“ Blockchain et Digital ID Wallet : vers une identité européenne décentralisée ? ”

Pauline Elie, Thibault Langlois-Berthelot, Seghier Neil

Les Temps Numériques est une série d'ateliers scientifiques à destination des chercheurs en sciences sociales (philosophie, droit, sciences politiques, sociologie) et des professionnels du numérique. La ligne éditoriale se propose d'articuler la contradiction de deux temps singuliers que représentent celui des sciences sociales, et celui de la création numérique. Les objectifs sont d'une part, de créer des synergies scientifiques entre chercheurs et professionnels, puis d'autre part, de favoriser une visibilité scientifique sur des thématiques émergentes.

Atelier n°2

« *Blockchain et Digital ID Wallet : vers une identité européenne décentralisée ?* »

Document scientifique issu de travaux préalables[1]

*

Auteurs : Thibault Langlois-Berthelot, Pauline ELIE, SEGHIER Neil

[1] Thibault Langlois-Berthelot. Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés. *« Blockchain et Cryptos / 60 experts vous expliquent tout »*, IS EDITION, pp.516, juillet 2022, Wallcrypt, 978-2-37-692-343-5. ⟨hal-03384875⟩

❖ Intérêt scientifique

La Commission européenne entend introduire à la fin de l'année 2022 un portefeuille européen d'identité numérique par la révision du règlement eIDAS datant de 2014. Facultatif pour les citoyens, mais applicable directement pas les États d'ici à 2024, il permettra par des protocoles communs aux Etats membres d'octroyer des documents officiels (dits « *attributs authentiques* ») intégrés à ce portefeuille, tels que le permis de conduire ou encore les diplômes universitaires ou professionnels. De manière inédite, ce portefeuille numérique d'identité pourra être techniquement fourni par des prestataires de service. En effet, le règlement eIDAS V2 ouvre ces protocoles aux acteurs privés et non plus seulement étatiques ou publics. Ces acteurs privés pourront dès lors proposer des registres horodatés et interopérables fondés sur la technologie blockchain qui, en tant que registres certifiés, bénéficieront d'une présomption de fiabilité.

Si ce portefeuille promet de simplifier les démarches administratives, fiscales ou transfrontalières en vertu des principes de protection des données (RGPD), son caractère centralisé en 36 nœuds regroupant de nombreuses données personnelles interroge. En effet, la première blockchain fondée en 2008 par un auteur non-identifié (« Satoshi Nakamoto ») cherchait à décentraliser la validation des transactions financières entre un maximum d'acteurs pour optimiser leur fiabilité, en limitant toute altération, rejetée par le consensus. En outre, cette première chaîne de blocs visait à préserver l'anonymat de ses acteurs, sans identification de la personne, au détriment parfois de la légalité des transactions.

Ainsi, comment comprendre la volonté de l'autorité européenne par la révision du règlement eIDAS de proposer un portefeuille d'identité numérique fondé sur une blockchain ? En quoi cette nouvelle forme d'identification basée sur une chaîne de blocs administrée par la puissance publique pourrait-elle être décentralisée, et dans quelle mesure diffère-t-elle d'un registre d'état civil ? Si les blockchains sont corruptibles malgré le design de leur infrastructure décentralisée, quels risques et quels avantages comportent ce portefeuille européen d'identité pour la personne ?

❖ Organisation

L'Atelier se tiendra **vendredi 6 mai, à 16h30, à l'EHESS, à la Fondation Maison des sciences de l'homme, au 1er étage, 54 boulevard Raspail,** 75 006 Paris. Par la suite, intervenants et invités pourront se restaurer autour d'un cocktail organisé dans le jardin de l'Ecole de 19h à 21h, pouvant se prolonger dans les cafés et restaurants attenants.

- **Site internet : www.lestempsnum.hypotheses.org**
- **Lien pour l'atelier en distanciel : https://webinaire.ehess.fr/b/mal-ake-wnl**

❖ Déroulé de la table-ronde 16h45-19h00

- 10 min de présentation du centre Georg Simmel et des doctorants Pauline Elie (EHESS/ Georg Simmel) et Thibault Langlois-Berthelot (EHESS/Georg Simmel) et leur nouvelle recrue, Neil Seghier (pré-doctorant, EHESS)
- 15 min de présentation de **Antonio Casilli (sociologue,Télécom Paris/EHESS/CNRS)**
- 15 min de présentation de **Matthieu Quiniou (avocat, Paris VIII, UNESCO ITEN)**
- 15 min de présentation de **Primavera de Filippi (juriste, chercheuse, CNRS, Harvard)**
- 15 min de présentation de **Louis Margot-Duclot (entrepreneur blockchain, 97 SAS)**
- 30 min de discussion lancée à partir des questions ci-après rédigées
- 10 min de questions avec la salle

Cocktail à partir de **19h** : **jardin de l'EHESS**, au 54 boulevard Raspail, 75006 Paris

***

❖ Petit glossaire[1] généraliste sur la blockchain

- **Blockchain ou chaîne de blocs**[2] **:** Selon le dictionnaire *Le Robert*, la blockchain désigne un « *mode de stockage et de transmission de données sous forme de blocs liés les uns aux autres et protégés contre toute modification* », et, par extension, la « *base de données contenant l'historique des échanges par blockchain*[3] » La chaîne de blocs permet en effet de valider divers types de transactions actuellement en plein développement : cryptomonnaies, smart contracts, NFTs, etc. Ces blocs enchaînés successivement et par là-même horodatés sont ajoutés par des « mineurs » (i.e. des personnes physiques ou morale équipées d'une forte puissance informatique de calcul), qui enregistrent ces « preuves de travail » (*proof of work*), c'est-à-dire, une copie de la plus longue chaîne possible de blocs[4]. Les mineurs constituent ce faisant des nœuds du réseau et comparent par validations successives avec les autres mineurs la chaîne de blocs, créant ainsi un consensus autour de leur registre/*ledge*r/chaîne de blocs. Comme voulu par son mystérieux créateur Satoshi Nakamoto et promoteur de la monnaie numérique *Bitcoin* suite à la crise des *subprimes* de 2008 : plus les nœuds et les mineurs sont nombreux, plus la chaîne de blocs ainsi gérée de manière décentralisée par l'enregistrement de chacun est fiable, diminuant dès lors son risque d'altération ou de corruption.

  Or, il existe depuis 2008 divers types de blockchains : « à permission », « sans permission », publique ou privée, en fonction de l'accès donné à la chaîne de blocs et au nombre de mineurs ou de nœuds sur le réseau. Par exemple, les chaînes de blocs resserrées sur quelques nœuds seulement sont plus centralisées mais moins énergivores. La CNIL distingue notamment trois types d'acteurs[5] de la blockchain : les « *accédants* » (qui disposent d'un droit de lecture et d'obtention d'une copie de la chaîne), les « *participants* », (au droit d'écriture, tel la proposition d'une transaction soumise à validation) ; et les « *mineurs* » (qui jouissent du droit de validation de la transaction en créant les blocs « acceptés » par la communauté)**.**
- **Bitcoin :** *« Version purement pair à pair de la monnaie électronique »* qui permet *« d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière*[6] *»*. Le bitcoin est ainsi la première blockchain décrite et popularisée dans l'article *« Bitcoin : un système de monnaie électronique en pair-à-pair*[7] *»*, publié sous le pseudonyme jusqu'ici jamais levé de Satoshi Nakamoto en 2008. En référence à son ou ses créateurs, le bitcoin (au cours présentement équivalent peu ou prou à 40 000 euros) est divisé en 100 millions de « satoshis », sa plus petite unité de mesure, qui lui confère une grande divisibilité comparée à d'autres monnaies fiduciaires. À compter de sa création, de nombreuses autres cryptomonnaies ou crypto-actifs que le Bitcoin ont été créés.
- ***Smart contract* ou contrat intelligent** *: « Un ensemble de fonctions définies par une séquence d'instructions inscrite sur une blockchain. Cette notion attribuée à Nick Szabo trouve ses origines dans le mouvement des cypherpunks et vise à faire la synthèse entre l'informatique*

