Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique

Thibault Langlois-Berthelot

Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique

Article rédigé par Thibault LANGLOIS-BERTHELOT pour le compte de la société IN Groupe.
Voir la version francophone ou anglophone sur le site officiel.

L'identité décentralisée et la technologie blockchain proposent une redéfinition technique et conceptuelle de l'identité numérique : quelles définitions, progrès et défis face à l'émergence d'une identité numérique décentralisée ?

Aujourd'hui, la notion d'identité n'a jamais été aussi centrale dans nos sociétés. Pourtant, un milliard de personnes ne peuvent toujours pas prouver leur existence légale[1].

Depuis l'avènement d'internet, jusqu'à ses nouvelles technologies et applications, notre identité physique et traditionnelle se transforme. Plus précisément, elle se transpose et se renouvelle depuis l'univers physique vers celui numérique. Historiquement matérialisée par des titres d'identité physiques, elle se connecte et se digitalise face aux nouveaux usages et comportements informatiques : les titres d'identité deviennent digitaux et font naître une identité numérique régalienne.

Aujourd'hui, l'identité numérique semble plus que jamais sans frontières. Nos usages et nos comportements digitaux s'accroissent et se développent rapidement (réseaux sociaux, applications mobiles, sites intranet/internet, objets connectés). Si l'identité numérique est un progrès sans précédent pour nos sociétés, sa gestion par une poignée d'acteurs - bien souvent privés (GAFAM, BATX)[2] - soulève de nombreuses questions techniques, économiques, juridiques et politiques.

L'identité décentralisée : un changement de paradigme conceptuel et technique

L'identité d'une personne renvoie à tous les attributs susceptibles de la caractériser par rapport à d'autres personnes. Dès lors, notre identité personnelle se compose d'une infinité d'attributs personnels fixes (couleur de nos yeux), variables (couleur des cheveux), mais aussi racines (nom et prénom légaux) et étendus (diplômes).

Dans le cadre de nos identités numériques actuelles, ces innombrables attributs et données d'identité sont généralement sous le contrôle d'organisations et de serveurs externes aux individus auxquels ils se réfèrent. Ainsi, l'identité numérique soulève régulièrement diverses problématiques : elle est fragmentée entre diverses organisations (bien souvent privées), peu interopérable et accessible, onéreuse et complexe à sécuriser. Dans certains cas, sa gestion est opaque, au détriment des utilisateurs et de leurs données personnelles qui sont commercialisées en toute impunité.

Pour faire face à ces limites, l'identité décentralisée[3] donne aux utilisateurs le contrôle sur l'utilisation et l'échange de leurs données : elle propose une réinvention sans précédent de la manière de concevoir, de générer et d'exploiter l'identité numérique des personnes.

Techniquement, un modèle d'identité décentralisée[4] propose à l'utilisateur de reprendre le contrôle sur sa propre identité en créant un ou plusieurs identifiants uniques nommés des identifiants décentralisés[5], auxquels il va associer ses attestations d'identité vérifiables aussi nommés « verifiable credentials (VCs) »[6].

Thibault LANGLOIS-BERTHELOT
Doctorant en droit à l'EHESS

Concrètement, les personnes utilisent des attestations au quotidien pour prouver qu'elles sont bien qui elles prétendent être : passeports, permis de conduire, certifications et diplômes, cartes d'assurance, attestation médicales, etc. De manière générale, ces attestations et preuves d'identité sont en format plastique ou en papier.

Par analogie, ces attestations physiques deviennent des attestations vérifiables (VCs), dès lors qu'elles sont dans un format numérique standardisé, et directement sauvegardé dans le téléphone de l'utilisateur et/ou parfois dans un cloud souverain. Ainsi, les attestations vérifiables sont des certificats numériques standardisés qui facilitent l'échange et le partage d'informations en ligne, de manière souveraine et sécurisée. Le terme de « standardisation » indique qu'il existe une méthode conforme pour programmer informatiquement une attestation vérifiable (VC). Cette méthode est actuellement en cours de normalisation par le World Wide Web Consortium[7].

En associant des attestations vérifiables provenant d'autorités reconnues, comme par exemple des gouvernements ou des sociétés, les utilisateurs peuvent créer des homologues numériques[8] qui prolongent leurs attestations physiques : une carte nationale d'identité devient alors un « jumeau numérique » tout aussi recevable que sa version physique et officielle. Une fois générées, les attestations vérifiables d'une personne peuvent être partagées par l'utilisateur - par email, SMS, QR code - à tous tiers afin de leur prouver certaines informations racines ou étendues rattachées à leur identité.

