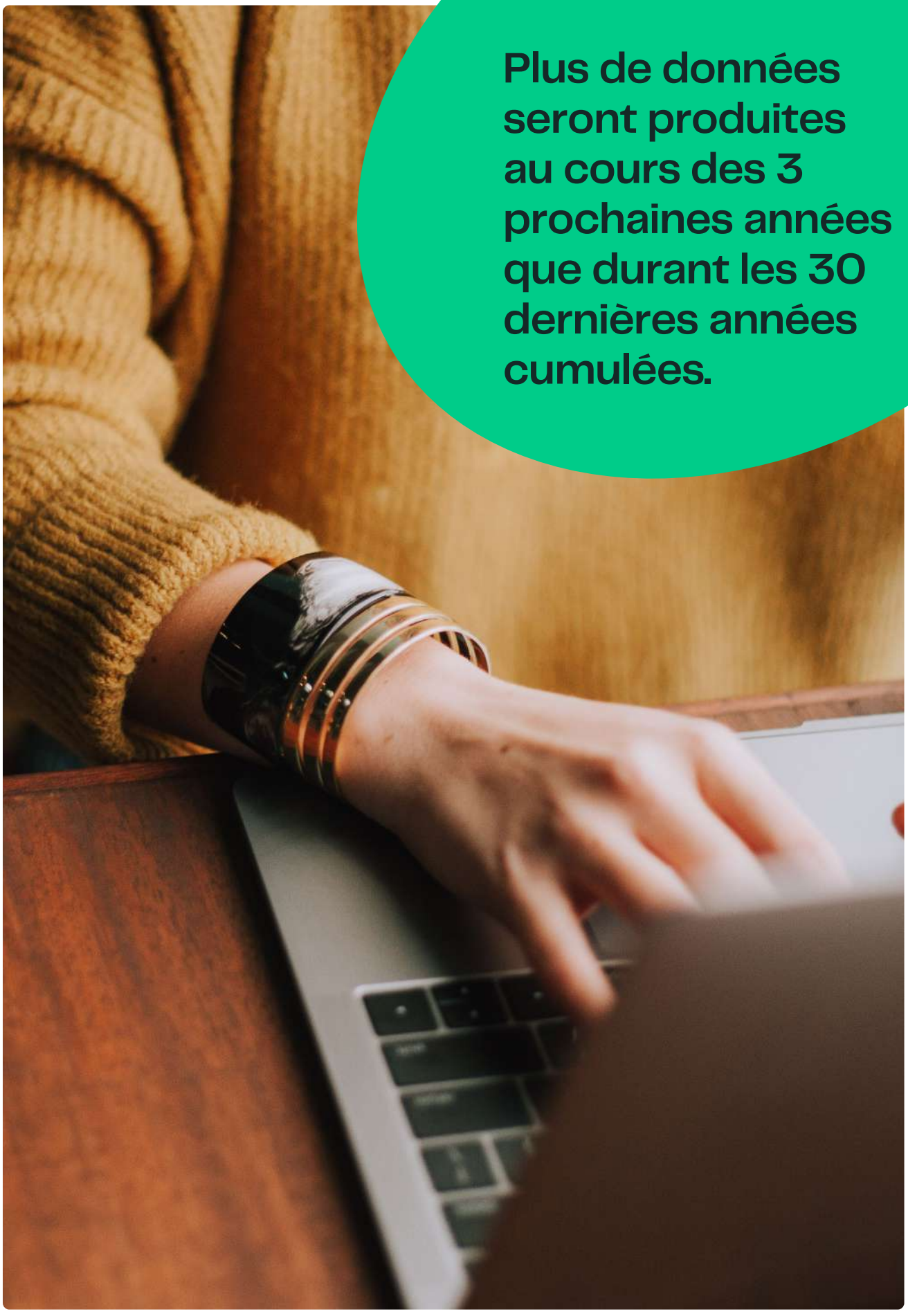
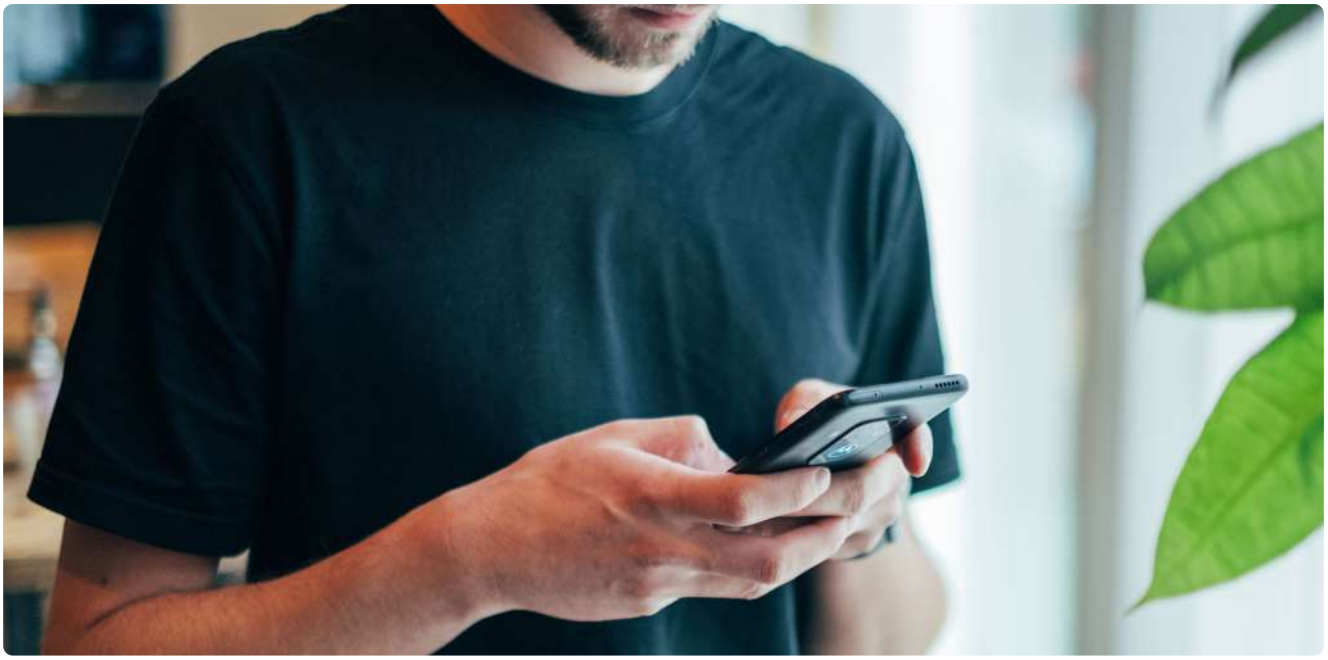
Le futur de l'identité numérique est décentralisé

Archipels



Plus de données seront produites au cours des 3 prochaines années que durant les 30 dernières années cumulées.



Les quantités de données échangées chaque jour ont considérablement augmenté ces dernières années, allant de pair avec la multiplication des sources et des moyens de collecte d'information. On estime qu'on produira plus de données dans les 3 ans à venir que pendant les 30 dernières années.[1] En parallèle de cette augmentation spectaculaire, on assiste à une défiance croissante des individus sur la manière dont leurs données personnelles sont traitées et conservées.

Et pour cause, selon le baromètre du Forum International de la Cybersécurité 2021, les violations de données sont en constante hausse : en un an et demi, le nombre de violations de données par jour est passé de 4,5 à 7.[2] Dans le viseur, la manière centralisée dont nos données sont conservées. Cette centralisation augmente considérablement les points de défaillance et s'accompagne d'une accumulation de données personnelles chez les géants de la technologie. C'est pourquoi, à l'instar de la nouvelle proposition de règlement pour établir un cadre d'identité numérique européenne[3], de plus en plus de voix s'élèvent pour l'émergence de nouveaux systèmes de gestion de notre identité numérique : décentralisés et contrôlés par l'utilisateur.