---

[1] Sans ordre alphabétique par volonté didactique

[2] Article I. Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), *JORF* n°0121 du 23 mai 2017, texte n° 20. Consulté en ligne le 15 avril 2022 et disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034795042

[3] Dictionnaire *Le Robert* [en ligne],entrée « Blockchain ». Consulté le 15 avril 2022 et disponible sur : https://dictionnaire.lerobert.com/definition/blockchain

[4] Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », bitcoin.org *[en ligne],* 31 octobre 2008, 9 p. Consulté en ligne le 12 avril 2022 et disponible sur : https://bitcoin.org/fr/
« *The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.* »

[5] CNIL, Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?, CNIL.fr *[en ligne],* 24 septembre 2018. Consulté en ligne le 12 avril 2022 et disponible sur : https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

[6] Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », bitcoin.org *[en ligne],* 31 octobre 2008, 9 p. Consulté en ligne le 12 avril 2022 et disponible sur : https://bitcoin.org/fr/

[7] ibid.

et le droit des contrats notamment grâce à des dispositifs cryptographiques. […] Les contrats intelligents permettent notamment de créer des tokens, de réaliser des ICO, des DAO ou encore de créer des dApp[8] ».

- ***Token* ou jeton :** « *Un token est un actif numérique émis et échangeable sur une blockchain […] Les tokens sont au coeur du modèle des ICO (Initial Coin Offerings), ces levées de fonds en cryptomonnaies (lire notre article. Techniquement, un token est créé par un smart contract, le plus souvent sur la blockchain Ethereum*[9] ».
- **Tokenisation :** *« Désigne la création d'une nouvelle catégorie de jetons dans une blockchain pour déployer une économie propre à un écosystème. La tokenisation est souvent conçue de manière à créer des mesures incitatives pour les contributeurs et usagers de l'écosystème*[10] ». Par exemple, selon le protocole Bitcoin, les mineurs reçoivent des bitcoins pour inciter le réseau à diversifier ses nœuds et donc assurer une plus grande fiabilité.
- ***dApp* (Decentralized Application) :** « *Un programme avec plusieurs smart contracts fonctionnant sur une blockchain et généralement une interface utilisateur. Parmi les dApps qui ont le plus fait parler d'elles, on peut citer La'Zooz - un Uber décentralisé, OpenBazaar - une place de marché, Lighthouse - une plateforme de financement participatif.*[11]»
- ***NFT* (*non-fungible token)* ou JNF (jeton non-fongible)** : Unité de valeur qui n'est pas interchangeable avec d'autres, au contraire de la monnaie ou des cryptomonnaies. Il s'agit d'un certificat numérique enregistré dans une blockchain authentifiant un bien, une œuvre, matériel ou virtuel[12].
- ***Proof of work* ou preuve de travail :** Notion définie par l'article fondateur de Satoshi Nakamoto en 2008 qui désigne le « *système de validation de blocs par consensus fonctionnant avec la force brute de calcul, aléatoire et itérative et attribuant les cryptoactifs en fonction de la puissance de calcul mise en disposition. La preuve de travail est, notamment, le mode de consensus de la blockchain Bitcoin. Ce mode de consensus a été critiqué pour sa consommation d'énergie.*[13] »
- ***Proof of stake* ou preuve d'enjeu :** Notion introduite par Sunny King et Scott Nadal en 2012[14] pour remédier à la consommation d'énergie de la preuve de travail, prônée notamment par le cofondateur de la blockchain Ethereum, Vitalik Buterin[15]. Il s'agit d'un **«** *système de consensus alternatif à la preuve de travail qui prévoit le droit de créer le prochain bloc à un validateur actif sur le réseau ayant mis en dépôt des unités de la crypto-monnaie de cette blockchain. Les consensus à preuve d'enjeu s'inspirent de la théorie des jeux pour fonctionner.*[16] » S'il est moins energivore, ce système de validation de la blockchain repose pourtant sur un biais de possession de crypto-actifs qui induit une certaine monopolisation et un manque de distribution.
- ***Zero knowledge proof* ou preuve à divulgation nulle de connaissance :** Protocole de cryptage selon lequel un bloc de base est utilisé pour l'identification ou l'authentification : un « fournisseur de preuve » démontre mathématiquement au « vérificateur » la véracité d'une

---

[8] Matthieu Quiniou, Christophe Debonneuil, *Glossaire blockchain*, UNESCO, Paris : Les Editions de l'immatériel, 60 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

[9] Clément Jeanneau, Qu'est-ce qu'un token ?, blockchainfrance.net *[en ligne]*, 22 mai 2018. Consulté le 12 avril 2022 et disponible sur : https://blockchainfrance.net/2018/05/22/comprendre-les-tokens/

[10] Matthieu Quiniou, Christophe Debonneuil, *Glossaire blockchain*, UNESCO, Paris : Les Editions de l'immatériel, 60 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

[11] ibid.

[12] Aurore Sauviat, Sophie Tribondeau, Les « NFT » : petit guide pour les néophytes, village-justice.com *[en ligne]*, 28 février 2022. Consulté en ligne le 12 avril 2022 et disponible sur : https://www.village-justice.com/articles/les-nft-petit-guide-pour-neophytes,41688.html

[13] Matthieu Quiniou, Christophe Debonneuil, *Glossaire blockchain*, UNESCO, Paris : Les Editions de l'immatériel, 60 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

[14] Sunny King, Scott Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [en ligne], 19 août 2012. Consulté le 12 avril 2022 et disponible sur : https://decred.org/research/king2012.pdf

[15] Yvonne Lau, Ethereum founder Vitalik Buterin says long-awaited shift to 'proof-of-stake' could solve environmental woes, *Fortune*, 27 mai 2021. Consulté en ligne le 13 avril et disponible sur : https://fortune.com/2021/05/27/ethereum-founder-vitalik-buterin-proof-of-stake-environment-carbon/ « *The Ethereum Foundation wrote in its blog that if the switch to POS is successful, it could reduce Ethereum's energy use by up to 99.95%.* »

[16] Matthieu Quiniou, Christophe Debonneuil, *Glossaire blockchain*, UNESCO, Paris : Les Editions de l'immatériel, 60 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

proposition sans pourtant donner d'autres informations, par exemple sous la forme de défi/ réponse.

