application à la *blockchain*
	2.1.3 Preuve et vérification d'identité (personne morale)	L'enregistrement des nœuds mineurs (ou minteurs) devra être conforme à la charte de gouvernance, et les possesseurs de ces nœuds, d'identité publique, devront être enrôlés de manière nominale avec un moyen permettant leur identification par les nœuds validateurs participant au consensus. Il faut noter qu'eIDAS ne s'applique pas aux machines mais aux personnes morales ou physiques.
	2.1.4. Lien établi entre les moyens d'identification électronique de personnes physiques et morales	Le lien entre la personne physique agissant au nom de la personne morale doit être établi selon une procédure reconnue à l'échelle nationale et enregistré par une autorité. L'usage d'une DPKI et l'enregistrement dans le *ledger* des certificats des autorités et des personnes morales d'identité publique peut être effectué avec des *smart contracts*.
	2.2. Gestion des moyens d'identification électronique	
	2.2.1. Caractéristiques et conception des moyens d'identification électronique	Cette exigence fait ressortir le besoin d'établir un lien fort et vérifiable entre la personne physique et l'identité numérique décentralisée (DID) qui soit conforme aux moyens d'identification et aux principes d'eIDAS. Sur la blockchain, l'enregistrement de ZKP via des *smart contracts* peut permettre de contribuer à ce besoin.
	2.2.2. Délivrance, mise à disposition et activation	Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement à la personne à laquelle il destiné. Le dispositif qui embarque le portefeuille (*wallet*) devra préserver les clés secrètes de l'utilisateur, sous-jacentes à son identifiant numérique, qui lui seront confiées dans les conditions requises par le règlement.
	2.2.3. Suspension, révocation et réactivation	Il devrait être possible de suspendre et/ou de révoquer, puis de réactiver le cas échéant un moyen d'identification électronique de manière rapide et efficace, ainsi que des DID dans le cas de la blockchain. Ceci devrait s'appliquer aux portefeuilles (*wallet*) des utilisateurs (personnes physiques) et des personnes morales possédant un ou plusieurs nœuds mineurs (ou minteurs).
	2.2.4. Renouvellement et remplacement	Il devrait être possible de renouveler ou de remplacer son moyen d'identification électronique en apportant les preuves de son identité à une autorité qualifiée.
	2.3. Authentification	
	2.3.1. Mécanisme d'authentification	Le dispositif de l'utilisateur doit être conçu de façon à assurer la protection des données d'identification ou données à caractère personnel, y compris hors ligne. Le

Exigences eIDAS Références	Description	Application à la *blockchain*
		mécanisme d'authentification mis en œuvre doit être robuste aux attaques par man-in-the-middle, aux attaques par rejeu, et garantir la confidentialité et l'intégrité des données échangées. La *blockchain* présente une technologie assurant par construction ces exigences, la confidentialité étant à considérer en lien avec des éléments de stockage « *off-chain** », conformément à la règlementation RGPD. Le service d'authentification du prestataire de service doit être reconnu comme qualifié.
	2.4. Gestion et organisation	
	2.4.1. Dispositions générales	Charte de gouvernance de la *blockchain*
	2.4.2. Avis publiés et information des utilisateurs	La charte de gouvernance de la *blockchain* doit être disponible. Des fonctionalités de "*discoverability*" devraient être offertes pour fournir des informations telles que le nombre de nœuds mineurs (ou minteurs), la personne morale qui en répond, la nature et la garantie des "*smart contracts*", le type de consensus déployé, la localisation des actifs, etc.
	2.4.3. Gestion de la sécurité de l'information	Un référentiel est requis pour évaluer les risques liés au système d'information utilisé et les qualifier.
	2.4.4. Conservation d'informations	Le DID ne comporte pas de données personnelles, il fait uniquement référence à des revendications sur de telles données qui peuvent être prouvées par le porteur du DID. Si des données personnelles sont sauvegardées sur la *blockchain* , s'appuyer sur les recommandations de la CNIL en matière d'exigence.
	2.4.5. Installations et personnel	Les accès du personnel aux installations doivent être authentifiés, autorisés et tracés.
	2.4.6. Contrôles techniques	Les dispositifs personnels doivent comporter les moyens de sécurité matérielle pour protéger les secrets contre de possibles attaques physiques, et contre toute forme de divulgation. Les canaux de communication doivent être sécurisés et confidentiels. La sécurité de l'ensemble des éléments doit pouvoir être maintenue tout au long du cycle de vie.
	2.4.7. Conformité et audit	Les audits doivent être effectués par des organismes indépendants. La *blockchain* offre le moyen de permettre l'audit du *ledger* en permanence et par construction.