Ici, la cryptographie mêlée à de nouveaux standards en cours de développement, joue un rôle central dans la réalisation technique d'une identité décentralisée. En effet, ses implémentations utilisent des preuves cryptographiques (des « empreintes numériques infalsifiables »), afin de fournir une certitude mathématique du lien entre une personne et ses données à caractère personnel.

Cependant, l'identité décentralisée ne requiert pas nécessairement - comme infrastructure numérique sous-jacente - une blockchain (c'est-à-dire un registre électronique décentralisé)[9]. En effet, les standards techniques utilisés par l'identité décentralisée permettent d'offrir, à tous types d'entités (comme des personnes, des objets connectés), des attestations vérifiables autonomes et partageables quel que soit le registre numérique sur lequel elles évoluent (serveurs centralisés, distribués ou décentralisés).

Toutefois, force est de constater que le binôme entre ces nouveaux standards du W3C et la technologie blockchain, est incontestablement judicieux. Par voie de conséquence, les avantages intrinsèques[10] qu'offre une infrastructure blockchain décentralisée se transposent naturellement à ces standards, dès lors qu'ils reposent sur cette dernière. De fait, de nombreux projets d'identité décentralisée recourent aujourd'hui à la technologie blockchain.

Une identité numérique « augmentée », un nouveau champ des possibles

Les apports de l'identité décentralisée en comparaison aux méthodes et techniques conventionnelles de management de l'identité sont nombreux.

Pour les utilisateurs :

Avec l'identité décentralisée, l'identité numérique devient davantage accessible et facile d'utilisation. Une fois déployée, une attestation vérifiable peut être facilement partagée entre différents services internet afin de s'authentifier : les utilisateurs n'ont plus besoin de mot de passe pour chaque service et l'identité devient consentie, portable et interopérable d'un service numérique à l'autre.

De nombreux services et applications traditionnels peuvent se connecter à ce système décentralisé pour solliciter la permission d'accéder à l'identité des utilisateurs. Ainsi, il est à l'unique discrétion des utilisateurs d'accepter de partager certaines informations souhaitées ou encore de choisir quand attribuer ou révoquer l'accès à leurs données (VCs) par des tiers.

De par sa conception - par essence respectueuse de la vie privée et des données personnelles[11] - l'identité décentralisée rend moins probable l'agrégation des données ou encore les abus de confidentialité des utilisateurs, par des services et tiers numériques.

L'identité décentralisée est plus sécurisée que l'identité numérique centralisée puisque l'utilisateur contrôle seul l'accès et le partage de ses attributs d'identité. L'identité devient plus complexe à usurper, une aubaine pour 8 pourcent des Français qui déclarent avoir été victimes d'usurpation d'identité au cours des dix dernières années[12].

Pour les organisations :

Un système d'identité décentralisée confère une sécurité ainsi qu'une fiabilité cryptographique aux données stockées et à leurs interactions entre différentes entités : cela permet une traçabilité technique, en temps réel ou a posteriori, des actes et des responsabilités.

Par exemple, en cas d'injustices ou de « censures numériques » sans motifs légitimes par un service en ligne (comme un réseau social), ces actes non motivés (concurrence déloyale, censures, fermetures de comptes professionnels injustifiées) seraient aisément et techniquement retraçables puis démontrables par les utilisateurs ou entreprises, un élément qui faciliterait d'éventuelles poursuites judiciaires : le droit deviendrait « augmenté » par cette nouvelle confiance et efficience numérique.

Avec l'identité décentralisée, chacune des interactions se fonde sur une preuve cryptographique uniques stockée dans un système distribué et/ou décentralisé, luimême résiliant par nature. De cette façon, certains des coûts d'infrastructures sont partagés entre les entreprises, les institutions publiques et toutes autres organisations parties prenantes à l'infrastructure – bien souvent blockchain – sous-jacente et commune.

Par conséquent, une nouvelle ère de collaboration se dessine pour les organisations : ces dernières peuvent bénéficier d'une même infrastructure technique, tout en développant des applications privées et souveraines sur cette dernière. La « collaboration en silo » disparaît au profit d'utilisateurs qui contrôlent leurs données, leurs identifiants et leurs attestations vérifiables. Du reste, puisque l'utilisateur gère théoriquement seul son identité, il en devient ainsi responsable, sans que cette responsabilité n'incombe au fournisseur d'identité, comme actuellement.

En fin de compte, le champ d'application de l'identité décentralisée est proportionnel aux besoins des secteurs qui requièrent l'identification systématique de leurs utilisateurs. En d'autres termes, il est presque infini : secteur bancaire (processus KYC), secteur des assurances (attestations de sinistres), secteur privé (digitalisation des cartes professionnelles), secteur public (digitalisation des permis de conduire, des passeports), secteur éducatif (diplômes, attestations de stage), secteur de la santé (attestation de vaccination), et bien d'autres à venir.