- **ICO (*Initial Coin Offering*) ou première émission de jetons :** « *L'émission de crypto-actifs pour une acquisition par le grand public ou des investisseurs agréés en contrepartie de devises, ou plus généralement d'autres crypto-monnaies. Les contrats intelligents permettent d'automatiser la réalisation des ICO en procédant à cette opération sur une blockchain préexistante.*[17] »
- **DAO (*Decentralized Autonomous Organisation*) ou organisation autonome décentralisée :** « *Le terme DAO désigne un système d'organisation autonome et décentralisé dont les règles de fonctionnement et de participation sont prévues par un smart contract inscrit dans une blockchain*[18] ». La plus célèbre est Ethereum.
- **Plantoid :** Promu par Primavera de Filippi, juriste et chercheuse au CNRS et à Harvard, le plantoid[19] est un robot fait pour ressembler, agir, croître et se reproduire comme une plante. Concrètement des humains sont invités à lui verser 2 bitcoins, jusqu'à ce qu'un *smart contract* programmé dans le plantoid lance un appel d'offres automatisé pour trouver un artiste fabriquant un autre spécimen, intégrant le code source du premier.
- **Gouvernance :** Désigne les **«** *méthodes de décision et de mise en œuvre des choix organisationnels. Par principe dans les blockchains, la prise de décision est, comme l'architecture du réseau, décentralisée. L'administration de la blockchain est répartie entre les nœuds du réseau et les règles de prise de décisions bien que différentes d'une blockchain à l'autre reposent sur des mesures d'incitation au maintien de l'intégrité des données et à l'amélioration des composantes techniques et des méthodes de cryptage. L'algorithme de consensus est une composante essentielle de la gouvernance d'une blockchain*[20] **»**
- **Blockchain publique :** Forme historique de la blockchain sur laquelle sont fondés Bitcoin, Ethereum et de nombreuses autres cryptomonnaies. La chaîne de blocs publique confère à tous indistinctement la possibilité d'y participer en conservant son anonymat et ainsi une partie de l'autorité sur le réseau en constituant de nouveaux nœuds. Si cette ouverture permet d'accroître le nombre de participants à la blockchain et donc de renforcer sa fiabilité entre les pairs, elle laisse également possible les opérations frauduleuses (blanchiment d'argent, financements occultes, etc.). Selon la théorie des jeux à son fonctionnement, le bon comportement de ce consensus récompense les acteurs sains et honnêtes et pénalisent les acteurs coûteux.
- **Blockchain privée :** Contrairement à la blockchain publique, elle est administrée par un seul ou plusieurs acteur(s) qui a ou ont autorité sur le réseau et ses nœuds à l'origine du minage de la blockchain. La plupart du temps les blockchains privées sont des blockchains à permission.
- **Blockchain « à permission » ou ou « sans permission » :** Lorsqu'elle n'est pas publique, la blockchain peut être administrée ou « *à permission* ». Concrètement « *le fonctionnement de la blockchain est organisé et encadré par un administrateur, qui détient la majorité de la puissance de calcul disponible sur le réseau, en consortium (plusieurs acteurs s'entendent pour contrôler le réseau) ou privée (un seul acteur a autorité sur le réseau)*[21] ». Une autorité publique ou privée peut donc resserrer les nœuds du réseau et re-centraliser les transactions en les contrôlant et en les rectifiant. La levée de l'anonymat et l'identification est donc souvent requise pour obtenir une autorisation de lecture, de proposition ou de validation de blockchain à permission. *A contrario*, une blockchain sans permission ne nécessite pas de connaître l'identité de celles et ceux qui

[17] ibid.

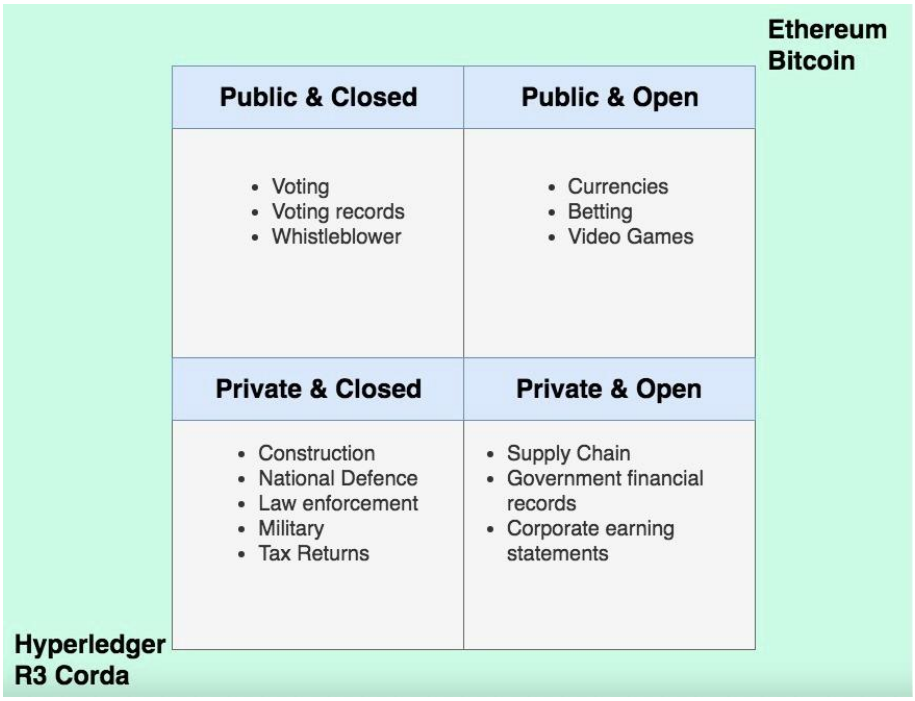
[18] ibid.

[19] Primavera de Filippi. Plantoïde : une forme de vie fondée sur la blockchainGenevieve Vidal; Olga Kisseleva. Double Vie d'Artistes, 2020. Consulté en ligne le 12 avril 2022 et disponible sur : https://hal.archives-ouvertes.fr/hal-03098591/document
Voir également : https://plantoid.org/#history

[20] Matthieu Quiniou, Christophe Debonneuil, *Glossaire blockchain*, UNESCO, Paris : Les Editions de l'immatériel, 60 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf

[21] Caroline Martin-Forissier, Blockchain et RGPD, une union impossible ?, LINC, CNIL. 24 août 2017. Consulté en ligne le 11 avril 2022 et disponible sur : https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0

accèdent à sa lecture et son écriture, voire à sa validation par le minage sous réserve d'une forte capacité technique de calcul.



Source : Auteur inconnu, Blockchain privée et blockchain publique : différences, *lecryptopolitain.fr [en ligne]*, 17 novembre 2019. Disponible sur : https://www.lecryptopolitain.fr/blockchain-privee-et-blockchain-publique-differences/

- **Intervention humaine/recours vs. *smart contract* :**

  En se fondant sur l'article 22 al. 3 du RGPD[22] qui impose une intervention humaine si une décision est entièrement automatisée, la CNIL propose de limiter « *l'utilisation des données dans les smart contracts, simplement en le prévoyant en amont dans le programme*[23] ». Ainsi face au caractère automatisé du *smart contract* une possibilité de recours dans sa conception devrait permettre à la personne concernée d' « *obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision après que le smart contract ait été exécuté […], et ceci indépendamment de ce qui est inscrit dans la Blockchain.*[24] »

❖ Focus chronologique et textes de référence (en liens hypertextes)

➢ Règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur « eIDAS » (entré en vigueur le 17 septembre 2014 et applicable depuis 2018)[25]

[22] Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 4 mai 2016, *JOUE*. Consulté en ligne le 11 avril 2022 et disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

[23] CNIL, *Premiers éléments d'analyse de la CNIL. Blockchain. Cnil.fr [en ligne]*, septembre 2018, p. 10. Consulté en ligne le 14 avril 2022 et disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

[24] ibid.