Références

[1] Roger WattenHoffer, « The science of blockchain », *Published by Createspace Independent Publishing Platform*, Jan 2016, ISBN : 978-1-5227-5183-0, *en ligne*, https://dl.acm.org/doi/book/10.5555/300270

[2] Journal officiel, Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse, *JORF n°0101 du 29 avril 2016, texte n° 16*, *Legifrance*, *en ligne*, https://www.legifrance.gouv.fr/eli/ordonnance/2016/4/28/FCPT1608300R/jo/texte

[3] Andrew Tanenbaum et David Wetheral, « Réseaux », 5ème édition, *Eyrolles*, ISBN : 978-2-7440-7521-6, *en ligne*, https://www.pearson.ch/download/media/9782744075216_SP_01.pdf

[4] « BitTorrent (BTT) White Paper », *Bitorrent Fundation v0.8.7 Working draft*, Feb 2019, *en ligne*, https://www.bittorrent.com/btt/btt-docs/BitTorrent_Token_Whitepaper.pdf

[5] Vitalik Buterin and Virgil Griffith, « Casper the Friendly Finality Gadget », *arXiv:1710.09437v4 [cs.CR],* 22 Jan 2019, *en ligne*, https://arxiv.org/pdf/1710.09437.pdf

[6] Intel Corporation, « PoET 1.0 specifications », Sawtooth v1.2.4, 2015-2017, *en ligne*, https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html

[7] Péter Szilágyi, « EIP 225: Clique proof-of-authority consensus protocol », *Ethereum Improvement Proposals*, Mar 2017, *en ligne*, https://eips.ethereum.org/EIPS/eip-225

[8] The original POA Whitepaper, « Proof of Authority, AuthorityRound (AuRa) », *edit on GitHub*, Oct 2017, *en ligne*, https://hackmd.io/@F67-rdJCQ0yHlzTN8AoRfw/HkV8Vw7

[9] CNIL, « Le règlement général sur la protection des données - RGPD », mai 2018, *en ligne*, https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[10] ANSSI, « Le référentiel Général de Sécurité », *en ligne*, https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

[11] Journal officiel, Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, version consolidée au 14 février 2020, *Legifrance*, *en ligne*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411

[12] Code des postes et des communications électroniques, version consolidée au 1 janvier 2020, *Legifrance*, *en ligne*, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987

[13] Journal officiel de l'Union européenne, « identification électronique et services de confiance pour les transactions électroniques au sein du marché intérieur, abrogeant la directive 1999/93/CE », juillet 2014, *Règlement (UE) No 910/2014 du parlement européen et du conseil*, *en ligne*, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910

[14] ANSSI, « Le règlement eIDAS », Référentiel documentaire lié au règlement eIDAS, *en ligne*, https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

[15] Journal officiel, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, version consolidée au 14 février 2020, *Legifrance*, *en ligne*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

[16] Journal officiel, « Décret n° 2017-676 du 28 avril 2017 relatif à l'autoconsommation d'électricité et modifiant les articles D. 314-15 et D. 314-23 à D. 314-25 du code de l'énergie », JORF n°0102 du 30 avril 2017, texte n° 6, *Legifrance*, *en ligne*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034517272