Une nouvelle technologie en devenir

En théorie, l'identité décentralisée permettrait à ses utilisateurs, non seulement de devenir « maître » de leur identité numérique, mais aussi peut-être par extension, de devenir maître de leurs *destins numériques*. Parallèlement, ce nouveau modèle d'identité augmentée, basée sur la confiance numérique, représente une nouvelle opportunité pour les entreprises, les États et plus généralement toutes autres entités évoluant dans l'univers digital.

Dans les faits, l'identité décentralisée restera, à moyen terme, hybride (centralisée et décentralisée). En effet, pour prétendre un jour à une adoption massive, elle devra faire naître une unanimité technique, économique, politique et juridique.

D'ici quelques décennies, une identité libre, autonome et fondée sur *« le droit d'être soi »*[9], pourrait bien dépasser la réalité de l'identité numérique imparfaite que nous portons aujourd'hui.

Notes

1 Desai, V. T., Diofasi, A., Lu, J. (2018, 25 avril). The global identification challenge, (The global identification challenge: Who are the 1 billion people without proof of identity?)

2 GAFAM est l'acronyme des cinq plus grandes entreprises du Web américain — Google, Apple, Facebook, Amazon et Microsoft — qui dominent le marché numérique mondial tout en proposant des systèmes d'identification numériques à leurs utilisateurs. BATX est l'acronyme de Baidu, Alibaba, Tencent, Xiaomi, les quatre plus grandes entreprises technologiques de Chine.

3 Traduit du terme anglais « Decentralized Identity ». Cependant, les auteurs français ne s'accordent pas encore sur un terme univoque, sa traduction est donc plurielle : identité distribuée, identité décentralisée, identité désintermédiée, etc.

4 Comme pour toutes les nouvelles technologies, les approches techniques, les terminologies et les courants philosophiques sont nombreux et évolutifs. L'identité décentralisée n'échappe pas à cette règle : certains auteurs distinguent les notions d'identité décentralisée et « d'identité en propre », plus connue sous l'appellation « d'identité auto souveraine ». L'identité en propre propose un nouvel agencement informatique dans lequel l'utilisateur est pleinement souverain - depuis la création en ligne de ses attributs d'identité jusqu'à leur partage à des tiers – sur le cycle de vie et la gestion de son identité numérique. Elle offre un degré de contrôle par l'utilisateur qui va plus loin que la notion générique « d'identité décentralisée ». S'il est convenu que l'identité en propre constitue nécessairement une identité décentralisée, l'identité décentralisée ne constitue pas systématiquement une identité en propre. Pour plus de simplicité, la majorité des auteurs regroupe ces deux termes sous la même notion « d'identité décentralisée », que nous privilégierons dans cet article.

5 Traduit du terme anglais des « Decentralized Identifers (DIDs) » qui représente « Des identifiants permanents, uniques, qui ne nécessitent pas d'autorité d'enregistrement centralisée et qui sont souvent générés et/ou enregistrés de manière cryptographique. De nombreuses méthodes de DID, mais pas toutes, utilisent la technologie blockchain (DEEP) ou d'autres types de réseaux décentralisés/distribués. ». Source : (https://www.w3.org/TR/did-core/terminology)

6 Les attestations vérifiables possèdent un standard défini par le World Wide Web Consortium

7 Le W3C représente l'un des principaux organismes de normalisation de l'Internet : (https://www.w3.org/)

8 Si l'intégrité des informations d'une attestation vérifiable peuvent être simplement vérifiées, leurs véracités ne peuvent l'être. De ce fait, bien que le vérificateur soit obligé de faire confiance à l'émetteur de l'attestation, il n'a pas besoin de le contacter directement pour vérifier les informations, dès lors qu'il lui fait confiance.

9 Cf. article explicatif sur la technologie blockchain, Thibault Langlois-Berthelot : La blockchain, un nouveau fondement pour la confiance numérique ? (Observatoire d'IN Groupe, 2021, pp.5.)

10 Il est fait référence aux caractéristiques/avantages issus de la technologie blockchain : immuabilité, rapidité, sécurité, accessibilité, pseudonymat des transactions du registre.

11 Les standards techniques du W3C se fondent sur les « *10 principes de l'identité auto souveraine* » énoncée en 2016 par Christopher Allen sur son blog personnel : « *Existence, Contrôle, Accès, Transparence, Pérennité Portabilité, Interopérabilité, Consentement, Minimisation, Protection* ». *(http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html)*

12 CSA, Les Français et la criminalité identitaire, sondage, Fellowes, oct. 2012, page 4.

9 Cf. vidéo de présentation sur la chaîne Youtube de la société IN Groupe : « Le droit d'être soi »