IdentitÃ© dÃ©centralisÃ©e

Description

La question de lâ€™identitÃ©, de lâ€™identification et de lâ€™authentification varie considÃ©rablement, dans le monde, selon la situation personnelle et gÃ©ographique de chacun. Alors que 1 milliard de personnes sont dans lâ€™incapacitÃ© de prouver leur identitÃ©, par dÃ©faillance des institutions rÃ©galiennes, le reste de lâ€™humanitÃ© semble impuissant Ã prÃ©server la sienne pour des raisons commerciales et financiÃ¨res (capitalisme de la surveillance â€“ voirÂ *La rem* nÂ°50-51, p.69 et nÂ°59, p.102), ou pour des raisons politiques et sÃ©curitaires (lutte contre le terrorisme et blanchiment de capitaux, voirÂ *La remÂ* nÂ°18-19, p.14 et nÂ°63, p.28).

Lâ€™identitÃ© numÃ©rique dÃ©signe gÃ©nÃ©ralement Â«Â *la capacitÃ© Ã utiliser de faÃ§on sÃ©curisÃ©e les attributs de son identitÃ© pour accÃ©der Ã un ensemble de ressourcesÂ* Â».Â Or, force est de constater que la sÃ©curitÃ© fait cruellement dÃ©faut aux systÃ¨mes dâ€™identitÃ© numÃ©rique en question, et quâ€™il suffit dâ€™une faille, parfois humaine, pour mettre en pÃ©ril les donnÃ©es de millions voire de milliards de personnes. Selon le site de Troy Hunt (haveibeenpwned.com), plus de 13 milliards de comptes e-mail ont Ã©tÃ© compromis depuis 2013. En janvier 2024, le chercheur en sÃ©curitÃ© Bob Dyachenko a dÃ©couvert une base de donnÃ©es en ligne de 12 tÃ©raoctets dâ€™informations, soit la compilation de 26 milliards de donnÃ©es personnelles rÃ©parties dans 3 800 dossiers â€“ chacun correspondant Ã une violation de donnÃ©es particuliÃ¨re â€“ provenant notamment de Tencent QQ, MySpace, X (ex-Twitter), Deezer, LinkedIn, AdultFriendFinder, Adobe, Dailymotion, Dropbox ou encore Telegram. Se trouvaient Ã©galement dans cette base de donnÃ©es des documents issus dâ€™organisations gouvernementales situÃ©es aux Ã‰tats-Unis, au BrÃ©sil, en Allemagne, aux Philippines, en Turquie et dans dâ€™autres pays.

RÃ©seaux sociaux, complÃ©mentaires santÃ©, banques, musique ou vidÃ©o, commerce Ã©lectronique, jeux, stockage de fichiers, livraison de repas… Ã chaque fois quâ€™une personne interagit avec un service numÃ©rique, elle crÃ©e un identifiant, fournit une adresse e-mail, parfois un numÃ©ro de tÃ©lÃ©phone, renseigne son nom et son prÃ©nom et y associe un mot de passe pour sâ€™authentifier. Selon le type de service, lâ€™internaute pourra Ãªtre amenÃ© Ã fournir dâ€™autres informations, comme une adresse postale, une date et un lieu de naissance, un numÃ©ro de sÃ©curitÃ© sociale, la copie dâ€™un passeport ou dâ€™une carte dâ€™identitÃ©, une feuille dâ€™imposition, une attestation dâ€™assurance, etc. Chaque interaction avec un nouveau service en ligne est lâ€™occasion de dissÃ©miner un peu plus ses informations personnelles. Selon une Ã©tude de NordPass, conduite en 2020 et citÃ©e par CNN, un individu possÃ©dait Ã cette Ã©poque une centaine de comptes en ligne. Seulement deux ans plus tard, une Ã©tude mondiale menÃ©e par Dashlane estime quâ€™une personne utilise dÃ©sormais 240 comptes en ligne.Â Or, il sâ€™avÃ¨re que cette maniÃ¨re de sâ€™identifier et de sâ€™authentifier en ligne est

dÃ©faillante par conception (*by design*),Â le systÃ¨me hypertexte public inventÃ© par Tim Berners-Lee et Robert Cailliau dans les annÃ©es 1990 nâ€™ayant jamais Ã©tÃ© conÃ§u pour cela.