[17] Commission européenne, « favoriser la libre circulation des citoyens et des entreprises en simplifiant l'acceptation de certains documents publics dans l'Union européenne, et modifiant le règlement (UE) n° 1024/2012 », avril 2013, *Règlement du parlement européen et du conseil*, *en ligne*, http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2013/0228/COM_COM(2013)0228_FR.pdf

[18] Journal officiel de l'Union européenne, « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation », juin 2019, *Règlement (UE) 2019/1157 du parlement européen et du conseil*, *en ligne*, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R1157

[19] Elise Guilhaudis, « Comprendre la *blockchain* à travers l'étude d'un cas d'usage : le covoiturage, blockcar », Livre Blanc, Numetik Avocats, , *en ligne*, https://www.numetik-avocats.fr/wp-content/uploads/2018/05/NUMETIK-AVOCATS-Livre-blanc-Blockchain.pdf

[20] Christine Hennebert, « La blockchain, chef d'orchestre des objets connectés », *Industrie et Technologies, Cahier Technique n°1019*, avril 2019.

[21] Dirk van Bokkem , Rico Hageman, Gijs Koning, Luat Nguyen et Naqib Zarin, « Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology », *arXiv: 1904.12816v1,* Apr 2019, *en ligne*, https://arxiv.org/pdf/1904.12816.pdf

[22] Christopher Allen, « Forging self-sovereign identities in the age of the blockchain », conférence Rebooting the Web of Trust, Nov 2018, *en ligne,* https://bitcoin.fr/christopher-allen-blockchain-et-identite-video/

[23] World Economic Forum, « A blue print for digital identity », *An Industry Project of the Financial Services Community, prepared in collaboration with Deloitte*, Aug 2016, *en ligne*, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[24] W3C working draft, « Decentralized Identifiers (DIDs) v1.0 », *w3.org*, Nov 2019, *en ligne*, https://www.w3.org/TR/did-core/

[25] W3C working draft, « Verifiable Credentials Data Model 1.0 », *w3.org*, Dec 2019, *en ligne*, https://www.w3.org/TR/vc-data-model/

[26] The European union blockchain observatory and forum, « Blockchain and digital identity », *thematic report v1.0*, May 2019, *en ligne*, https://www.eublockchainforum.eu/reports

[27] The European union blockchain observatory and forum, « Blockchain and the GDPR », *thematic report v1.0*, Oct 2018, *en ligne*, https://www.eublockchainforum.eu/reports

[28] Guy Zyskind, Oz Nathan, et al., « Decentralizing privacy: Using blockchain to protect personal data », In *IEEE Security and Privacy Workshops (SPW)*, 2015, pages 180–184.

[29] Sarah Azouvi, Mustafa Al-Bassam et Sarah Meiklejohn, « Who am i? Secure identity registration on distributed ledgers », *In Data Privacy Management, Cryptocurrencies and Blockchain Technology*, *Springer*, 2017, pages 373– 389.

[30] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya et Christoph Meinel, « A Survey on Essential Components of a Self-Sovereign Identity », *axXiv: 1807.06346v1*, Jul 2018, *en ligne*, https://arxiv.org/pdf/1807.06346.pdf

[31] Sovrin, « A protocol and token for self-sovereign identity and decentralized trust », January 2018, *en ligne*, https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[32] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, Michael Sena, « uPort: a platform for self-sovereign identity », white paper

[33] Makoto Takemiya and Bohdan Vanieiev, « Sora Identity: Secure, Digital Identity on the Blockchain », 2018 42nd IEEE International Conference on Computer Software & Applications, DOI: 10.1109/COMPSAC.2018.10299.