[25] Le règlement eIDAS est applicable depuis le 1er juillet 2016 pour la majeure partie de ses dispositions. La reconnaissance mutuelle des moyens d'identification électronique est obligatoire depuis le 29 septembre 2018.
Commission européenne, Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE*, 28 août 2014. Consulté en ligne le 11 avril 2022 et disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=hr

- **Objectif**

Abrogeant la directive 1999/93/CE[26], ce règlement directement applicable par les Etats membres vise à construire un environnement interopérable pour cinq services de confiance numériques : (i) la signature électronique pour les personnes physiques, (ii) les cachets électroniques pour les personnes morales, (iii) l'horodatage électronique, (iv) l'authentification en ligne de sites internet et enfin (v) les services d'envoi recommandé électronique.

- **Constats et limites d'eIDAS**

L'application de ce règlement est confrontée à certaines limites depuis son entrée en vigueur. Tout d'abord, seulement 60% de la population de l'Union européenne, soit quatorze États membres, sont en mesure d'utiliser pleinement leurs systèmes d'identités numériques nationaux de manière transfrontalière. En effet, les autres États membres ne disposent pas de nœuds eIDAS[27] dont les fonctions d'envoi sont pleinement opérationnelles. Ainsi, seuls 14 % des principaux prestataires de services publics dans l'ensemble des États membres autorisent l'authentification transfrontalière au moyen d'un système d'identité électronique.

Selon le rapport publié par le ministère français de l'Intérieur en 2020 « *[…] le cadre eIDAS est trop limité pour intégrer la blockchain. Destiné à encadrer la fourniture d'un ensemble d'attributs déterminés (l'ensemble minimum d'attributs obligatoires qui identifient la personne, ou « identité pivot ») définis dans l'acte d'exécution 2015/1501, eIDAS ne permet : (i) ni la minimisation des données et la divulgation sélective d'attributs, (ii) ni l'utilisation de références anonymisées comme par exemple les assertions vérifiables certifiées (Verifiable Credentials [VCs]) basées sur le modèle de données du W3C, (iii) ni la communication d'attributs connexes d'identification, autres que les « données pivot » (qui, renvoyant à l'identité juridique, servent à identifier la personne), (iv) ni des services en ligne offerts par le privé, (le Règlement traite uniquement de l'action des administrations publiques), (v) ni l'hébergement des données personnelles sur un dispositif personnel mobile de façon sécurisée.*[28] »

➢ **Le 10 avril 2018, sur initiative de la Commission européenne, 21 États membres et la Norvège signent une déclaration[29] pour un Partenariat Européen pour la Blockchain (European Blockchain Partnership/EBP) à l'origine d'une blockchain européenne : l'European Blockchain Service Infrastructure (EBSI)**

Depuis 2020, EBSI déploie un réseau consortium de 36 nœuds blockchain à travers l'Europe[30], soutenant des applications centrées sur des cas d'utilisations spécifiques. Chaque nœud est composé de trois couches : « *(1) La couche d'infrastructure fournit des capacités génériques et une connectivité aux réseaux Blockchain ; (2) La chaîne et la couche de stockage englobent à la fois la blockchain et les protocoles de stockage hors chaîne actuellement pris en charge par EBSI et ; (3) Les services de base sont un ensemble d'interfaces standardisées (API)*

[26] Directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques, 13 décembre 1999, abrogée par le règlement n° 910/2014. Consulté en ligne le 11 avril 2022 et disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31999L0093&from=FR

[27] Ces nœuds représentent des serveurs standardisés qui fonctionnent avec un protocole commun maintenu par le bras droit technique de la Commission européenne : le « Connecting Europe Facility ».

[28] France, Ministère de l'Intérieur, Blockchain et identification numérique. Restitution des ateliers du groupe de travail (BCID), octobre 2020. Consulté en ligne le 11 avril 2022 et disponible sur : https://www.vie-publique.fr/sites/default/files/rapport/pdf/280103.pdf

[29] Commission européenne, *Declaration on European partnership on blockchain*, 10 avril 2018, 8 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/newsroom/dae/redirection/document/50954

[30] EBSI, *What is EBSI?*, *ec.europa.eu [en ligne]*, date inconnue. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/EBSI

qui permettent à des tiers de développer des applications et d'assurer le respect des principes directeurs définis et approuvés par l'EBP.[31] »

Première infrastructure[32] blockchain à l'échelle de l'Espace Economique Européen, pilotée par le secteur public, l'EBSI, réunissant à présent 29 États, est conçue comme un écosystème favorable au marché, basé sur des normes ouvertes et un modèle de gouvernance transparent.

En théorie, l'EBSI se développe autour de **cinq principes fondateurs** :

- **Bien commun** : L'administration de l'EBSI doit servir le bien commun et il lui incombe de limiter son utilisation aux services publics et privés qui apportent un bien public net aux citoyens des États membres dans leur ensemble ;
- **Gouvernance** : Le système de gouvernance de l'EBSI garantit que les décisions sont prises par consensus entre les parties prenantes ;
- **Harmonisation** : La gouvernance des EBSI doit encourager et maintenir l'harmonisation des exigences techniques et de l'architecture afin d'éviter la prolifération des protocoles supportés ou des hypothèses architecturales contradictoires ;
- **Source ouverte** : Dans la mesure du possible, le code de base de tous les services et structures EBSI doit être open source afin de permettre un audit et une sécurité maximaux, ainsi qu'une concurrence saine entre les fournisseurs de services, les vendeurs et le secteur privé ;
- **Conformité** à la réglementation européenne : L'EBSI doit non seulement se conformer à l'interprétation actuelle du RGPD[33] et à son perfectionnement continu, mais aussi s'aligner sur le règlement eIDAS et d'autres réglementations.

En pratique, l'EBSI développe **plusieurs cas d'usages** spécifiques dont :

- **L'identité** (mise en œuvre d'un modèle d'identité autonome en Europe, permettant aux utilisateurs de créer et de contrôler leur propre identité au-delà des frontières) ;
- **Les diplômes** (les citoyens obtiennent le contrôle numérique de leurs titres de formation, ce qui réduit considérablement les coûts de vérification et améliore la confiance dans l'authenticité des documents) ;
- **La traçabilité** (créer des pistes d'audit numériques fiables, automatiser les contrôles de conformité et prouver l'intégrité des données) ;
- **Le partage de données** en toute confiance (partage sécurisé de données (telles que les numéros d'identification TVA IOSS et le guichet unique d'importation) entre les autorités douanières et fiscales de l'UE).

➢ Discours du 16 septembre 2020 de la Présidente de la Commission européenne, Ursula von der Leyen, sur l'état de l'identité numérique au sein de l'UE

- Lors de son discours sur l'état de l'Union européenne en 2020, la présidente de la Commission a déclaré : « *Chaque fois qu'une application ou un site web nous propose de créer une nouvelle identité numérique ou de nous connecter facilement via une grande plateforme, nous n'avons aucune idée de ce que deviennent nos données, en réalité. C'est pourquoi la*

[31] EBSI, *EBSI's architecture, ec.europa.eu [en ligne]*, date inconnue. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/EBSI

[32] Pour plus de détails sur l'infrastructure : EBSI, *EBSI Architecture, explained.*, *ec.europa.eu [en ligne]*, 10 juin 2021, 22 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/cefdigital/wiki/download/attachments/113541243/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf?api=v2

[33] Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 4 mai 2016, *JOUE*. Consulté en ligne le 11 avril 2022 et disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Commission proposera une identité électronique européenne sécurisée. Une identité fiable, que tout citoyen pourra utiliser partout en Europe pour n'importe quel usage, comme payer ses impôts ou louer un vélo. Une technologie qui nous permettra de contrôler quelles données nous partageons et l'usage qui pourra en être fait.[34] »

➢ **Lancement d'un processus de consultation en juillet 2020**[35] **puis d'une proposition de révision (« eIDAS-V2 » publiée en juin 2021)**[36] **du règlement eIDAS-V1 daté de 2014.**

- **Adoption du texte**

La version finale du texte devrait être publiée au deuxième trimestre 2022[37].