Lâ€™identitÃ© numÃ©rique centralisÃ©e est obsolÃ¨te

Le principe selon lequel les personnes sâ€™identifient en ligne repose aujourdâ€™hui sur le fait que les services en ligne collectent les donnÃ©es personnelles de leur clients, patients, administrÃ©s, diplÃ´mÃ©s, citoyens, etc.Â Il sâ€™agit dâ€™un modÃ¨le dâ€™identitÃ© numÃ©rique dit Â« centralisÃ© Â», au sein duquel les attributs de lâ€™identitÃ© dâ€™une personne sont gÃ©rÃ©s en un point unique,Â par une entitÃ© qui en assure tout Ã la fois la collecte, la sÃ©curisation et lâ€™authentification â€“ et dont ce nâ€™est bien souvent pas le mÃ©tier. En plus dâ€™Ã©viter dâ€™utiliser le mÃªme mot de passe pour des dizaines ou des centaines de services diffÃ©rents, chacun doit, en outre, faire confiance Ã cette entitÃ© pour protÃ©ger ses informations personnelles et sâ€™assurer que son identitÃ© est utilisÃ©e de faÃ§on appropriÃ©e.

Or, ce modÃ¨le souffre dâ€™un manque de transparence, dâ€™un manque de contrÃ´le par lâ€™utilisateur, dâ€™un potentiel de surveillance de masse, et surtout des risques encourus en matiÃ¨re de confidentialitÃ© et de protection des donnÃ©es en raison dâ€™une trop grande vulnÃ©rabilitÃ©, chaque service en ligne constituant un point de dÃ©faillance. Le modÃ¨le actuel est donc devenu obsolÃ¨te. Les vols de donnÃ©es, les usurpations dâ€™identitÃ© (chaque annÃ©e, en France, prÃ¨s de 400 000 personnes en seraient victimes) et les coÃ»ts engendrÃ©s par de tels systÃ¨mes suscitent depuis longtemps lâ€™intÃ©rÃªt des ingÃ©nieurs et des cryptographes.

Vers une identitÃ© numÃ©rique dÃ©centralisÃ©e

Par opposition, lâ€™identitÃ© numÃ©rique dÃ©centralisÃ©e est un systÃ¨me qui permet Ã quiconque de stocker et de gÃ©rer personnellement les attributs de son identitÃ©, Ã©mis par des tiers (Ã©metteurs), et de les partager de maniÃ¨re autonome, sÃ©lective et parfois anonyme avec dâ€™autres tiers (vÃ©rificateurs) afin dâ€™utiliser leurs services, regagnant ainsi une forme de souverainetÃ© Ã lâ€™Ã©chelle individuelle, que la numÃ©risation de la sociÃ©tÃ© a tendance Ã avoir fait disparaÃ®tre.

Un systÃ¨me dâ€™identitÃ© numÃ©rique dÃ©centralisÃ©e, parfois appelÃ©e Â« identitÃ© auto-souveraine Â» (*self sovereign identity*) propose dâ€™inverser le modÃ¨le actuelÂ fondÃ© sur lâ€™authentification et le contrÃ´le dâ€™accÃ¨s gÃ©rÃ©s tous deux par une seule organisation, vers un modÃ¨le tripartite fondÃ© sur une collection dâ€™attestations vÃ©rifiables, constitutives de lâ€™identitÃ© numÃ©rique dâ€™une personne.

Ce concept repose sur lâ€™idÃ©e que chaque individu devrait avoir le contrÃ´le exclusif de son identitÃ© numÃ©rique, sans dÃ©pendre dâ€™une autoritÃ© centrale ou dâ€™un tiers de confiance pour sâ€™identifier ou sâ€™authentifier.