[1] International Data Corporation, Global DataSphere Forecast. 2020. Traduit de l'anglais vers le français
[2] Forum international de la Cybersécurité (FIC), Baromètre Data Breach 2021. Juin 2021
[3] Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity

De l'identité à l'identité numérique : des facettes multiples

Archipels

De manière classique, lorsqu'il est fait référence à l'identité, l'on pense aisément aux attributs d'état civil d'une personne :

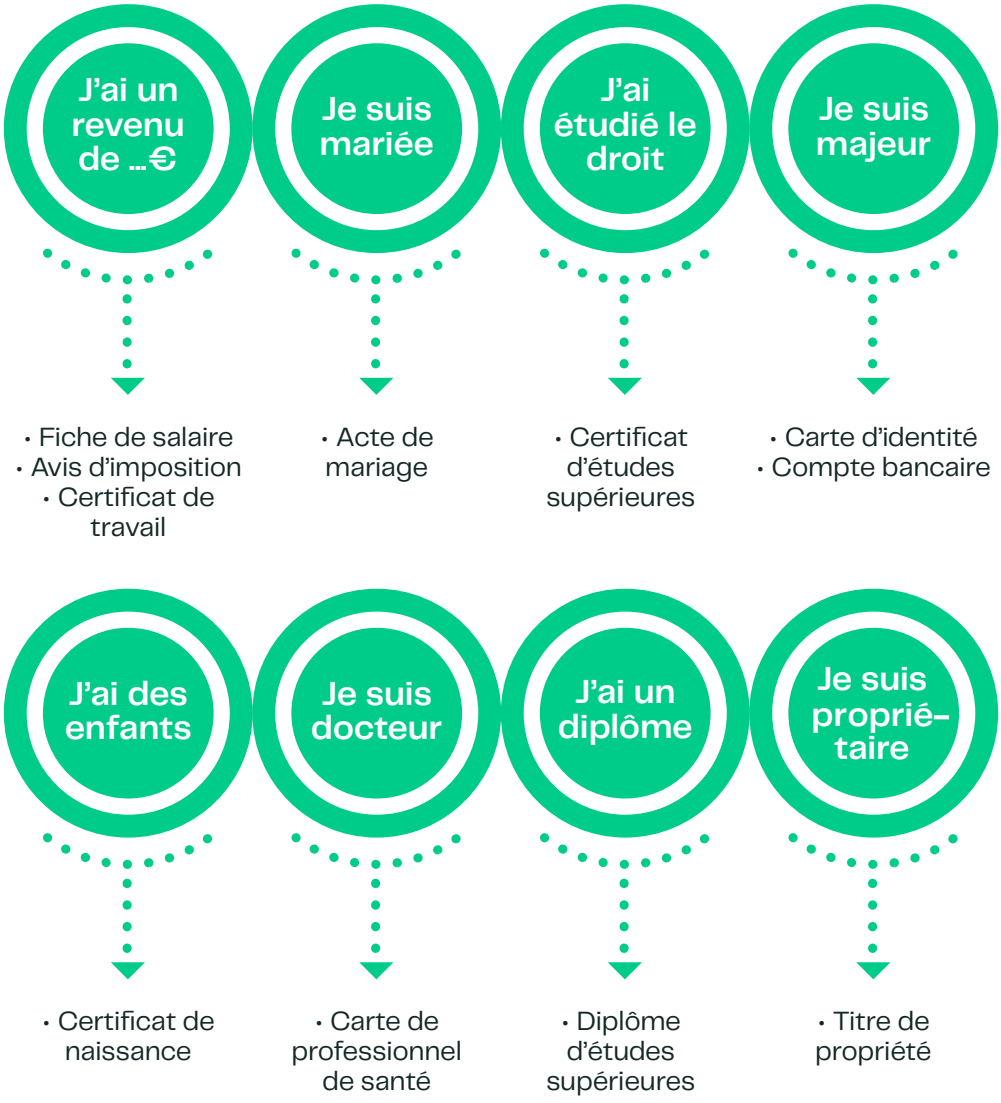
son nom, son prénom, sa date et lieu de naissance, son sexe ou encore sa nationalité. Cette identité dite pivot[4] est généralement inscrite dans les registres de l'état civil. Elle figure ensuite dans les titres d'identités qui permettent à toute personne de prouver son identité, d'être reconnue par la société et d'exercer ses droits dans le monde physique. Il en va de même pour les entreprises lors de leurs enregistrements au Registre du Commerce et des Sociétés. Avec les avancées d'Internet, et, dans un monde numérique en plein essor où les échanges sont de plus en plus digitaux, la notion d'identité s'est complexifiée. Un ensemble très disparate de données sont utilisées pour représenter et distinguer une personne incluant par exemple le courriel, des identifiants de connexion divers, des caractéristiques biométriques, un numéro de carte bancaire ou encore l'adresse IP.

[4]La terminologie d'identité pivot est celle retenue par le Ministère de l'Intérieur. Ministère de l'Intérieur, Livre blanc Blockchain et Identification Numérique. Restitution des ateliers du groupe de travail « blockchain et identité » (BCID)V1. Octobre 2020

L'identité est désormais numérique et consacre la projection des droits de la personnalité dans l'espace Internet. L'identité numérique opère une distinction entre le sujet – la personne ou l'entité – et ses attributs qui sont des éléments se rapportant à lui et pouvant être vérifiés, ou, au contraire, être contestés. Par exemple, un attribut concernant un individu pourrait être que celui-ci a plus de dix-huit ans. Pour une entreprise, cela pourrait être que celle-ci a régulièrement publiée ses comptes annuels.

De manière très intuitive, l'on comprend que certains attributs seront prouvés dans la vie de tous les jours sous forme de justificatifs. L'identité numérique se définit ainsi comme l'ensemble des attributs et des justificatifs numériques concernant une personne ou une entité qui sont utilisés pour la représenter et la distinguer dans ses interactions digitales avec les autres. D'un point de vue plus technique, l'identité numérique résulte de la codification numérique de ces identifiants et attributs de manière à pouvoir être traités et interprétés par des systèmes informatiques.

Certaines affirmations doivent être prouvées par des justificatifs.



Les attributs constitutifs de l'identité numérique, vont quant à eux varier en fonction du contexte dans lequel la personne ou l'entité veut exercer ses droits. Ainsi, s'il fait sens d'utiliser un attribut d'identité émis par l'Etat, par exemple, une attestation numérique d'affiliation à la sécurité sociale, pour se connecter à une plateforme de santé, l'utilisation de cet attribut n'est en rien nécessaire pour s'inscrire à un service de livraison de courses à domicile. La diversité des informations pouvant être demandées va donc de paire avec la variété des services de la société civile. Ce pluralisme est d'ailleurs à l'origine des modèles actuels de gestion de l'identité numérique.

Pourquoi les modèles actuels de gestion de l'identité numérique sont insuffisants ?

Archipels

Pour mieux comprendre les modèles actuels de gestion de l'identité numérique, il faut remonter aux origines d'Internet.

Internet a été construit sans couche – ou "layer" – d'identité.[5] Lorsque qu'Internet a été conçu à la fin des années 1960[6], la question était de savoir comment connecter des machines à travers des réseaux locaux.

Bien loin du World Wide Web, le réseau ARPANET initial était ainsi constitué uniquement de quatre ordinateurs hôtes.[7] Le problème de leurs identifications était résiduel puisque le réseau fonctionnait en architecture fermée. Cependant, pour étendre ce réseau à une architecture ouverte et globale, encore fallait-il créer de nouveaux protocoles de communication permettant d'identifier l'ensemble des machines connectées au réseau.

C'est ainsi que le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) vit le jour : fournissant une adresse IP à chaque machine du réseau afin de pouvoir acheminer et échanger des paquets de données. Pour autant, cette adresse IP ne permet que de connaître l'identité de la machine connectée au réseau, et ne dit rien sur l'identité de la personne ou de l'organisation qui contrôle cette machine et communique avec l'ensemble du réseau.

[5] PREUKSCHAT, Alex, REED, Drummond, Self-Sovereign Identity Decentralized digital identity and verifiable credentials. Mai 2021. 504 pages
[6] LEINER, Barry M.; et al, A Brief History of the Internet. MIT Computer Communication Review Volume 39, Number 5. Octobre 2009
[7] Id.

Ainsi et comme constaté par Kim Cameron :

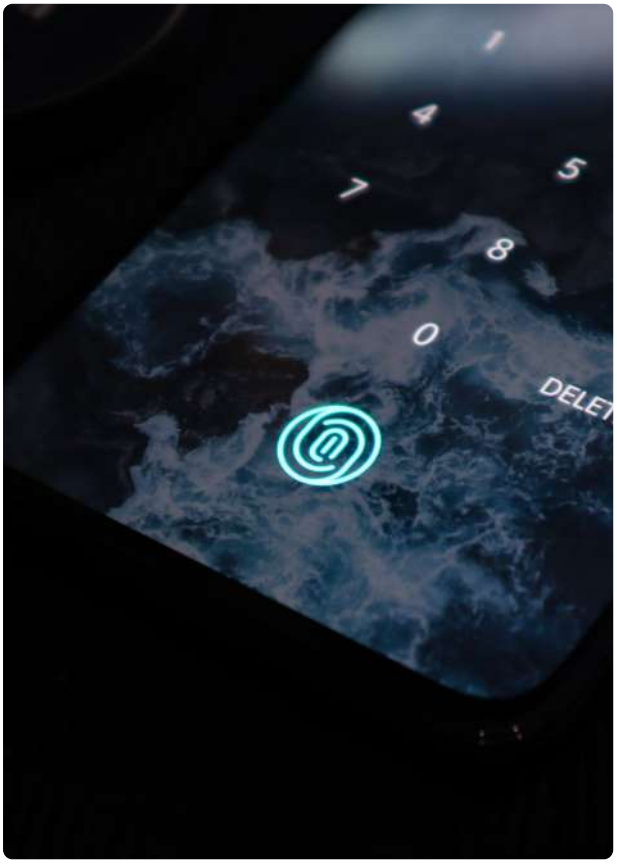
«Internet a été dessiné sans qu'il soit possible de savoir à qui et à quoi vous vous connectez. Cela limite ce que nous pouvons en faire et nous expose à des dangers croissants (…) qui auront pour effet d'éroder la confiance du public dans Internet.»[8]

Des solutions ont été trouvées mais sont encore insuffisantes. Les systèmes dit « centralisés » sont les plus couramment utilisés. Ils reposent sur la création d'un compte utilisateur par individu pour l'accès à une offre, un service ou plus généralement à une plateforme. Dans ce format, l'individu a autant d'identités numériques qu'il a de profils. Il est ainsi estimé que chaque personne a en moyenne 150 comptes sur Internet.[9]

Ce nombre est en proportion avec autant de potentielles failles de sécurité – les individus utilisant souvent le même mot de passe. De plus, les informations fournies à la plateforme sont généralement ré-utilisées par les opérateurs de services en ligne, en application des règles contenues dans des politiques de confidentialité aussi variées qu'opaques.