- **Objectifs**

Son objectif est de passer de 60% d'utilisation actuelle des identités numériques nationales mises en place par *eIDAS-V1*, à 80%[38]. Cet objectif est d'autant plus ambitieux qu'il fait face à un temps d'application très court, d'environ trois ans. Dans une logique d'optimisation de la version en vigueur d'eIDAS, cette récente proposition d'amendement aura pour effet de fournir une nouvelle reconnaissance juridique aux technologies de registres et d'identité décentralisée. De ce fait, les *« attestations électroniques qualifiées d'attributs*[39] » et la technologie blockchain en tant que « *registre électronique*[40] » sont respectivement évoquées dans cette même proposition.

❖ Focus sur plusieurs propositions d'eIDAS-V2

- eIDAS-V2 propose l'ajout de trois nouvelles catégories[41] de services de confiance qualifiés : les services d'archivage électronique[42], la gestion des dispositifs de création de signatures électroniques[43] et de cachets à distance[44], enfin les *registres*

---

[34] Commission européenne, Discours sur l'état de l'Union 2021 de la présidente von der Leyen sur l'état de l'identité numérique au sein de l'UE, Strasbourg, le 15 septembre 2021, 18 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/commission/presscorner/api/files/document/print/fr/speech_20_1655/SPEECH_20_1655_FR.pdf

[35] Commission européenne, Digital identity and trust : Commission launches public consultation on the eIDAS Regulation, *ec.europa.eu [en ligne]*, 24 juillet 2020. Consulté en ligne le 27 mars 2022 et disponible sur : https://digital-strategy.ec.europa.eu/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation

[36] Commission européenne, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021. Consulté en ligne le 11 avril 2022 et disponible sur : https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0023.02/DOC_1&format=PDF

[37] Thibault Langlois-Berthelot. Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés. *Blockchain & Crypto : 50 experts vous expliquent tout*, IS EDITION, A paraître, 50 experts vous expliquent la blockchain, p. 2. Consulté en ligne le 11 avril 2002 et disponible sur : ⟨hal-03384875⟩

[38] « *[…] by 2030, all key public services should be available online […] and 80% citizens should use an eID solution.* »
Commission européenne, Commission proposes a trusted and secure Digital Identity for all Europeans, 3 juin 2021. Consulté en ligne le 11 avril 2022 et disponible sur : https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_2663/IP_21_2663_EN.pdf

[39] La proposition eIDAS-V2 désigne les attestations vérifiables en tant que « *attestation électronique qualifiée d'attributs* » (cons. 27). « *Toute entité qui collecte, crée et délivre des attributs attestés tels que des diplômes, permis et certificats de naissance devrait pouvoir devenir fournisseur d'attestations électroniques d'attributs. Les parties utilisatrices devraient utiliser les attestations électroniques d'attributs comme des équivalents aux attestations sur papier. Par conséquent, une attestation électronique d'attributs ne devrait pas se voir refuser un effet juridique au motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de l'attestation électronique qualifiée d'attributs. À cet effet, il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a un effet juridique équivalent à celui des attestations délivrées légalement sur papier.* »
Ainsi, une attestation électronique qualifiée d'attribut est une « *attestation électronique d'attributs délivrée par un prestataire de services de confiance qualifié* » (art. 1er (3) (i) 45., chargé de vérifier l'authenticité de cet attribut (cons. 30).

[40] La proposition eIDAS-V2 ne nomme ni ne cite la technologie blockchain, mais préfère le terme « *registre électronique* » dans un souci de neutralité technologique. Si cette ambivalence peut faire référence à tous types de registres électroniques qu'ils soient centralisés, décentralisés ou hybrides, il convient d'admettre que la volonté du législateur européen est de permettre une qualification puis une reconnaissance juridique aux technologies blockchains en les incluant dans cette large définition.

[41] Motifs, 1. Contexte de la proposition, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, p. 2.
« *la présente proposition élargit la liste actuelle des services de confiance eIDAS à trois nouveaux services de confiance qualifiés, à savoir la fourniture de services d'archivage électronique, les registres électroniques et la gestion des dispositifs de création de signatures et de cachets électroniques à distance.* »

[42] Section 10, art. 45 octies, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.

[43] Section III, art. 29 bis, ibid.

[44] Section III, art. 39 bis, ibid.

électroniques (y compris blockchain)[45] pouvant conférer des *attestations électroniques d'attributs*[46] a minima définis comme : l'**adresse, l'âge, le sexe, l'état civil, la composition de famille, la nationalité, les diplômes, les titres et certificats du système éducatif et professionnels, les permis et licences, les informations financières et les données des entreprises**[47].

- **Il introduit une présomption de fiabilité et d'authenticité conférée aux registres électroniques dits qualifiés, tels que la blockchain.** *De facto*, « *un registre électronique qualifié bénéficie d'une présomption quant au caractère univoque et à l'authenticité des données qu'il contient, à l'exactitude de la date et de l'heure de ces données et à leur classement chronologique séquentiel dans le registre*[48] ». Donc un registre électronique sera considéré comme qualifié aux conditions[49] suivantes : (i) ledit registre est créé par un ou plusieurs prestataires de services de confiance qualifiés ; (ii) il garantit l'unicité, l'authenticité et l'ordre correct des entrées de données enregistrées ; (iii) il assure l'ordre chronologique séquentiel et l'exactitude de la date et de l'heure correcte des données ; (iv) il enregistre les données de manière à ce que toute modification ultérieure des données soit immédiatement détectable.

- Concernant l'identification électronique (soit l'identité numérique), de nouveaux portefeuilles numériques nommés **« *European Digital Identity Wallets » (EIDW) ou*** en français, ***« portefeuilles européens d'identité numérique[50] » (PEIN)***, devront être proposés puis **mis en place par les États membres d'ici à 2024** (cette obligation leur incombe selon l'applicabilité directe des règlements européens).
    - Plus précisément, ces PEIN seront mis à disposition des **citoyens, des résidents et des entreprises de l'Union européenne** qui souhaitent s'identifier ou fournir la confirmation de certaines informations personnelles[51]. Ils pourront être utilisés pour accéder à des services en ligne et hors-ligne, publics et privés, et de façon **transfrontalière et non limitative** dans tous les États membres de l'UE.