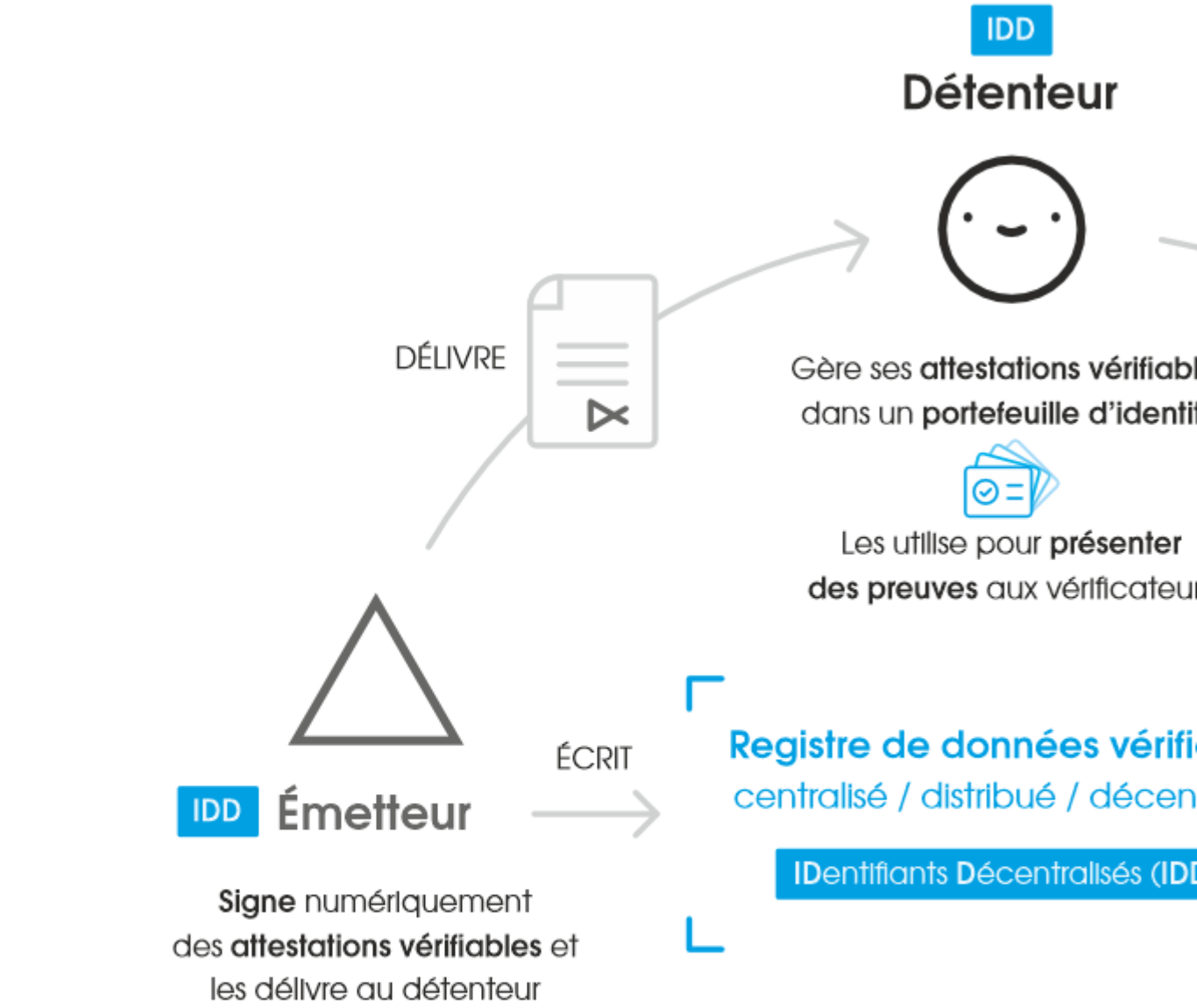
Lâ€™identitÃ© numÃ©rique dÃ©centralisÃ©e est centrÃ©e sur lâ€™individu, et se fonde sur les principes de souverainetÃ©, de portabilitÃ© et de sÃ©curitÃ©.Â Le modÃ¨le dâ€™identitÃ© dÃ©centralisÃ©e requiert dâ€™une personne quâ€™elle dÃ©tienne personnellement un logiciel appelÃ© Â« portefeuille dâ€™identitÃ© Â». Câ€™est un service numÃ©rique, une application qui permet de dÃ©tenir et de gÃ©rer un ou des Â« identifiants dÃ©centralisÃ©s Â» (DID), et de recevoir des Â« attestations vÃ©rifiables Â» (en anglaisÂ *Verifiable Credentials*, VC) associÃ©es Ã ces identifiants. Ces attestions vÃ©rifiables sont lâ€™Ã©quivalent numÃ©rique dâ€™attestations imprimÃ©es, comme un permis de conduire atteste de notre aptitude Ã conduire un vÃ©hicule ou comme un diplÃ´me universitaire atteste dâ€™un niveau dâ€™Ã©tudes.