Prenant en compte les nombreux désavantages liés aux systèmes centralisés de gestion de l'identité numérique, depuis quelques années on assiste à l'émergence de systèmes dit « fédérés ». Ces solutions ont été pour la plupart développées sous l'égide du désormais célèbre Internet Identity Workshop, et ont toutes pour but de créer une identité centrée sur l'utilisateur.

[8] CAMERON, Kim, The Laws of Identity. Novembre 2005. Traduit de l'anglais vers le français.
[9] WANG, Chun; et al. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. Department of Computer Science, Virginia Tech, Blacksburg, VA, 24060. 2018. Voir aussi : Dashlane, Dashlane Uncovers Troubling Password Patterns. Mai 2018



Le principal apport de l'approche fédérée est en effet de permettre aux individus d'utiliser la même identité numérique – ou du moins les mêmes informations d'identification – pour accéder à des services sur différents sites. Le modèle fédéré permet de remédier à l'inconvénient de devoir créer une multiplicité de comptes. L'innovation a consisté à introduire des « fournisseurs d'identité » (Identity providers ou IdP). Ce sont des autorités de confiance qui gèrent les données d'identité et les comptes des utilisateurs.

Trois générations de protocoles d'identité fédérée ont été développées depuis 2005 – SAML (Security Assertion Markup Language), OAuth et OpenID Connect. Grâce à ces protocoles, le SSO (Single Sign-On) est désormais une fonctionnalité standard de la plupart des intranets et extranets d'entreprise. OpenID Connect a quant à lui permis au grand public d'utiliser les boutons de connexion des grandes entreprises de la technologie, telles que Facebook, Google, Twitter, LinkedIn. En France, FranceConnect est un exemple de fournisseur d'identité connaissant un véritable succès avec déjà plus de 28 millions d'utilisateurs.[10]

[10] Acteurs publics, Les grands chantiers de transformation numérique de la rentrée. Août 2021

Exemples de prolifération de boutons « connexion sociale » pour tenter de simplifier l'usage de l'identité sur Internet

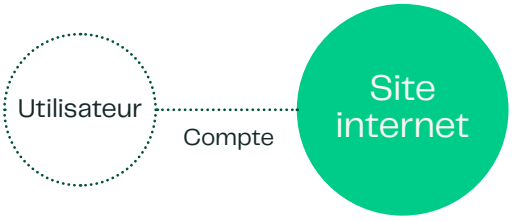
Bien que les données soient moins fragmentées que dans le modèle centralisé, les systèmes fédérés ne permettent pas pour autant de fournir une couche d'identité numérique suffisante pour Internet. En effet, l'approche reste plurale : il n'existe pas un seul fournisseur d'identité qui fonctionne avec tous les sites. Les utilisateurs vont donc avoir besoin de créer plusieurs comptes, chez plusieurs fournisseurs.

Pour contrer ce phénomène, les fournisseurs d'identité vont tenter de servir le plus grand nombre de sites possibles et vont donc adopter des politiques de confidentialité et de sécurité de relativement bas niveau, peu protectrices des données d'identité numérique de l'utilisateur. Or, une fuite de données chez le fournisseur d'identité pourrait conduire à des connexions non autorisées à de nombreux services.

Ces problèmes de sécurité et de confidentialité font qu'un certain nombre d'attributs numériques d'identité sensibles comme un passeport numérique ou des données financières, ne peuvent être hébergés par ces fournisseurs d'identité, limitant ainsi considérablement leur portée.

Les modèles actuels, qu'ils soient centralisés ou fédérés, échouent à doter les individus et les entreprises d'une véritable identité numérique. Cet échec se double d'une perte de confiance du public dans la manière dont leurs données personnelles sont gérées.

Il est d'ailleurs estimé que plus de 90 % des américains pensent qu'ils ont perdu le contrôle de la façon dont leurs données personnelles sont collectées et utilisées par toutes sortes d'entités.[11] Les scandales les plus récents ne font que confirmer cette érosion de la confiance[12] et que seule une identité numérique décentralisée et véritablement auto-contrôlée par les utilisateurs peut venir à bout de ces problèmes.



Le système centralisé de gestion des données

Le système fédéré de gestion de l'identité numérique

[11]Pew Research Center, Americans' complicated feelings about social media in an era of privacy concerns. Mars 2018

[12]Par exemple, la violation de données de Facebook d'août 2019. La fuite de données comprenait les données personnelles de plus de 533 millions d'utilisateurs de Facebook dans 106 pays. Voir notamment : Data Protection Commissioner, DPC launches inquiry into Facebook in relation to a collated dataset of Facebook user personal data made available on the internet, avril 2021

Pourquoi l'identité numérique doit-elle être décentralisée et auto-contrôlée ?

Archipels

L'identité décentralisée peut être définie comme un mécanisme permettant aux utilisateurs d'administrer directement leur propre identité numérique grâce à l'utilisation d'une architecture de registre distribué comme la technologie blockchain.

En effet, une avancée majeure dans le domaine de l'identité numérique est intervenue avec l'avènement de la technologie blockchain. D'abord pensée pour le domaine des monnaies et actifs numériques,[13] cette innovation amorce une transformation fondamentale dans la façon dont personnes et organisations peuvent prouver leur identité et établir la confiance en ligne. Dès 2015, les gouvernements américain[14] et estonien[15] se saisissaient du potentiel de cette technologie pour une gestion décentralisée de l'identité numérique.

[13] NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System. Octobre 2008

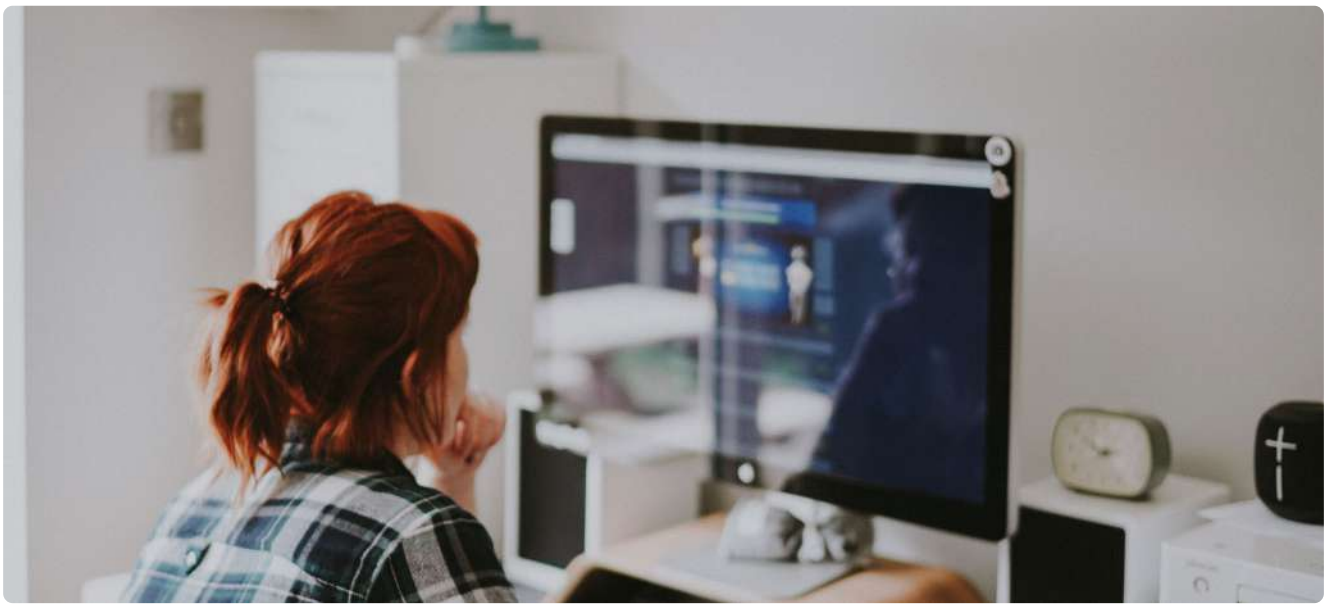
[14] Le 16 décembre 2015, la division Science et technologie du ministère américain de la Sécurité intérieure a publié un dossier de subvention pour la recherche sur l'innovation intitulé : L'applicabilité de la technologie Blockchain à la gestion de l'identité dans le respect de la vie privée. Titre traduit de l'anglais vers le français