---

[45] Section 11, art. 45 nonies 2., ibid.
Voir cons. 34 ibid. : « *Les registres électroniques combinent les effets de l'horodatage des données à une garantie concernant le créateur des données, à l'instar des processus de signature électronique, et présentent l'avantage supplémentaire de permettre des modèles de gouvernance plus décentralisés adaptés aux coopérations multipartites. Par exemple, ils créent une piste d'audit fiable pour la provenance des matières premières dans les échanges transfrontaliers, soutiennent la protection des droits de propriété intellectuelle, permettent une plus grande adaptabilité des marchés de l'électricité, sont à la base de solutions d'identité autonomes avancées, et soutiennent des services publics plus efficaces et plus transformateurs.* »

[46] Art. 3 pt. 44. ibid.: « *"attestation électronique d'attributs", une attestation sous forme électronique qui permet l'authentification d'attributs;* »
Art. 6 bis 3. (a) ibid. : « *3. Les portefeuilles européens d'identité numérique permettent à l'utilisateur: (a) de demander et d'obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité, d'une manière qui soit transparente pour l'utilisateur et traçable par ce dernier, les données légales nécessaires d'identification personnelle et l'attestation électronique d'attributs pour s'authentifier en ligne et hors ligne en vue d'utiliser des services publics et privés en ligne; »*
Art. 6 bis 4 (a) (3) ibid.*: « En particulier, les portefeuilles européens d'identité numérique: (a) offrent une interface commune : (3) pour la présentation aux parties utilisatrices de données d'identification personnelle, de l'attestation électronique d'attributs ou d'autres données telles que des justificatifs, en mode local ne nécessitant pas d'accès à l'internet pour le portefeuille »*

[47] Annexe VI Liste minimale d'attributs, ibid.
« *Conformément à l'article 45 quinquies, les États membres veillent à prendre les mesures nécessaires pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité des attributs suivants, par rapport à la source authentique pertinente au niveau national ou via des intermédiaires désignés reconnus au niveau national, en conformité avec le droit national ou le droit de l'Union, et lorsque ces attributs sont fondés sur des sources authentiques dans le secteur public: 1.l'adresse ; 2.l'âge ; 3.le sexe ; 4.l'état civil ; 5.la composition de famille ; 6.la nationalité ; 7.les diplômes, titres et certificats du système éducatif ; 8.les diplômes, titres et certificats professionnels ; 9.les permis et licences ; 10.les informations financières et les données des entreprises. »*

[48] Section 11, art. 45 nonies 2., Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.
« Effets juridiques des registres électroniques
« *1. L'effet juridique et la recevabilité d'un registre électronique comme preuve en justice ne peuvent être refusés au seul motif que ce registre se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences applicables aux registres électroniques qualifiés.*
2. Un registre électronique qualifié bénéficie d'une présomption quant au caractère univoque et à l'authenticité des données qu'il contient, à l'exactitude de la date et de l'heure de ces données et à leur classement chronologique séquentiel dans le registre. »

[49] Section 11, art. 45 decies 1., Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.

[50] Art. 3, pt. 42 & Section I, art. 6 bis, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.

[51] Art. 3, pt. 42, Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.
« *"portefeuille européen d'identité numérique", un produit et un service qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 bis; et de créer des signatures et cachets électroniques qualifiés;* »

- La responsabilité de ces portefeuilles d'identité incombera aux États membres[52] et leurs certifications ne seront pas soumises à des processus « *d'examen par les pairs* »[53] comme l'exige actuellement eIDAS-V1. **Un État membre devra fournir une interface commune aux utilisateurs et citoyens afin de permettre une interaction facilitée avec le portefeuille d'identité numérique européen**. À cette fin, un « ***label de confiance*** *du portefeuille d'identité numérique européen*[54] » sera institué. Le PEIN se présente comme une nouvelle alternative[55] pour l'authentification forte du client ou du citoyen[56].
- En matière de protection des données personnelles, l'utilisation des données doit tout d'abord être **sous le contrôle de l'utilisateur** et lui permettre une « ***divulgation sélective***[57] » ou discrétionnaire de **ses attributs d'identité** dont les modalités restent à définir. Les Etats membres qui usent de « *moyens d'identification électronique notifiés*[58] » reconnus mutuellement ou de portefeuilles européens d'identité numérique pour l'authentification des individus doivent fournir une « ***identification univoque***[59] **».** De plus, les **prestataires de services** sont tenus d'une part, de **ne pas combiner les données personnelles du portefeuille avec d'autres données** dont ils disposeraient sur la personne, **et d'autre part, de les séparer d'un point de vue logiciel et physique**[60]**.**

---

[52] Les PEIN doivent être « délivrés » ou « approuvés » par les autres États membres, selon un protocole commun et une administration particulière.
Cons. 23 : « *Une attention particulière devrait être accordée à l'efficacité de la coopération entre les autorités SRI et eIDAS. Lorsque l'organe de contrôle au titre du présent règlement est différent des autorités compétentes désignées au titre de la directive XXXX/XXXX [SRI 2], ces autorités devraient coopérer étroitement, en temps utile, en échangeant les informations pertinentes afin de garantir un contrôle efficace et le respect, par les prestataires de services de confiance, des exigences énoncées dans le présent règlement et dans la directive XXXX/XXXX [SRI 2].* »
Cons. 30 *: « Les attributs fournis par les prestataires de services de confiance qualifiés dans le cadre d'une attestation d'attributs qualifiée devraient faire l'objet d'une vérification par rapport aux sources authentiques, effectuée soit directement par le prestataire de services de confiance qualifié, soit par des intermédiaires désignés reconnus au niveau national conformément au droit national ou au droit de l'Union, aux fins de l'échange sécurisé d'attributs attestés entre les prestataires de services de confiance et les parties utilisatrices. »*
Art. 3, pt. 46, ibid. « *"source authentique", un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient les attributs concernant une personne physique ou morale et qui est considéré comme étant la source première de ces informations ou est reconnu comme authentique en droit national;* »
Art. 18 4., ibid. « *4. Les organes de contrôle et les autorités nationales compétentes désignées en vertu de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2] coopèrent et se prêtent mutuellement assistance afin de veiller à ce que les prestataires de services de confiance respectent les exigences établies dans le présent règlement et dans la directive (UE) XXXX/XXXX [SRI 2]. L'organe de contrôle demande à l'autorité nationale compétente désignée en vertu de la directive (UE) XXXX/XXXX [SRI 2] de mener des actions de surveillance pour vérifier que les prestataires de services de confiance respectent les exigences énoncées dans la directive (UE) XXXX/XXXX [SRI 2], d'exiger des prestataires de services de confiance qu'ils remédient à tout non-respect de ces exigences, de fournir en temps voulu les résultats de toute activité de surveillance ayant trait aux prestataires de services de confiance et d'informer les organes de contrôle des incidents pertinents notifiés conformément à la directive (UE) XXXX/XXXX [SRI 2].* »

[53] Les Etats ont la possibilité de s'appuyer sur la certification pour garantir la conformité au règlement eIDAS-V2 en remplacement du processus d'examen par les pairs (art. 12 bis) « *1. La conformité des schémas d'identification électronique notifiés aux exigences énoncées à l'article 6 bis, à l'article 8 et à l'article 10 peut être certifiée par les organismes publics ou privés désignés par les États membres. 2. L'évaluation par les pairs des schémas d'identification électronique prévue à l'article 12, paragraphe 6, point c), ne s'applique pas aux schémas d'identification électronique ni à une partie de tels schémas qui ont été certifiés conformément au paragraphe 1. Les États membres peuvent utiliser un certificat ou une déclaration de conformité de l'Union délivré(e) conformément à un schéma européen de certification de cybersécurité pertinent établi en application du règlement (UE) 2019/881 afin de démontrer la conformité de ces schémas avec les exigences énoncées à l'article 8, paragraphe 2, relatives aux niveaux de garantie des schémas d'identification électronique ».*
Les PEIN seront évalués par référence à des « *normes et références techniques communes* » et seront donc reconnus de manière équiprobable au sein de l'Union européenne dans le respect du RGPD (cf. Exposé des motifs, 5. Autres éléments, ibid. : « *Cette certification est sans préjudice du RGPD en ce sens que les opérations de traitement de données à caractère personnel liées au portefeuille européen d'identité numérique ne peuvent être certifiées que selon les modalités prévues par les articles 42 et 43 du RGPD.* »)

[54] Section I, art. 6 bis 4. (a) (4), Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021.