[34] Blockstack, « Blockstack Technical Whitepaper v 2.0 », May 2019, *en ligne*, https://blockstack.org/whitepaper.pdf

[35] ShoCard inc., « Identity Management Verified Using the Blockchain », *Whitepaper*, 2017, *en ligne*, http://shocard.com/wp-content/uploads/2018/01/ShoCard-Whitepaper-Dec13-2.pdf

[36] digi-ID, https://www.digi-id.io/

[37] Hugh Morris, « To be, to have, to know, Smart Ledgers & Identity Authentication », *Technical report from Cardano foundation*, Feb 2019, *en ligne*, https://www.longfinance.net/media/documents/To_Be_To_Have_To_Know_Smart_Ledgers__Identity_Authentication.pdf

[38] Bob Reid et Bob Witteman, « EverID », *Whitepaper*, May 2018, *en ligne*, https://coinosophy.files.wordpress.com/2018/05/everid-whitepaper.pdf
[39] LifeID, « An open-source, blockchain-based platform for self-sovereign identity », LifeID Technical Report, Mar 2018, *en ligne*, https://lifeid.io/whitepaper.pdf
[40] Loïc Lesavre, Priam Varin, Peter Mell, Michael Davidson et James Shook, « A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems », *NIST cybersecurity whitepaper, Computer Security Division Information Technology Laboratory,* Jan 2020, *en ligne*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf
[41] A. Buldas, R. Laanoja, and A. Truu, « Efficient quantum-immune keyless signatures with identity », *IACR Cryptology ePrint Archive*, n°321, 2014, *en ligne*, https://eprint.iacr.org/2014/321.pdf
[42] Paul Dunphy et Fabien A. P. Petitcolas , « A First Look at Identity Management Schemes on the Blockchain », *In IEEE Security & Privacy*, volume 16, issue 4, Aug 2018, *en ligne*, https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf
[43] Kim Cameron, « The law of identity », 2005, *en ligne*, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
[44] Goodell and Aste, « A Decentralized Digital Identity Architecture », *In Frontiers in Blockchain*, volume 2, article 17, Nov 2019, *en ligne*, https://www.frontiersin.org/articles/10.3389/fbloc.2019.00017/full
[45] Blockchain Bundesverband, « Self-Sovereign Identity, A position paper on blockchain enabled identity and the road », Oct 2018, *en ligne*, https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf
[46] eIDAS, Règlement d'exécution (UE) 2015/1502 de la commission, 8 septembre 2015, , *en ligne*, http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502&from=FR
[47] ANSSI, « Services d'horodatage électronique qualifiés, Critères d'évaluation de la conformité au règlement eIDAS », Version 1.1 du 3 janvier 2017, *en ligne*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf
[48] ANSSI, « Services d'horodatage électronique qualifiés, Critères d'évaluation de la conformité au règlement eIDAS », Version 1.1 du 3 janvier 2017, *en ligne*, https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf
[49] *ISO/IEC 7498-1:1994, Open Systems Interconnection – Basic Reference Model: The Basic Model*
[50] eIDAS supported Self-Sovereign Identity, *en ligne*, https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf
[51] Alicem, la première solution d'identité numérique régalienne sécurisée, *en ligne*, https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee
[52] ISO/IEC 18013-5 *Personal identification — ISO-compliant driving licence — Part 5:Mobile driving licence (mDL) application*
[53] Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cedric Lauradoux, Daniel Le Metayer, Vincent Roca « DESIRE: A Third Way for a European Exposure Notification System », PRIVATICS Team, Inria, France, May 2020, https://hal.inria.fr/hal-02568730/document
[54] K. Benyekhlef et P. Trudel. (eds.), « *Etat de droit et virtualité »,* Thémis, pages 157-222, *en ligne*, http://www.crid.be/pdf/public/6050.pdf
[55] C. Terwangne, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ? » Dans Le droit à l'oubli numérique : données normatives - approche comparée, 2015, pages 23-50, Création Information Communication, Larcier, *en ligne*, http://www.crid.be/pdf/public/7684.pdf