[15] International Business Time, Bitnation and the Estonian government start spreading sovereign jurisdiction on the blockchain. Février 2016

Au lieu de créer et de gérer manuellement des comptes (identité centralisée) ou de faire confiance à des fournisseurs d'identité (identité fédérée), l'identité décentralisée place l'individu au centre de chacune de ses interactions numériques. Pour ce faire, l'identité décentralisée est fondée sur la base d'une relation de pair à pair entre trois parties :

L'émetteur de l'identité (issuer)

Dans la vie physique, comme numérique, chaque justificatif d'identité est généré par un émetteur. L'émetteur constitue la source des justificatifs prouvant les attributs d'identité d'une personne – l'auteur de ces documents en quelque sorte. La plupart des émetteurs sont des entités comme des agences gouvernementales (par exemple, l'Agence Nationale des Titres Sécurisés pour les cartes d'identité numérique, permis de conduire, etc.) mais il peut également s'agir d'institutions financières (relevés d'identité bancaire), de fournisseurs d'énergie (facture d'électricité pour justifier de l'adresse du domicile) et ainsi de suite. Il faut ici souligner qu'un individu peut lui aussi être émetteur de justificatif le concernant, par exemple pour les attestations de déplacement dérogatoire utilisées pendant la pandémie de Covid-19 ou pour tout autre type d'attestation auto-générée. Les objets connectés peuvent enfin aussi occuper cette fonction : un compteur d'électricité pourrait par exemple émettre un certificat numérique attestant de la consommation électrique d'un foyer.



Le titulaire de l'identité ou le sujet (holder)

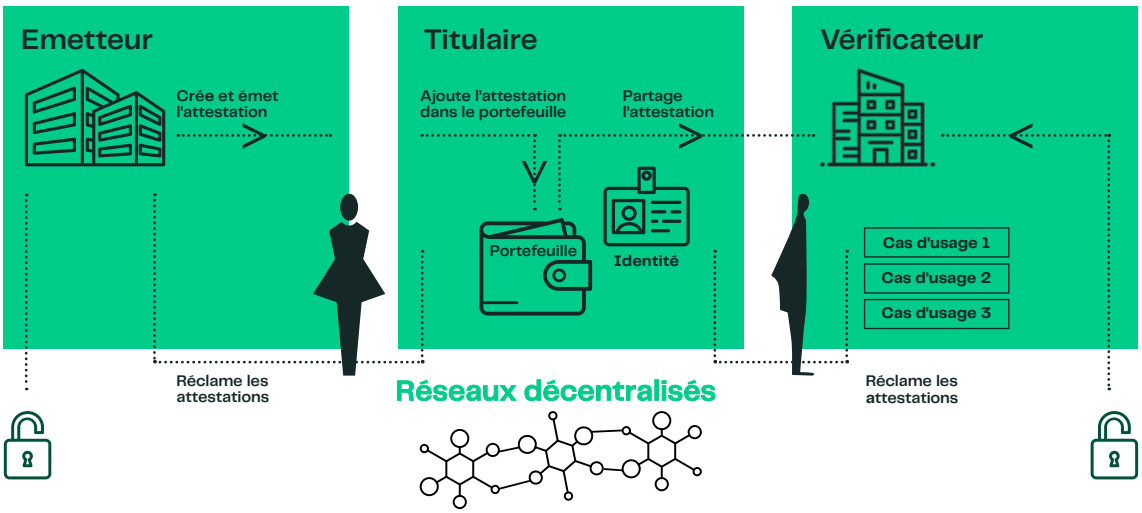
Il s'agit de la personne qui désire prouver son identité ou se connecter à un service en ligne. Le titulaire de l'identité demande des justificatifs portant sur son identité à l'émetteur sous la forme d'attestation vérifiable. Il conserve ensuite ces justificatifs dans son portefeuille numérique afin de pouvoir les présenter aux vérificateur lorsque ceux-ci en font la demande. Au centre de cette relation tripartite, le titulaire a toujours le choix de révéler ou non ses attributs d'identité. Il faut noter ici que dans certains cas d'usage, comme pour la gestion de l'identité d'une personne morale, une distinction peut être opérée entre le holder et le titulaire de l'identité. En effet, si le holder est généralement la même personne que le titulaire d'identité, dans certains cas, il peut aussi être un tiers qui stocke les informations d'identification pour le compte des titulaires d'identité.

Le vérificateur de l'identité (verifier)

Il représente n'importe quelle personne ou entité qui veut vérifier les informations d'identité numérique relatives à un titulaire d'identité afin de lui permettre d'exercer ses droits ou d'utiliser un service. C'est notamment le cas d'une assurance qui veut vérifier l'adresse de son client pour lui faire bénéficier d'un contrat d'assurance habitation. Si le titulaire d'identité accepte de révéler ses informations, le vérificateur va s'assurer à la fois de l'identité numérique qui lui est présentée et de la source de l'information. Le vérificateur s'assure notamment que la signature numérique de l'émetteur est bien présente dans l'attestation fournie. Cette dernière vérification garantit la confiance numérique et réduit considérablement les possibilités de fraude.

Le modèle tripartite de l'identité décentralisée reproduit ce que nous connaissons dans le monde physique.

Dans la vie de tous les jours, si un individu désire prouver son adresse, par exemple pour s'abonner à une salle de sport, il montrera sa carte d'identité à la personne chargée de son inscription. Ce justificatif d'identité fera foi car il est lui-même émis par un tiers de confiance. Avec l'identité numérique décentralisée, c'est exactement la même chose : l'individu pourra tout simplement prouver son identité numérique grâce aux attestations d'identité figurant dans son portefeuille numérique. Le vérificateur pourra ensuite s'assurer que cette attestation n'est pas un faux puisque signée par son émetteur officiel.

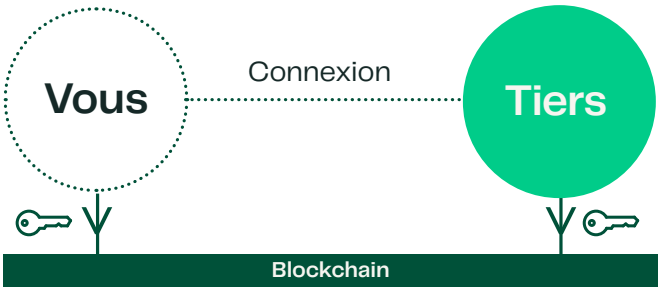


Au coeur de l'identité decentralisée : un individu en contrôle de ses données

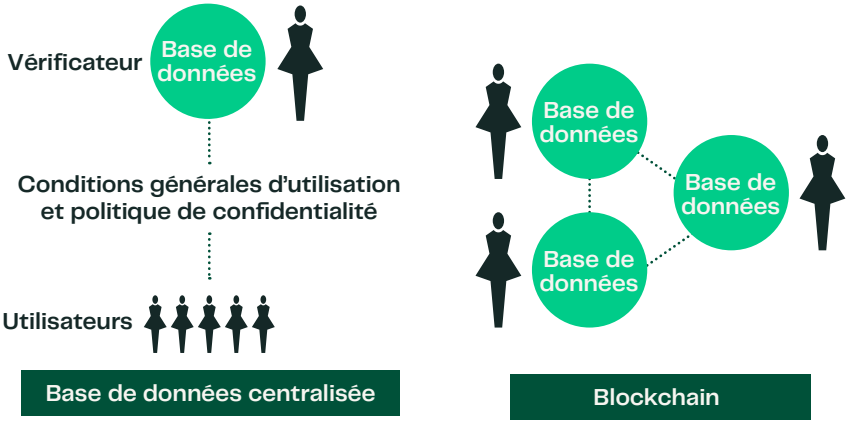
Il faut ici insister sur le fait que l'architecture décentralisée est essentielle pour le bon fonctionnement de ce système. C'est elle qui fournit la base technique nécessaire à la vérification des attestations numériques qui sont au cœur de l'identité décentralisée. En effet, comme décrit précédemment, le titulaire de l'identité doit faire signer numériquement ses informations d'identité, avant de les fournir au vérificateur.

Dans ce processus, la signature se fait à base d'un couple de clé publique-privé. Ce sont à la fois les clés publiques du titulaire de l'identité et de l'émetteur qui vont être utilisées. L'ensemble des clés publiques nécessaire à la signature des données d'identité, sont enregistrés dans un registre distribué.