Une attestation dite Â« vÃ©rifiable Â» fournit un mÃ©canisme en ligne, respectueux de la vie privÃ©e, permettant de reprÃ©senter cryptographiquement ces justificatifs afin quâ€™ils soient extrÃªmement complexes Ã falsifier tout en Ã©tant facilement vÃ©rifiables Ã lâ€™aide dâ€™un programme informatique.

Le modÃ¨le dâ€™identitÃ© dÃ©centralisÃ©e fait interagir trois entitÃ©s :

- le dÃ©tenteur (*holder*)Â est une entitÃ©, comme un Ã©tudiant, une personne, un employÃ©, qui acquiert, conserve, un ou plusieurs identifiants dÃ©centralisÃ©s, suivant ses besoins et les services auxquels il veut accÃ©der.
- lâ€™Ã©metteur (*issuer*)Â est une entitÃ©, comme une entre- prise, une ONG, un gouvernement, une universitÃ©, un club de pÃ©tanque, qui certifie certains champs de cette identitÃ© en signant Ã©lectroniquement les attestations vÃ©rifiables : nom, Ã¢ge, pays de naissance, avoirs bancaires, adhÃ©sion Ã jour etc. Ces champs ne sont pas nÃ©cessairement tous prÃ©sents dans un mÃªme identifiant dÃ©centralisÃ©, et une personne aura de nombreux identifiants dÃ©centralisÃ©s diffÃ©rents. Par exemple, un identifiant dÃ©centralisÃ©Â *civiqueÂ* peut encoder lâ€™Ã©tat civil dâ€™une personne, alors quâ€™un identifiant dÃ©centralisÃ©Â *bancaireÂ* pourrait encoder des informations relatives Ã un numÃ©ro de compte. Sur la base dâ€™un identifiant dÃ©centralisÃ©, son dÃ©tenteur peut gÃ©nÃ©rer une attestation vÃ©rifiable, qui est lâ€™Ã©noncÃ© dâ€™un fait portant sur un ou plusieurs champs de lâ€™identifiant dÃ©centralisÃ©, qui restent secrets. Par exemple, sur la base dâ€™un identifiant dÃ©centralisÃ©Â *civique*, une personne peut fournir un justificatif de majoritÃ© sans rÃ©vÃ©ler son Ã¢ge.Â Sur la base dâ€™un identifiant dÃ©centralisÃ©Â *bancaire*, une personne peut prouver sa solvabilitÃ© sans rÃ©vÃ©ler son nom ni le montant de son compte en banque.
- le vÃ©rificateur (*verifier*)Â est une entitÃ©, comme un employeur, les forces de lâ€™ordre ou un service. Il reÃ§oit une attestation vÃ©rifiable et la contrÃ´le suivant Â« la technique de vÃ©rification de preuves Ã divulgation nulle de connaissance Â», ZKP pourÂ *Zero Knowledge Proof*, technique cryptographique qui permet Ã une partie (le dÃ©tenteur) de prouver Ã une autre partie (le vÃ©rificateur) quâ€™elle possÃ¨de certaines caractÃ©ristiques ou quâ€™elle a effectuÃ© certaines actions, sans rÃ©vÃ©ler aucune autre information que le strict nÃ©cessaire. PlutÃ´t que

dâ€™avoir une piÃ¨ce dâ€™identitÃ© sur laquelle figurent le nom, le prÃ©nom, la date et ville de naissance, la taille, la ville de dÃ©livrance, etc., une personne gÃ©nÃ¨re et prÃ©sente une attestation vÃ©rifiable sur son Ã¢ge Ã un tiers qui, en la vÃ©rifiant, nâ€™aura accÃ¨s Ã aucune autre information que la rÃ©ponse par Â« oui Â» ou par Â« non Â» pour savoir si cette personne a plus de 18 ou de 21 ans.