[55] Exposé des motifs, 5. Autres éléments, ibid. « *La section 3 présente de nouvelles dispositions relatives au recours transfrontalier au portefeuille européen d'identité numérique, afin que les utilisateurs puissent s'appuyer sur les portefeuilles européens d'identité numérique pour accéder à des services en ligne fournis par des organismes du secteur public et par des prestataires de services privés et nécessitant le recours à une authentification forte des utilisateurs* »
Section I, art. 6 bis 4. (d), ibid. « *4. En particulier, les portefeuilles européens d'identité numérique : […] (d) fournissent un mécanisme permettant de faire en sorte que la partie utilisatrice puisse authentifier l'utilisateur et recevoir des attestations électroniques d'attributs ;* »

[56] Art. 3, pt. 50, ibid. "*authentification forte de l'utilisateur", une authentification reposant sur l'utilisation d'au moins deux éléments qui appartiennent aux catégories 'connaissance de l'utilisateur', 'possession' et 'inhérence' et qui sont indépendants, de manière à ce que la compromission de l'un ne remette pas en question la fiabilité des autres, et qui est conçue de façon à protéger la confidentialité des données d'authentification;* ». Par exemple, un code en mémoire par la personne (« une connaissance de l'utilisateur »), une carte (« une possession »), des données biométriques (« inhérence ») telles l'iris, les empreintes digitales, etc.

[57] Exposé des motifs, 3. Résultats des évaluations ex post, des consultations des partes intéressées et des analyses d'impact, ibid. : « *les mesures sont conçues pour être pleinement conformes à la législation en matière de protection des données. Par exemple, la proposition améliore les possibilités de partage de données et de divulgation discrétionnaire. En utilisant le portefeuille européen d'identité numérique, l'utilisateur pourra exercer un contrôle sur la quantité de données fournies aux parties utilisatrices et être informé des attributs qui seront exigés pour la fourniture d'un service particulier. Les prestataires de services devront informer les États membres de leur intention d'avoir recours à un portefeuille européen d'identité numérique, ce qui permettra aux États membres de contrôler que les demandes des prestataires de services portant sur des ensembles de données confidentielles, par exemple en rapport avec la santé, sont faites dans le respect du droit national.* »
Cons. 29 : « *Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel.* »

[58] Section III, Ar. 12 quater, ibid.

[59] Section II, art. 11 bis, ibid.

[60] Section 9, art. 45 septies, ibid.
En principe, il ne doit pas s'opérer de collecte des données d'utilisation pour ces portefeuilles d'identité : l'émetteur d'un portefeuille ne peut pas collecter les données d'utilisation sauf si elles sont strictement identifiées comme nécessaires au fonctionnement du portefeuille.

- En effet, le PEIN s'imposera aux « ***très grandes plateformes en ligne***[61] » bien que **gratuit et facultatif**[62] pour les citoyens européens. Astreintes au principe de minimisation des données, elles devront traiter seulement des attributs nécessaires à l'accès au service tel que l'âge.
- À l'heure actuelle, si certains principes d'eIDAS-V2 sont formels et inédits, la généralité de **certaines définitions peut laisser place à une certaine ambiguïté d'interprétation**, notamment pour les États membres et les fournisseurs d'identité. De nouvelles modifications dudit texte devraient en principe intervenir avant son **adoption courant 2023** tandis que de nombreux éléments et détails techniques et juridiques demeurent à préciser.
- En définitive, la proposition eIDAS-V2 affirme la nécessité d'« *un processus de* ***coopération étroite et structurée entre la Commission, les États membres et le secteur privé*** [63] ». Pour cela, une « ***boîte à outils*** » permettra de mettre en place une architecture technique qui repose sur des standards et des pratiques communes que les États membres devront respecter. La Commission européenne envisage ainsi de mettre en place des « ***codes de conduite autorégulateurs***[64] » pour faciliter la mise à disposition et l'utilisation des PEIN. Cette boîte à outils devrait être implémentée en septembre 2022[65].

- Par conséquent, si cette proposition est adoptée, **un service en ligne (public ou privé)**[66] **qui recourt à la technologie blockchain pourra être accessible à travers toute l'Union européenne**, dès lors qu'il répond aux exigences du règlement eIDAS (V1 & V2). Par conséquent, la solution d'identité décentralisée déployée par un État membre se verra attribuer l'un des trois niveaux de confiance initialement institués par eIDAS V1[67].

➢ Lancement des premières coopérations stratégiques et multilatérales sur l'identité décentralisée entre certains Etats membres

- En France, le ministère de l'Intérieur a déjà manifesté son intérêt pour le sujet de l'identification par la blockchain, autrement appelée « *identité auto-souveraine* », en témoigne de la publication en octobre 2020 d'un rapport en partenariat avec les entreprises Nanoelec et Thales[68].

---

[61] Les grandes plateformes comme Amazon, Google ou Facebook seront également tenues d'accepter l'utilisation des portefeuilles d'identité numérique de l'UE à la demande de l'utilisateur, par exemple pour prouver son âge.
Cons. 28 : « *[…] Lorsque de très grandes plateformes en ligne au sens de l'article 25, paragraphe 1, du règlement [référence du règlement sur les services numériques] exigent des utilisateurs qu'ils s'authentifient pour accéder à des services en ligne, ces plateformes devraient être tenues d'accepter l'utilisation de portefeuilles européens d'identité numérique à la demande volontaire de l'utilisateur. Les utilisateurs ne devraient pas être tenus d'utiliser le portefeuille pour accéder à des services privés, mais, lorsque l'utilisateur le souhaite, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données. […]* »
Art. 12 ter 3. Ibid. : « *[…] elles acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 bis uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge.* »

[62] Commission européenne, Commission proposes trusted and secure Digital Identity for all Europeans - Questions and Answers, *ec.europa.eu [en ligne]*, 3 juin 2021. Consulté en ligne le 12 avril 2022 et disponible sur : https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664

[63] Cons. 36, ibid. : « *[…] les États membres devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. Le contenu de la boîte à outils devrait continuer à évoluer parallèlement au débat et au processus d'adoption du cadre européen relatif à une identité numérique et tenir compte de leurs résultats.* »

[64] Art. 12 ter 4. et cons. 28, ibid. : « *Des codes de conduite d'autorégulation au niveau de l'Union ("codes de conduite") devraient être élaborés afin de contribuer à une large disponibilité et à une grande facilité d'utilisation des moyens d'identification électronique, y compris les portefeuilles d'identité numérique européens, dans le cadre du présent Règlement. Les codes de conduite devraient faciliter une large acceptation des moyens d'identification électronique, y compris les portefeuilles européens d'identité numérique. Ils devraient être élaborés dans les douze mois suivants l'adoption du présent Règlement.* »

[65] Arthur Olivier, Vers une identité numérique européenne ?, *Toutel'*europe.eu *[en ligne],* 4 juin 2021. Consulté en ligne le 12 avril 2022 et disponible sur : https://www.touteleurope.eu/societe/vers-une-identite-numerique-europeenne/

[66] Et non plus simplement public comme dans la version actuellement en vigueur du règlement eIDAS (V1), qui limite les services d'identification électronique aux seuls services publics.

[67] **Trois niveaux d'assurance** sont spécifiés pour les identités électroniques dans le cadre d'eIDAS, qui font référence au degré de confiance dans l'identité revendiquée d'une personne. Ces niveaux comprennent des critères détaillés permettant aux États membres de comparer leurs moyens d'identification électronique à un point de référence (**faible**, **substantiel** et **élevé**). Les mises en œuvre actuelles de l'identité décentralisée ont pour objectif d'être reconnues avec un niveau d'assurance spécifié comme à minima substantiel et si possible élevé.