La blockchain agit comme un stockage décentralisé de clés qui assure sécurité et résilience puisque qu'aucun tiers ne peut compromettre l'intégrité et la sécurité du système dans son ensemble. Sans architecture décentralisée, l'identité ne serait plus véritablement auto-contrôlée car on passerait nécessairement par un administrateur central, qui hébergerait toutes les attestations et identités des signataires de ce système, ce qui résulterait en une perte de contrôle de l'individu et une érosion de la sécurité de l'infrastructure. Finalement, tout ce que la blockchain permet de faire pour l'échange d'actifs numériques est également possible pour les informations d'identité des personnes et des entreprises.



La relation de pair à pair sans intermédiaire que permettent les solutions d'identité decentralisée

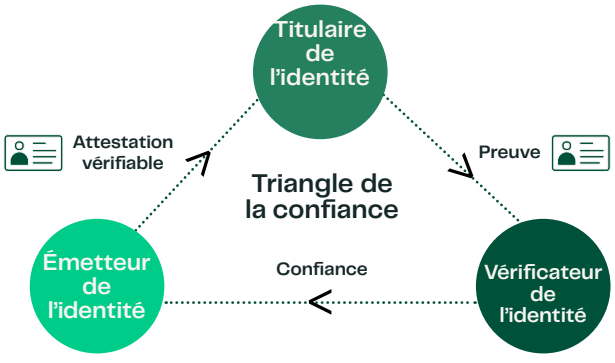


Base de données centralisées vs. blockchain

Cette architecture décentralisée est de plus génératrice de confiance. La relation tripartite de l'identité décentralisée est d'ailleurs couramment appelée triangle de la confiance dans le milieu de l'identité décentralisée.[16] Ce sont les titulaires d'identité ou les individus, qui décident des entités ou personnes à qui ils veulent révéler leur information d'identité.

Le principe au cœur de l'identité décentralisée est donc celle d'une identité numérique dont l'utilisateur porte les attributs, certifiés par des tiers émetteurs. Ce modèle novateur promet de garantir un haut niveau de confiance dans les données échangées tout en rétablissant l'individu au cœur des flux de données le concernant.

Ce système nécessite pour autant que tous les émetteurs d'identité soient capables d'émettre des attestations numériques et que celles-ci soient émises dans un format lisible par tous et interopérable. L'excellente nouvelle est qu'au niveau européen, le cadre réglementaire est en train de changer pour supporter cette vision novatrice de l'identité numérique.



Le triangle de la confiance de l'identité numérique décentralisée

[16] Voir par exemple PREUKSCHAT, Alex, REED, Drummond, Self-Sovereign Identity Decentralized digital identity and verifiable credentials. Mai 2021. 504 pages

Qu'est ce qui va changer avec le futur cadre pour une Identité Numérique Européenne ?

Archipels

Lors de son discours sur l'État de l'Union 2020, Ursula von der Leyen, présidente de la Commission européenne, a très justement rappelé : « Chaque fois qu'une App 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 Commission proposera bientôt 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. »[17]

Moins d'un an après cette annonce, le 3 juin 2021, la Commission européenne proposait un nouveau règlement pour l'établissement d'une identité numérique européenne (EUid).[18]

[17] VON DER LEYEN, Ursula, Discours sur l'État de l'Union 2020, 16 septembre 2020.
[18] Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity.

Cette proposition découle de la révision réglementaire du règlement 910/2014/UE (règlement eIDAS), et constitue une refonte complète du cadre européen d'identité numérique. Ce projet très ambitieux doit encore être voté par le Parlement Européen et le Conseil de l'Europe pour être définitivement adopté.

La proposition de règlement se veut neutre technologiquement et laisse une marge d'implémentation à plusieurs modèles de gestion de l'identité numérique des personnes et des entités. Pour autant, sa rédaction ouvre clairement la voie à une implémentation européenne de l'identité décentralisée. Pour preuve, l'Allemagne et l'Espagne ont déjà signé un protocole d'accord témoignant de leur volonté commune d'échanger sur le domaine de l'identité numérique décentralisée d'un point de vue technique, réglementaire et opérationnel.[19] Cette collaboration est ouverte aux autres États membres européens engagés dans le développement de tel écosystème. [20] La France, sous l'égide du Ministère de l'Intérieur, s'intéresse d'ailleurs de près au sujet de l'identité numérique décentralisée avec la publication d'un récent livre blanc traitant de ce que la blockchain peut apporter à l'identité numérique.[21]

La proposition devrait avoir un impact positif sur l'innovation, le commerce international et la compétitivité de l'Union Européenne en contribuant à sa croissance économique. Il est estimé que des investissements dans les solutions d'identité numérique devraient avoisiner les 3,2 milliards d'euros. Les bénéfices générés par ce changement réglementaire ont quant à eux été estimés à entre 3,9 et 9,6 milliards d'euros.

[19] Gouvernement fédéral Allemand, Germany and Spain and join forces on the development of a cross-border, decentralised digital identity ecosystem. Juillet 2021
[20] Explanatory Memorandum – Impact assessment. Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity
21 Ministère de l'Intérieur, Livre blanc Blockchain et Identification Numérique. Restitution des ateliers du groupe de travail « blockchain et identité (BCID). V1. Octobre 2020

La proposition devrait également avoir un impact positif sur l'emploi, en générant entre 5 000 et 27 000 emplois au cours des 5 années suivant sa mise en œuvre. Cela s'explique par l'investissement supplémentaire ainsi que par la réduction des coûts pour les organismes qui recourent à des solutions d'identification électronique.[22] Les entreprises utilisant des services d'identité qualifiée pour la souscription de nouveaux clients pourraient ainsi économiser jusqu'à 90% des coûts d'onboarding client.[23] Ce nouveau projet de règlement ambitieux comporte plusieurs volets, qu'il convient de détailler pour mieux comprendre son potentiel impact sur le modèle d'identité numérique décentralisé.

Un portefeuille numérique pour tous les citoyens et résident européens

Comme précédemment décrit, le portefeuille numérique revêt une importance cruciale dans les systèmes d'identité numérique décentralisée. **Comme pour le portefeuille dans le monde physique, le portefeuille numérique est en effet l'outil qui permet à tout individu de stocker ses informations d'identification et de les protéger du vol tout en les conservant dans un endroit accessible.** Le concept de portefeuille numérique n'est d'ailleurs pas inconnu du grand public, à l'instar des portefeuilles numériques pour smartphones les plus populaires (Apple Wallet et Google Pay) ou de ceux développés par des acteurs bancaires (Paylib en France). Pour autant, l'ambition de la Commission européenne dépasse largement ces trois exemples.

De manière inédite, la proposition de règlement EUid impose à chaque Etat Membre de fournir de manière gratuite un portefeuille numérique européen certifié à leurs citoyens et résidents.[24] Le portefeuille numérique doit pouvoir être utilisé sur l'ensemble du territoire de l'Union Européenne pour permettre aux individus de s'identifier et s'authentifier pour accéder à des services dans les secteurs public et privé, y compris transfrontaliers. **Sa reconnaissance sera ainsi obligatoire dans le secteur public et pour de nombreuses entreprises du secteur privé, y compris les grandes plateformes en ligne.[25]**

[22] Id.
[23] McKinsey Global Institute, Digital identification: A key to inclusive growth. Avril 2019
[24] Article 6(a). Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity
[25] Article 12(b). Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity

Aligné avec le concept du triangle de la confiance de l'identité numérique décentralisée, les futurs portefeuilles numériques devront permettre aux citoyens européens d'obtenir, stocker et combiner des attestations numériques émises par des tiers de confiance.

Les vérificateurs devront quant à eux être autorisés à authentifier l'utilisateur et à recevoir ces attestations. **Ce faisant, la proposition de règlement crée de nouveaux services de confiance.**

Création de nouveaux services de confiance autour de l'identité numérique

La proposition de règlement EUid consacre le secteur privé comme fournisseur de services liés à l'identité numérique avec la création de nouveaux services de confiance incluant les services liés aux attestations électroniques d'attributs et de registre électronique.

Concernant les attestations électroniques d'attributs, le futur règlement EUid définit un attribut comme une caractéristique ou une qualité d'une personne physique ou morale ou d'une entité, sous forme électronique. La similarité avec la définition des verifiable credentials du modèle de l'identité décentralisée est frappante[26]. Les émetteurs d'identités se voient ainsi confier un nouveau service de confiance : celui d'émettre des attestations électroniques – qualifiées ou non – pouvant interagir avec les portefeuilles européens. Pour l'heure, seuls les effets juridiques des attestations électroniques d'attributs sont spécifiés dans la proposition. **Il est notamment prévu que l'attestation électronique qualifiée d'attributs produise les mêmes effets juridiques que les attestations légalement délivrées sur papier.[27]** Pour autant, les règles relatives à l'émission, au format, au fonctionnement et à l'interopérabilité de ces attestations ne sont pas encore précisées.[28] Elles devront faire l'objet d'une définition par les États Membres dans le cadre du programme Toolbox débutant en septembre 2021.