Source : d'après Daniel H. Hardman, 2019, revu par Jacques-André Fines Schlumberger,

Le terme gÃ©nÃ©rique dâ€™identitÃ© dÃ©centralisÃ©e recouvre lâ€™ensemble des systÃ¨mes dâ€™identitÃ© dont le contrÃ´le ne dÃ©pend pas dâ€™une seule entitÃ©. Parmi eux, une variante met lâ€™accent sur lâ€™autonomie et sur le contrÃ´le de lâ€™utilisateur :Â lâ€™identitÃ© auto-souveraine ouÂ *self-sovereign identity*. NÃ© dans les annÃ©es 1990, ce concept est issu de la communautÃ© des cypherpunks,Â mot-valise formÃ© Ã partir deÂ *cipher*, chiffrement, et deÂ *cyberpunk*, un genre de science-fiction portÃ© sur les technologies de lâ€™information et leur impact sur la sociÃ©tÃ©. Les cypherpunks prÃ´nent la cryptographie forte et lâ€™utilisation de technologies dÃ©centralisÃ©es afin de protÃ©ger les libertÃ©s fondamentales que sont le droit Ã la vie privÃ©e et le droit Ã lâ€™anonymat, notamment face Ã lâ€™intrusion et Ã la surveillance des communications privÃ©es opÃ©rÃ©es par les gouvernements et par les entreprises.

Parmi les grandes figures de cette communautÃ© se trouvent Timothy C. May, auteur du Â« Crypto Anarchist Manifesto Â» en 1988, Eric Hughes, auteur du Â« Cypherpunk's Manifesto Â» en 1993, Phil Zimmermann, cryptographe amÃ©ricain, crÃ©ateur du logiciel de chiffrement Pretty Good Privacy (PGP) en 1991, Julian Assange, cofondateur de WikiLeaks en 2006 ou encore Hal Finney, ingÃ©nieur logiciel et cryptographe amÃ©ricain, lâ€™un des premiers dÃ©veloppeurs informatiques du protocole Bitcoin. Leur mouvement travaille Ã la sÃ©curisation des communications Ã©lectroniques, Ã lâ€™invention de systÃ¨mes de communication anonyme, Ã la mise en Å“uvre des signatures numÃ©riques ou au dÃ©veloppement de logiciels de chiffrement.

Dans les annÃ©es 2010, lâ€™identitÃ© auto-souveraine a gagnÃ© en popularitÃ©, avec lâ€™Ã©mergence des registres distribuÃ©s de type blockchain (voir *La rem* nÂ°44, p.97), aÌ€ lâ€™origine de lâ€™infrastructure dÃ©centralisÃ©e, qui a permis sa mise en Å“uvre. Les 21 et 22 mai 2015, lors de lâ€™IEEE Symposium on Security and Privacy Workshops (SPW), important Ã©vÃ©nement organisÃ© chaque annÃ©e par lâ€™Institute of Electrical and Electronics Engineers (IEEE), Guy Zyskind, Oz Nathan et Alex Â« Sandy Â» Pentland prÃ©sentent une mÃ©thode inspirÃ©e de Bitcoin et des blockchains dans une proposition intitulÃ©e Â« *Decentralizing Privacy: Using Blockchain to Protect Personal Data* Â» et selon laquelle Â« *les donnÃ©es personnelles, et les donnÃ©es sensibles en gÃ©nÃ©ral, ne devraient pas Ãªtre confiÃ©es aÌ€ des tiers, car elles sont susceptibles d'Ãªtre attaquÃ©es et utilisÃ©es aÌ€ mauvais escient. Au contraire, les utilisateurs devraient possÃ©der et contrÃ´ler leurs donnÃ©es sans compromettre la sÃ©curitÃ© ou limiter la capacitÃ© des entreprises et des autoritÃ©s aÌ€ fournir des services personnalisÃ©s* Â».