[68] France, Ministère de l'Intérieur, Blockchain et identification numérique. Restitution des ateliers du groupe de travail (BCID), *vie-publique.fr [en ligne]*, octobre 2020. Consulté en ligne le 11 avril 2022 et disponible sur : https://www.vie-publique.fr/sites/default/files/rapport/pdf/280103.pdf

- L'identité décentralisée fondée sur la blockchain fait l'objet d'un important soutien hors des frontières hexagonales, comme l'illustre la multiplication des standards et normes internationaux en la matière (*ISO/TC 307*[69], *UIT-T X.1403*[70], etc.)
- L'Allemagne et l'Espagne ont signé un protocole d'accord attestant de leur volonté commune d'échanger sur le domaine de l'identité auto-souveraine d'un point de vue technique, réglementaire et opérationnel[71]. Deux déclarations bilatérales similaires viennent d'être signées entre l'Allemagne et la Finlande[72] ainsi qu'entre l'Allemagne et les Pays-Bas[73].

❖ Quelques chiffres et ressources

- +13,5 millions de citoyens européens vivent dans un État membre de l'UE autre que leur pays d'origine.
- +0,5 million d'étudiants européens étudient dans un État membre de l'UE autre que leur pays d'origine.
- +7,5 millions de professionnels de l'UE travaillent dans un État membre de l'UE autre que leur pays d'origine.
- +2,7 millions de nouvelles entreprises ont été créées dans l'UE.
- Carte interactive sur « *l'État de l'art international des initiatives liées à l'identité décentralisée*[74] »

❖ Questions éventuelles pour lancer la table ronde

➢ Le *European Digital ID Wallet* ou portefeuille européen d'identité numérique (PEIN) comme futur dispositif (facultatif) de droit commun

- Quelles conséquences en terme de souveraineté numérique nationale le portefeuille européen d'identité numérique induit-il ?
- De quels usages pourront relever ces portefeuilles d'identité numérique aux frontières ?[75] Quel est le lien avec le certificat européen covid numérique[76] (ou passe sanitaire) ?
- À quelles sanctions s'exposent les Etats membres à ne pas mettre en œuvre le PEIN ?
- Comment s'articulerait la blockchain avec la protection du RGPD attribuée aux données personnelles ?

---

[69] ISO/TC 307 - Technologies des chaînes de blocs et technologies de registre distribué. Travaux sur cette norme ISO/TC 307 consultés en ligne le 11 avril 2022 et disponibles sur : https://www.iso.org/fr/committee/6266604.html

[70] IUT, Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités, septembre 2020, 23 p. Consulté en ligne le 11 avril 2022 et disponible sur : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1403-202009-I!!PDF-F&type=items

[71] Joint Declaration on cooperation and exchange of best practices in the field of self-sovereign identity between the Federal Republic of Germany and the Kingdom of Spain, 29 juillet 2021.

[72] Declaration for cooperation and exchange of best practices in the field of Self Sovereign Identity between the Federal Republic of Germany and the Republic of Finland, 22 septembre 2021.

[73] Nederland gaat met Duitsland werken aan digitale identiteit, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23 septembre 2021.

[74] Thibault Langlois-Berthelot, État de l'art international des initiatives liées à l'identité décentralisée. 4 juin 2021. Carte consultée en ligne le 11 avril 2022 et disponible sur : www.framacarte.org/m/101445

[75] La société IDEMIA du groupe Havas propose par exemple d'intégrer les passes sanitaires ou vaccinaux à un passeport de santé (« Health Travel Pass ») répondant aux normes établies par l'OACI (Organisation de l'Aviation Civile Internationale) pour faire face à la crise Covid19.
Voir à ce propos : Hanna Sebbah, IDEMIA Launches Health Travel Pass, Which Seeks to Help Governments Boost Border-Crossing Traveler Traffic, *Businesswire [en ligne]*, 16 avril 2021. Consulté en ligne le 11 aril 2022 et disponible sur : https://www.businesswire.com/news/home/20210412005367/en/IDEMIA-Launches-Health-Travel-Pass-Which-Seeks-to-Help-Governments-Boost-Border-Crossing-Traveler-Traffic
OACI, *Guidelines Visible Digital Seals ("VDS-NC") for TravelRelated Public Health Proofs*, 2021, 29 p. Consulté en ligne le 11 aril 2022 et disponible sur : https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf
D'autre part, la société urinis.io (France) et le Forum Économique Mondial (lobby international) dispensent un service de vérification de l'identité et du statut de santé des individus à partir d'une prise de sang, fondé sur la blockchain et pouvant intégrer le passe sanitaire ou vaccinal Covid19 requis aux frontières.
Uniris, *Be the only key to the next evolution of the Internet,* uniris.io *[en ligne],* date inconnue. Consulté en ligne le 12 avril 2022 et disponible sur : https://uniris.io/
Forum Economique Mondial, *World Economic Forums presents CovidPass*, *covid-pass.tech [en ligne]*, 2020. Consulté en ligne le 12 avril 2020 et disponible sur : https://www.covid-pass.tech/
Yannick Chatelain, Du pass vaccinal au portefeuille numérique obligatoire, *Contrepoints*, 5 janvier 2022. Consulté en ligne le 12 avril 2022 et disponible sur : https://www.contrepoints.org/2022/01/05/418467-du-pass-vaccinal-au-portefeuille-numerique-obligatoire

[76] Règlement 2021/953 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19, 14 juin 2021. Consulté en ligne et disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021R0953&from=FR

➢ Les techniques des blockchains et du *European Digital ID Wallet* (PEIN)

- Comment fonctionne une blockchain ? Quels avantages et inconvénients en retirer ?
- Comment fonctionne le PEIN (eDIW) ? Quels sont ses avantages et ses inconvénients ?
- Quelle(s) différence(s) existe-t-il entre l'identité numérique centralisée et décentralisée ?
- Peut-on réellement qualifier le PEIN d'identité décentralisée ou au contraire, s'agit-il d'une re-centralisation de l'identité par l'Union européenne (fondée certes sur une technologie décentralisée, la blockchain, mais au regard d'un registre centralisé) ?

➢ L'impact de ces technologies (blockchain, PEIN) pour les personnes

- Quelles conséquences et garanties en matière de droits fondamentaux des personnes physiques ou morales faut-il entrevoir par l'usage de la blockchain pour le PEIN ?
- Quels impacts sociaux et économiques faut-il envisager par les usages du PEIN des personnes physiques ou morales ?
- Quels liens existe-t-il entre la finance décentralisée et l'identité numérique décentralisée ?
- Quels sont les risques afférents aux vols de données, à l'altération de documents ou aux usurpations d'identité ?

➢ Prospective

- L'adoption prévue pour 2023 de la proposition d'amendement « eIDAS-V2 » est-elle trop ambitieuse ?
- Faut-il préférer une identité totalement décentralisée (sur blockchain publique comme Bitcoin) ou bien une identité numérique hybride (certaines composantes centralisées et d'autres décentralisées) ?
- Qu'adviendra-t-il du rapport entre la future blockchain européenne (EBSI) et les blockchains publiques (Bitcoin, Ethereum) ?
- Si les sanctions sont absentes du règlement eIDAS V2, de quels outils disposera la Commission européenne pour son effective application ?
- Quels sont les recours dont bénéficieront les utilisateurs du PEIN quant à l'enregistrement ou à la rectification de leurs attributs ?

***