[26] PREUKSCHAT, Alex, REED, Drummond, Self-Sovereign Identity Decentralized digital identity and verifiable credentials. Mai 2021. 504 pages
[27] Article 45(a). Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity
[28] Article 45(c) & 45(d). Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity

La nouvelle section dédiée au registre électronique qualifié consacre la présomption d'unicité, d'authenticité et d'immuabilité des données y étant contenues. De nouveau, il faut rappeler que si la proposition de règlement est agnostique technologiquement, ces nouvelles dispositions comprennent une rédaction suffisamment large pour s'appliquer à la technologie blockchain. Les entreprises opérant une blockchain permissionnée pourront donc demander à ce que celle-ci soit qualifiée officiellement en tant que service de confiance. **Cette ouverture est une excellente nouvelle pour l'ensemble de la communauté de l'identité décentralisée**, qui pourra se fonder sur une blockchain permissionnée à la valeur probante officiellement reconnue au niveau national et européen.

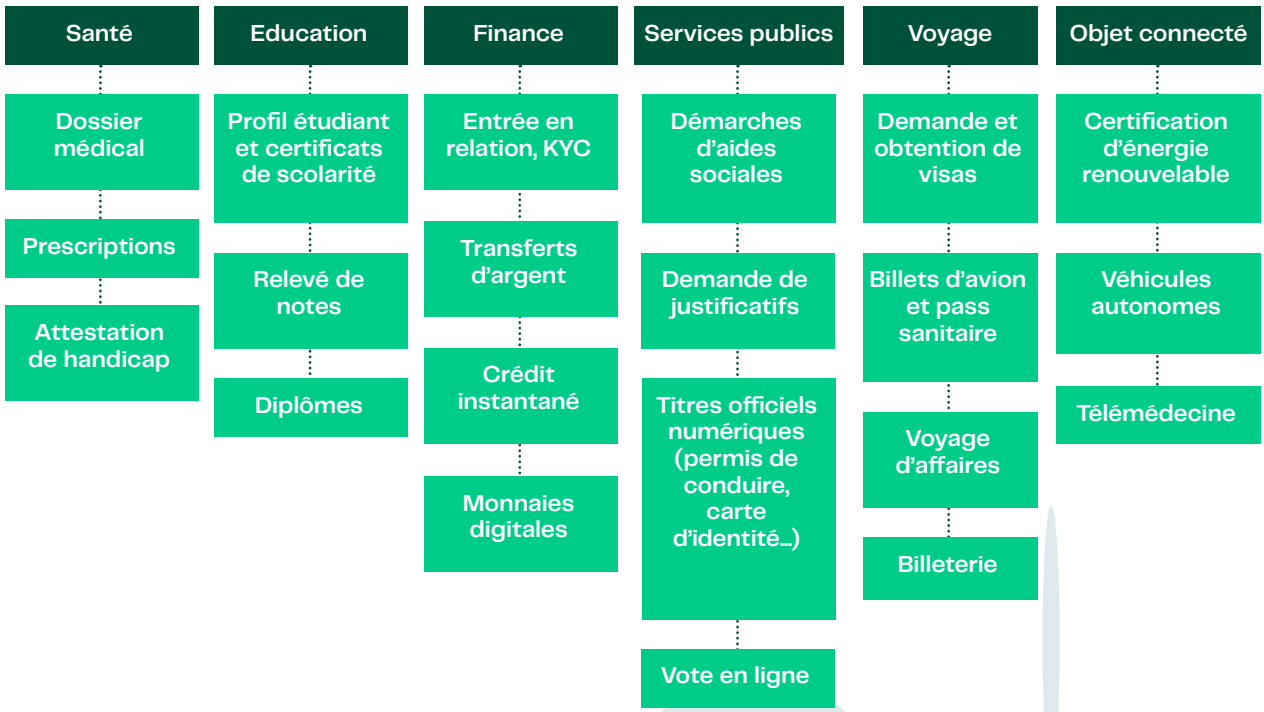
L'ambition de la commission européenne avec cette nouvelle proposition de règlement EUid ne peut être que saluée en ce qu'elle entrouvre une implémentation européenne uniforme de l'identité décentralisée. Si le règlement est adopté, les cas d'usages possibles seront aussi multiples qu'impactants pour la vie quotidienne des citoyens européens.

Quels sont les cas d'usage de l'identité décentralisée ?

Archipels

Les principaux cas d'usage liés à l'identité décentralisée

L'identité décentralisée permet de nombreux cas d'usage garantissant un accès simple, sécurisé et pérenne aux services numériques. **Finalement, ce sont tous les aspects de la société civile qui peuvent bénéficier des solutions d'identité décentralisée grâce à la généralisation prochaine des portefeuilles numériques.** Il convient de détailler quelques-unes des applications les plus prometteuses.



Les principaux cas d'usage de l'identité numérique decentralisée

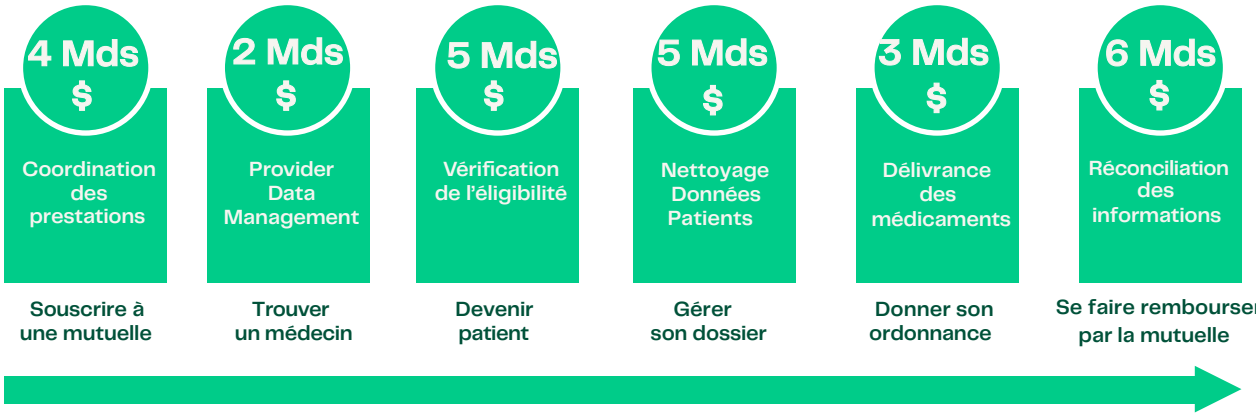
L'accès aux services de santé

Le secteur de la santé est également une industrie qui va être bouleversée par l'avènement de l'identité numérique décentralisée.

L'industrie de la santé est portée par la croissance exponentielle de la donnée. Ainsi le taux de croissance annuel prévisionnel de la quantité de données est estimé à 36% pour la période 2018-2025.[29]

Ce flux de données grandissant expose encore davantage les individus à des risques. Chaque fuite de données dans le secteur de la santé coûte très cher. Selon un très sérieux rapport d'IBM, chaque fuite de données coûterait en moyenne 7,13 millions de dollars en moyenne aux entreprises du secteur.[30]

En plus de diminuer les risques, l'identité numérique décentralisée permet de réduire les coûts à chaque étape du processus de vérification d'identité. Cette réduction des coûts ne se fait pas pour autant au détriment de la vie privée des patients. En effet, les systèmes de gestion de l'identité numérique décentralisée permettent de garantir le plus grand respect de la vie privée des individus grâce aux mécanismes de divulgation sélective décrits plus en détail ci-dessous.



L'identité numérique dans le secteur de la santé – Vérification des coûts
(Optum, CAQH, PokitSoc, M2SYS, J Emerg Med., Black Book Research)

[29] IDC & Seagate. Data Age 2025 : The Digitization of the World From Edge to Core. Novembre 2018.
[30] IBM Security, Rapport sur le coût d'une violation de données. 2020.

La simplification des services liés à l'éducation

Le domaine de l'éducation sera assurément transformé par les solutions d'identité décentralisée. De nombreuses applications sont envisageables à la fois pendant et après la scolarité de l'étudiant.

La création d'un système décentralisé de profils d'étudiants centré sur l'élève permet de réduire les nombreuses frictions ralentissant actuellement l'échange d'informations dans l'enseignement secondaire. Ce dossier pourrait contenir à la fois des données de profil (par exemple, nom et prénom de l'étudiant, statut de boursier ou non boursier, ses relevés de notes et diplômes.

Ce système d'identité décentralisée facilite par exemple l'échange de diplômes et leur reconnaissance transfrontalière entre universités. Ainsi, un étudiant souhaitant réaliser un échange dans une université étrangère pourra seulement partager une attestation numérique d'attributs relative à son diplôme ou aux unités d'enseignement précédemment suivies par lui, sans qu'une traduction officielle et qu'un processus d'audit supplémentaire de son dossier ne soit nécessaire pour l'université d'échange.