Des standards mondiaux et open source

Cette idÃ©e de mettre en Å“uvre un protocole qui transforme une blockchain en un gestionnaire dâ€™accÃ¨s automatisÃ© ne nÃ©cessitant pas de tiers de confiance, tout en garantissant aux utilisateurs de possÃ©der, maÃ®triser et contrÃ´ler leurs donnÃ©es, va progressivement faire lâ€™objet dâ€™une mobilisation mondiale rÃ©unissant des dÃ©veloppeurs, des chercheurs, des designers, des militants, des artistes et des citoyens Ã©clairÃ©s. Il sâ€™agit ni plus ni moins de repenser la maniÃ¨re dont la confiance

est Ã©tablie et vÃ©rifiÃ©e sur internet. Cette mobilisation sâ€™est faite notamment au sein de la Decentralized Identity Foundation (DIF), organisation aÌ€ but non lucratif fondÃ©e en 2016, par le biais dâ€™Ã©vÃ¨nements et dâ€™ateliers appelÃ©s Â« Rebooting the Web of Trust Â» initiÃ©s dÃ¨s 2017, et avec la Trust over IP Foundation (ToIP), organisation aÌ€ but non lucratif crÃ©Ã©e en 2019.

Le 29 avril 2016, Christopher Allen, cryptographe et cypherpunk de renommÃ©e mondiale, publie lâ€™article Â« *The Path to Self-Sovereign Identity* Â» et dÃ©taille les dix principes fondamentaux de lâ€™identitÃ© dÃ©centralisÃ©e, qui influenceront profondÃ©ment le dÃ©veloppement de projets et dâ€™initiatives en la matiÃ¨re. Â« *Les utilisateurs doivent avoir une (1) existence indÃ©pendante qui nâ€™est pas contrÃ´lÃ©e par une seule entitÃ©. Les utilisateurs doivent avoir le (2) contrÃ´le sur leur propre identitÃ© et leurs donnÃ©es personnelles. Les utilisateurs doivent avoir (3) accÃ¨s aÌ€ leur propre identitÃ© et aÌ€ leurs donnÃ©es personnelles. Les systÃ¨mes dâ€™identitÃ© doivent Ãªtre (4) transparents et comprÃ©hensibles pour les utilisateurs. Les identitÃ©s doivent Ãªtre (5) persistantes et durables dans le temps. Les utilisateurs doivent pouvoir (6) emporter leur identitÃ© et leurs donnÃ©es personnelles avec eux lorsquâ€™ils changent de fournisseur de services. Les systÃ¨mes dâ€™identitÃ© doivent Ãªtre (7) interopÃ©rables et fonctionner ensemble de maniÃ¨re transparente. Les utilisateurs doivent donner leur (8) consentement Ã©clairÃ© avant que leurs donnÃ©es personnelles ne soient partagÃ©es ou utilisÃ©es. Les systÃ¨mes dâ€™identitÃ© doivent (9) minimiser la collecte et le stockage de donnÃ©es personnelles. Les systÃ¨mes dâ€™identitÃ© doivent (10) protÃ©ger les donnÃ©es personnelles des utilisateurs contre les violations de donnÃ©es et les utilisations abusives.* Â»