Après sa scolarité, l'étudiant pourra partager une attestation électronique d'attributs à son futur employeur pour prouver qu'il a bien les qualifications requises pour le poste auquel il prétend. Les employeurs n'auront qu'à vérifier les attestations partagées par l'étudiant, sans avoir à contacter l'université pour s'assurer de leurs véracités.

Le cas d'usage éducation fait déjà l'objet de plusieurs expérimentations et preuves de concept au niveau français et européen afin de démontrer la viabilité des systèmes d'identité décentralisée. La société française BC Diploma propose par exemple des services dédiés à la certification de documents académiques.[31] L'échange de diplôme est également un des premiers cas d'usage développé au niveau européen par l'EBSI avec le soutien de l'Université de Lille.[32]

[31] Plus d'informations sur le site de BC Diploma. Disponible en ligne ici : https://www.bcdiploma.com/fr.
[32] Voir notamment : EBSI Documentation, Use case diploma. Disponible en ligne ici : https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=380862522.

L'accès aux services financiers digitaux

Les secteurs banque, assurance et courtage sont sans aucun doute les premiers intéressés par des identités numériques sécurisées et légalement reconnues. Dans ces domaines, la connaissance client est indispensable pour traiter des opérations. La réglementation applicable ainsi que les autorités de contrôle imposent notamment l'obligation aux banques de justifier d'une parfaite connaissance de leurs clients ainsi que de la cohérence des opérations initiées sur les comptes de ces derniers.

Les coûts de processus de connaissance client, de lutte contre la fraude et le blanchiment d'argent, se sont envolés ces dernières années avec le durcissement des réglementations et l'augmentation des tentatives de fraudes. **Le recours à l'identité numérique et ses multiples attributs certifiés (par exemple, l'adresse, les revenus, le statut marital, l'IBAN) facilitera ce processus de connaissance client et rendra plus fluide l'ouverture de comptes bancaires en ligne et la souscription de crédits de manière instantanée et sécurisée.**

L'identité numérique décentralisée ouvre également l'accès aux applications financières, y compris pour les personnes non-bancarisées. A ce titre, le projet d'euro numérique pourrait prendre la forme d'une architecture décentralisée et reposerait sur la création de portefeuilles numériques propre à chaque individu.[33] Si quatre options d'architecture sont aujourd'hui à l'étude par la Banque Centrale Européenne, il faut tout de même souligner que l'euro numérique basé sur la technologie blockchain permettra une véritable désintermédiation des échanges financiers avec partages pair-à-pair instantanés et frais de gestion bancaire diminués. Ce choix technique permettra également une plus grande transparence : les transactions étant enregistrées sur un registre vérifiable et auditable. Ce portefeuille numérique permettra enfin d'accéder à de futurs services de finance décentralisée (prêts, emprunts, investissements), sans passer par des intermédiaires, ouvrant ainsi la voie à une plus grande démocratisation des services financiers traditionnels.

[33] Les Echos, La BCE lance officiellement les travaux sur l'euro numérique. Juillet 2021.

L'accès aux services publics dématérialisés

L'identité numérique décentralisée présente tout autant d'avantages pour le secteur public, notamment pour tous les services liés à l'état civil, en simplifiant au maximum les interactions avec les services publics tout en réhaussant le niveau de sécurité (par exemple pour déclarer ses impôts, demander des aides publiques, demander des justificatifs).

Depuis plusieurs années, FranceConnect permet la connexion à plus de 900 services en ligne, offrant une première expérience de simplification de l'accès aux services publics via des identités numériques partenaires, dont L'Identité Numérique La Poste.

Allant encore plus loin, avec une véritable architecture décentralisée, le cas du gouvernement estonien est édifiant. À l'heure actuelle, 99% des services publics estoniens sont accessibles aux citoyens sous forme de services en ligne. La déclaration d'impôt prend moins de cinq minutes, le vote public se fait en ligne et la création d'une e-société est un jeu d'enfant.[34] Selon le gouvernement estonien, l'Estonie économise chaque année plus de 1400 ans de temps de travail et 2 % du PIB grâce à ses services publics numérisés.[35] Ces résultats spectaculaires s'expliquent par le fait que l'Estonie a été le premier État au monde à déployer dès 2012 la technologie blockchain avec un registre des successions tenu par le ministère de la justice.[36]

[34] Voir notamment PWC Estonia, Estonia the digital Republic Secured by Blockchain. 2019
[35] Id.
[36] Id.

Une expérience client améliorée pour les secteurs culture, loisirs et voyage

Les secteurs de la culture, des loisirs et du voyage bénéficieront également grandement d'identités numériques simples, sécurisées et portables.

L'accès aux évènements culturels et de loisirs ainsi que l'ensemble du secteur de la billetterie pourront utiliser des attributs spécifiques, tel que l'âge, ou encore l'appartenance à un groupe (par exemple le fait d'être salarié d'une entreprise mécène d'un musée afin de faciliter l'allocation de réduction tarifaires ou d'accès gratuits. L'enjeu pour les musées est la réduction des accès frauduleux par la contrefaçon de billets ou l'obtention de réductions indues.

En Allemagne, le gouvernement fédéral a déployé en coopération avec le secteur privé un pilote visant à démontrer l'avantage des identités numériques décentralisées. Il s'agit de faciliter l'enregistrement dans les hôtels pour les voyageurs d'affaires, en associant dans un portefeuille numérique l'état civil officiel délivré par le gouvernant et des attributs complémentaires délivrés par l'employeur à son salarié en déplacement. 120 hôtels partenaires peuvent d'ores et déjà accueillir de manière sécurisée, rapide et complètement dématérialisée les salariés de Lufthansa et de Bosch.[37] Ce projet constitue le premier pilote d'une stratégie d'écosystème à grande échelle autour de l'identité numérique en Allemagne. D'autres applications du secteur culture, loisir et voyages seront déployées très prochainement.

[37] Gouvernement fédéral Allemand, Digital identity ecosystem : Pilot hotel check-in project successfully launched. Mai 2021

L'intégration sécurisée des objets connectés à notre quotidien

En 2025, plus de 75 milliards d'objets intelligents et connectés auront envahi notre quotidien, nos maisons, nos villes, mais surtout nos usines.[38] **Il est critique de garantir la sécurité et la confiance dans les communications entre ces objets et le monde physique.** L'identité numérique décentralisée apporte une solution durable de standardisation, de sécurité et de confidentialité qui permet de réduire les risques de cyber attaques, de diminuer les coûts d'opération et de maintenance, mais surtout de favoriser le développement d'écosystèmes bâtis sur ces infrastructures d'objets connectées.

L'identité certifiée d'un objet est un premier élément fondamental qui peut être garanti par des attributs vérifiables relatifs à son origine, avec l'identité de son fabricant, et des informations relatives à son authenticité. **Aussi, l'identité numérique des objets permet de certifier les données relatives à leur fonctionnement, en signant électroniquement les données transmises.** Dans le secteur de l'énergie par exemple, la certification des émissions provenant des sources d'énergie renouvelable permet de garantir l'origine de l'énergie verte. De nombreuses industries bénéficieront grandement des identités numériques d'objets, comme par exemple le secteur automobile avec les véhicules autonomes, ou encore la télémédecine.

Ainsi, les cas d'usage liés à l'identité numérique décentralisée sont autant multiples qu'impactant pour la vie civile des personnes. Une grande partie de cet impact tient en ce que l'utilisation de solutions d'identité numérique décentralisée améliore considérablement la protection de la vie privée des utilisateurs.

[38] Security Today, The IoT Rundown For 2020: Stats, Risks, and Solutions. Janvier 2020.

En quoi l'identité décentralisée renforce-t-elle la protection de la vie privée ?

Archipels

En plaçant les individus au centre des données les concernant, les solutions d'identité décentralisée sont alignées avec les objectifs poursuivis par l'ensemble des législations en matière de protection des données personnelles, y compris le Règlement général sur la protection des données (RGPD).[39]

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

À ce sujet, il est particulièrement intéressant de constater que les principes fondateurs de l'identité décentralisée, tels que rédigés par Christopher Allen,[40] sont parfaitement alignés avec les principales dispositions du RGPD.

Les dix principes de l'identité décentralisée de Christopher Allen	RGPD
Existence. Les utilisateurs doivent avoir une existence indépendante	Objet et objectif du RGPD : protection des **personnes physiques** (article 2)
Contrôle. Les utilisateurs doivent contrôler leur identité	Les personnes physiques doivent avoi**r le contrôle de leurs propres données personnelles** (considérant §7)
Accès. Les utilisateurs doivent avoir accès à leurs propres données	**Droit d'accès** aux données (article 15)
Transparence. Les systèmes et les algorithmes doivent être transparents	Les données à caractère personnel sont **traitées de manière transparente** (articles 5a, 12 et 13).
Persistance. Les identités doivent avoir une longue durée de vie tout en respectant le droit à la suppression.	Articulation entre **conservation encadrée des données** (article 5e) et le **droit à l'effacement** (article 17)
Portabilité. Les informations et les services relatifs à l'identité doivent pouvoir faire l'objet d'une portabilité.	Droit à la **portabilité des données** (article 20)
Interopérabilité. Les identités doivent être aussi largement utilisables que possible	Les responsables du traitement des données sont encouragés à développer des f**ormats interopérables** qui permettent la portabilité des données (considérant §68)
Consentement. Les utilisateurs doivent consentir à l'utilisation de leur identité.	Un consentement **libre, spécifique éclairé, univoque et informée** (articles 6 & 7 + ligne directrice du CEPD)[41]
Minimisation. La divulgation des demandes doit être réduite au minimum.	Les données à caractère personnel sont **limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées (article 5c).
Protection. Les droits des utilisateurs doivent être protégés et prévaloir sur les besoins du réseau.	La protection des utilisateurs est **la raison d'être du RGPD.**

[40] ALLEN, Christopher, The Path to Self-Sovereign Identity. 2016
[41] EDPB Guidelines 05/2020 on consent under Regulation 2016/679

Identité décentralisée et RGPD promeuvent ainsi une gestion des données centrée sur l'utilisateur, et non sur la donnée en elle-même. Les solutions d'identité numérique décentralisée permettent d'ailleurs pour la première fois d'envisager un consentement véritablement granulaire des individus. Celui-ci est le corollaire de l'augmentation du contrôle de l'utilisateur qui lui permet d'empêcher un traitement automatique et incontrôlé de ses données personnelles.

L'identité décentralisée permet donc d'aller encore plus loin pour protéger les données personnelles des individus. Depuis quelques années, les professionnels de la protection de la vie privée critiquent l'approche adoptée par les législations en matière de protection des données.[42] Selon ces auteurs, si ces textes constituent une avancée fondamentale pour la protection de la vie privée des utilisateurs, ils sont encore insuffisants. Ils se focalisent en effet uniquement sur la régulation de la collecte et la conservation des données personnelles, et prévoient très peu de dispositions sur l'usage ultérieur qui sera fait de ces données. Or les plus grandes menaces sur la vie privée des individus résident bien dans l'usage et la combinaison subséquentes des données.

[42] Voir notamment : NISSENBAUM, Helen F., Deregulating Collection: Must Privacy Give Way to Use Regulation? Mai 2017 ; TENE, Omer and POLONETSKY, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 11, no. 5. 2013.

« L'ère de la big data, a rendu obsolète l'approche actuelle de la protection de la vie privée et des libertés civiles. Les lois et réglementations actuelles sont largement axées sur le contrôle de la collecte et de la conservation des données personnelles, une approche qui devient peu pratique pour les individus (...) Le temps est venu d'adopter une nouvelle approche : passer de la limitation de la collecte et de la conservation des données au contrôle des données au moment le plus important, celui de leur utilisation. »[43]

Alignée avec cette vision, la proposition de règlement EUid a pour ambition de permettre aux citoyens européens de contrôler non seulement quelles données sont communiquées mais surtout comment elles sont utilisées.[44] En régulant l'usage des données, une avancée fondamentale est ainsi réalisée au niveau européen pour la protection de la vie privée des personnes.

De manière encore plus significative, les solutions d'identité décentralisées facilitent le plein déploiement du concept de divulgation sélective. La divulgation sélective permet à un individu de partager des parties d'un ensemble de données plus important. Par exemple, un utilisateur souhaitant accéder à un site de paris sportifs en ligne n'est pas obligé de divulguer l'adresse figurant sur sa carte d'identité numérique pour prouver qu'il a plus de dix-huit ans. Il peut simplement partager sa date de naissance, et non l'intégralité du justificatif. **La proposition de règlement EUid prévoit d'ailleurs que les portefeuilles d'identité numérique doivent permettre techniquement la divulgation sélective des attributs des individus.[45]**

[43] MUNDIE, Craig, Privacy Pragmatism: Focus on Data Use, Not Data Collection,Foreign Affairs, Mars – Avril 2014.
[44] Explanatory Memorandum – Context of the Proposal. Proposal for a regulation of the European Parliament and of the Council amending Regulation EU 910/2014 (eIDAS) as regards establishing a framework for a European Digital Identity.
[45] Id. at considérant 29

Comme affirmé précédemment, les spécifications techniques des divulgations sélectives sont en cours d'élaboration dans le cadre du programme Toolbox. Il apparaît ici essentiel pour l'industrie de permettre l'utilisation de protocoles de preuve à divulgation nulle de connaissance (Zero-Knowledge Proof ou ZKP) dans l'implémentation de ces divulgations sélectives. Le ZKP permet de démontrer qu'un ensemble d'attributs satisfont à certaines caractéristiques sans avoir à divulguer la valeur de l'ensemble de ces attributs. **Ces protocoles permettent de démontrer une assertion, sans avoir à révéler les informations nécessaires à la démonstration de celle-ci.** Pour reprendre l'exemple précédent, un individu souhaitant accéder au même site de paris sportifs pourra seulement révéler l'assertion qu'il a plus de 18 ans sans pour autant révéler son âge précis.

Les protocoles ZKP apparaissent comme parmi les plus protecteurs au monde pour la protection de la vie privée des utilisateurs de services en ligne. Ils garantissent une limitation d'usage importante des attributs d'identité des personnes en allant bien au-delà du principe de minimisation des données, difficilement respecté en pratique. Il faut à ce sujet souligner que le Parlement Européen a déjà reconnu le potentiel du ZKP à résoudre le conflit entre la minimisation des données et la vérifiabilité des données entre plusieurs parties.[46] Le Parlement européen avait d'ailleurs appelé au financement de la recherche dans ce domaine en reconnaissant le fort potentiel de la technologie blockchain.[47]

[46] European Parliamentary Research Service, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? PE 634.445. Juillet 2019

[47] Parlement Européen, Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018). Novembre 2018.

Conclusion

Dans un monde où les frontières entre mondes physique et digital s'effacent de plus en plus, il est devenu indispensable de penser à de nouveaux mécanismes de gestion de l'identité numérique des personnes, des organisations et des biens. L'érosion de la confiance des individus dans les systèmes de gestion centralisés et fédérés des données personnelles justifie d'autant plus un changement de paradigme vers des architecture plaçant l'utilisateur au centre des données le concernant. **L'identité numérique décentralisée promet d'offrir aux individus de nombreux avantages sociaux, civiques et politiques tout en plaçant la protection de leur vie privée au cœur du système.** L'utilisation de la technologie blockchain, ses promesses en termes de désintermédiation, de sécurité et de résilience, scelle l'ouverture d'une ère ou l'identité numérique ne pourra prendre toute son ampleur qu'à la condition d'être décentralisée.

Auteurs

Ce document a été rédigé par Paola Heudebert, Hervé Bonazzi, Clement Bruneau et Quentin Drouot.

Archipels

À propos d'Archipels

Archipels développe le standard de l'identité décentralisée, sécurisée et vérifiée en conformité avec les normes européennes. Sa raison d'être est de permettre aux individus et aux entreprises de contrôler leurs identités numériques grâce à un premier service de certification d'attributs d'identité.

Archipels opère une infrastructure de confiance basée sur une blockchain permissionnée souveraine française. La blockchain Archipels est en effet hébergée et maintenue uniquement par des tiers de confiance Français. Eco-responsable, elle utilise l'algorithme de consensus le moins consommateur d'énergie (proof of authority) et l'ensemble des infrastructures utilisées sont bas carbone pour minimiser la consommation de ressources et maximiser l'efficience.

Archipels est une société de consortium fondée par le groupe Caisse des Dépôts, La Poste, EDF et Engie pour envisager les grands défis de demain liés à l'identité numérique des citoyens français et européens.

Archipels

Contacts

Hervé Bonazzi
Chief Executive Officer
herve@archipels.io
Linkedin

Clément Bruneau
Chief Revenue Officer
clement@archipels.io
Linkedin

Quentin Drouot
Chief Technology Officer
quentin@archipels.io
Linkedin

Paola Heudebert
Legal Operations Officer / WG Co-chair INATBA
paola@archipels.io
Linkedin

Remerciements

Les auteurs tiennent à remercier les nombreuses personnes ayant contribué à ce livre blanc par leurs conseils et commentaires :

Ignacio Alamillo Domingo, Alastria / Christine Balian, DINUM / Tim Bouma, Canada Treasury Board Secretariat / Richard Caetano, Akord / Perrine de Coëtlogon, Université de Lille / Candice Dauge, La Poste / Oskar van Deventer, NGI eSSIF-Lab / Olivier Dussutour, IN Groupe / Nadia Filali, Caisse des Dépôts / Etienne Gehain, Engie / Irene Hernández, GATACA
Luc Jarry-Lacombe, BCdiploma / Sebastian Manhart, Chancellerie Allemande / Valérie Péneau, France Identité Numérique / Olivier Senot, Docaposte / Pauline Tellier, EDF / Stergios Tsiafoulis, EU Commission / Xavier Vila Pueyo, Validated ID / Kai Wagner, Jolocom

Archipels