En juin 2019, le W3C, organisme de standardisation Ã but non lucratif assurant la compatibilitÃ© des techno- logies du World Wide Web, publie la spÃ©cification Â« Decentralized Identifiers (DIDs) v1.0 Â» en tant que recommandation, mise Ã jour le 19 juillet 2022. Elle dÃ©finit un modÃ¨le de donnÃ©es et une syntaxe pour les identifiants dÃ©centralisÃ©s, des identifiants uniques et persistants pour les entitÃ©s (personnes, organisations, objets, etc.) qui ne dÃ©pendent pas dâ€™une autoritÃ© centrale. Quiconque a dÃ©jÃ tapÃ© lâ€™adresse dâ€™un site web dans un navigateur web reconnaÃ®t le principe de Â« http Â», qui veut direÂ *HyperText Transfer Protocol*. Â« http Â» est le schÃ©ma dâ€™URI â€“ (*Uniform Resource Identifier*), le format dâ€™identifiant standard pour toutes les ressources accessibles sur le World Wide Web, des URL,Â *Uniform Ressource Locator*, qui indique la localisation dâ€™une ressource sur le web : Â« DID Â» pourÂ *Decentralized IDentifiersÂ* est, de maniÃ¨re similaire, le schÃ©ma dâ€™un format dâ€™identifiant standard pour des Â« identifiants dÃ©centralisÃ©s Â» qui peuvent dÃ©signer des personnes, des choses, des objets ou nâ€™importe quelle autre entitÃ©. ConcrÃ¨tement, câ€™est une chaÃ®ne de textes et de nombres composÃ©e de trois parties : lâ€™identifiant du schÃ©ma URL de lâ€™identifiant dÃ©centralisÃ© (DID), lâ€™identifiant de la mÃ©thode de lâ€™identifiant dÃ©centralisÃ© et enfin, lâ€™identifiant dÃ©centralisÃ©, lui-mÃªme.

Ces identifiants dÃ©centralisÃ©s sont un nouveau type dâ€™identifiant, qui permettent de mettre en Å“uvre une identitÃ© numÃ©rique vÃ©rifiable et dÃ©centralisÃ©e.

Un identifiant dÃ©centralisÃ© peut donc Ãªtre vu comme un lien qui pointe vers un document complet contenant les champs de lâ€™identifiant dÃ©centralisÃ© cryptographiquement protÃ©gÃ©. Ce document est stockÃ© dans un registre de donnÃ©es vÃ©rifiables (*Verifiable Data Registry*) dont la nature peut varier, entre un registre centralisÃ©, distribuÃ© ou dÃ©centralisÃ©. Comme nous avons aujourdâ€™hui des centaines de logins et de mots de passe, nous aurons probablement Ã lâ€™avenir des centaines voire des milliers dâ€™identifiants dÃ©centralisÃ©s. Chacun dâ€™entre eux nous donnera un canal privÃ© cryptÃ© avec une autre personne, une organisation ou un objet. Il nâ€™y aura pas dâ€™autoritÃ© centrale dâ€™enregistrement ; chaque identifiant dÃ©centra- lisÃ© Ã©tant enregistrÃ© directement par une personne, idÃ©alement sur une blockchain publique afin que le registre de donnÃ©es vÃ©rifiables soit le moins corruptible possible.

Ã€ partir de ses identifiants dÃ©centralisÃ©s, stockÃ©s dans un portefeuille dâ€™identitÃ©, unepersonne prouve,Â Ã lâ€™aide dâ€™attestations vÃ©rifiables quâ€™il sÃ©lectionne,Â ce quâ€™ilsaitÂ (comme un diplÃ´me, une autorisation dâ€™exercer un mÃ©tier, une certification),Â ce quâ€™ilaÂ (comme un compte bancaire, sa solvabilitÃ©, une citoyennetÃ©),Â ce quâ€™il possÃ¨deÂ (comme unterrain, une rÃ©sidence, un vÃ©hicule),Â qui il estÂ (comme sa taille, son poids, son Ã¢ge),Â ce quâ€™il faitÂ (comme un emploi, passÃ© ou prÃ©sent),Â oÃ¹ il est allÃ©Â (comme sa participation Ã un Ã©vÃ¨nement, sâ€™il a Ã©tÃ© ou non vaccinÃ© contre le Covid- 19, etc.). Cependant, il nâ€™envoie plus la copie dâ€™un diplÃ´me, dâ€™un passeport, dâ€™un justificatif de revenus, dâ€™un titre de propriÃ©tÃ©, dâ€™une carte grise, dâ€™une attestation dâ€™employeur… autant de donnÃ©es personnelles dissÃ©minÃ©es de faÃ§on hasardeuse. En revanche, il dispose de lâ€™ensemble de ses identifiants dÃ©centralisÃ©s dans un porte- feuille dâ€™identitÃ©, comme autant dâ€™attributs propres Ã son identitÃ© numÃ©rique, Ã partir desquels il gÃ©nÃ¨re, de maniÃ¨re sÃ©lective et temporelle, des attestations vÃ©rifiables afin de les prÃ©senter Ã des acteurs identifiÃ©s qui en vÃ©rifieront, cryptographiquement, la vÃ©racitÃ©.

Le concept dâ€™identitÃ© renvoie Ã une double reconnaissance, Ã la fois de soi-mÃªme et par les autres. Ãštre au monde et faire sociÃ©tÃ© ne se recouvrent pas forcÃ©ment : les Nations Unies parlent des Â«Â *invisiblesÂ* Â» et un rapport de lâ€™Unicef de 2023 indique quâ€™Â«Â *un enfant sur quatre de moins de cinq ans nâ€™existe pas oï¬ƒciellementÂ* Â».Â Et pourtant, Ãªtre en mesure de prouver son identitÃ©, câ€™est accÃ©der Ã Â«Â *la capacitÃ© dâ€™entrer en relationÂ* Â».Â Les systÃ¨mes dâ€™identitÃ© dÃ©centralisÃ©e sont extrÃªmement immatures et dÃ©ployÃ©s nulle part Ã grande Ã©chelle. MÃªme sâ€™il existe des normes communes, la diversitÃ© des mÃ©thodes empÃªche actuellement leur interopÃ©rabilitÃ©, ce qui freine leur adoption, qui, pour Ãªtre efficace, devrait faire lâ€™objet dâ€™une appropriation massive tout Ã la fois par les individus, les entreprises et les gouvernements. Or, il nâ€™en est rien. La pÃ©rennitÃ© des infrastructures sous-jacentes, telles que les registres distribuÃ©s, est Ã©galement essentielle pour garantir la disponibilitÃ© et la fiabilitÃ© des modÃ¨les dâ€™identitÃ© dÃ©centralisÃ©e.

Il existe dâ€™innombrables questions dont la plupart sont sans rÃ©ponse Ã ce jour. En revanche, ces systÃ¨mes sont infiniment moins coÃ»teux Ã dÃ©ployer, bien plus sÃ©curisÃ©s que les systÃ¨mes dâ€™identitÃ© centralisÃ©e traditionnels. Ils sont les seuls Ã proposer le regain dâ€™une souverainetÃ© numÃ©rique Ã lâ€™Ã©chelle individuelle.Â Tout le monde et le monde entier y gagneraient, sauf ceux dont le modÃ¨le dâ€™affaires repose sur le commerce des donnÃ©es personnelles.

Sources :

- Allen Christopher, Â« The Path to Self-Sovereign Identity Â», lifewithalacrity.com, April 26, 2016.
- Hennion Christine, Mis Jean-Michel, Â« Mission dâ€™information commune sur lâ€™identitÃ© numÃ©rique Â», rapport nÂ° 3190, AssemblÃ©e nationale, 8 juillet 2020.
- Â« Verifiable Credentials Data Model v1.1 Â», W3C Recommendation, w3.org, March 3, 2022.
- Â« Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations Â»,

W3C Recommendation, w3.org, July 19, 2022.
- Â« A look at Password Health Scores around the world in 2022 Â», dashlane.com
- Villeroy de Galhau FranÃ§ois, Â« Observatoire de la sÃ©curitÃ© des moyens de paiement â€“ Rapport annuel 2021 Â», Banque de France, juillet 2022.
- Fines Schlumberger Jacques-AndrÃ©, Â« Rapport Blockchains & dÃ©veloppement durable Â», association de loi 1901 Blockchain for Good, septembre 2022.
- Â« Censuses and vital registration systems, 2013-2022 Â», Unicef, mics.unicef.org/surveys, 2023.
- Murphy Kelly Samantha, Â« We each have an average of 100 online accounts. Hereâ€™s how to make sure they arenâ€™t a nightmare for your family if you die Â», CNN, edition.cnn.com, March 1st, 2024.

Categorie

1. A retenir

date crÃ©Ã©e
11 juillet 2024
Auteur
jacquesandrefines