Proposition d'une taxonomie francophone pour l'identité décentralisée

Thibault Langlois-Berthelot

Proposition d'une taxonomie francophone pour l'identité décentralisée

« Ce que l'on conçoit bien s'énonce clairement, et les mots pour le dire arrivent aisément »[1].

L'identité décentralisée est un concept technologique récent dont les contours et significations demeurent encore abstraits au regard de son adoption et expansion actuelle. Cet article a pour objet, d'une part, d'identifier les difficultés de traduction et d'interprétation de ce nouveau concept **(I)**, et d'autre part, d'y consacrer une première ébauche de taxonomie francophone **(II)**. Dans quelles mesures une taxonomie francophone pour l'identité décentralisée est-elle nécessaire et bénéfique à son adoption ?

L'émergence de nouvelles technologies entraîne fréquemment certaines difficultés de traduction, et en définitive, d'interprétation des idées et des concepts adjacents. L'objet de cet article est précisément de proposer une base d'interprétation et de perception intelligible et commune, pour l'identité décentralisée. Il s'agit d'étudier puis de constituer les fondements d'un vocabulaire minimum qui favorisera la compréhension et l'adoption de ce nouveau modèle d'identité numérique. De fait, tant le développement conceptuel que commercial de l'identité décentralisée, nécessitent une ossature de traduction minimale afin d'aborder sereinement ces concepts innovants.

Pour rappel[2], l'identité numérique décentralisée représente une nouvelle méthode de gestion de l'identité numérique des personnes. Elle se focalise sur les droits numériques de ces dernières et reflète davantage la gestion quotidienne et physique de leur identité. Elle permet « d'augmenter »[3] leurs actes et consentements quotidiens tout en respectant par conception leur vie privée et leurs libertés individuelles. Surtout, elle simplifie l'accessibilité et l'utilisation des services numériques (plateformes et commerces en ligne, réseaux sociaux, blogs et messageries, service public en ligne, etc.) pour ses utilisateurs, et contribue directement à un internet plus libre et respecteux de ses internautes.

En pratique, cette identité numérique 3.0 suppose l'utilisation d'un portefeuille d'identité numérique décentralisée. Cela représente l'équivalent numérique d'un portefeuille classique, à la différence qu'il permet d'interagir en toute confiance au sein de la sphère digitale. Parfois surnommé « mallette d'identité numérique », il s'agit d'une application pour smartphone dans laquelle chaque utilisateur peut conserver numériquement, et en toute assurance grâce à la technologie blockchain[4], les justificatifs de son quotidien : cartes de fidélité, permis de conduire, carte nationale d'identité (CNI), cartes bancaires, certificats et/ou diplômes, cartes de fidélité, entre autres.

Dans cette application mobile ou web, chaque interaction et partage d'informations peut théoriquement être contrôlé (totalement ou partiellement) par l'utilisateur. Lorsqu'un utilisateur souhaite se connecter à un service internet, le stockage et partage sécurisés et décentralisés de ses preuves de justificatifs, permettent un partage en ligne sélectif et optimum de ses attributs d'identité. Cette interaction et connexion d'un nouveau type (pair à pair et sans tiers de confiance) ne nécessite plus de procéder à de multiples inscriptions : les frictions traditionnellement imposées à l'utilisateur sur internet (en recourant à de multiples comptes, identifiants et mots de passe), se dissipent. Les mots de passes sont substitués par le partage de preuves numériques (cryptographiques) fiables et infalsifiables. Dès lors, de nombreuses démarches numériques (publiques ou privées) peuvent être effectuées avec un niveau de confiance et de transparence équivalent à une vérification d'identité en présentiel[5].

Thibault LANGLOIS-BERTHELOT
Doctorant en droit à l'EHESS

I/ Le besoin d'une taxonomie, face à de multiples définitions et interprétations

Evoquée pour la première fois par la formulation « Sovereign Source of Authority » en 2012[6], l'identité décentralisée connaît une accélération majeure de son attrait et de son adoption depuis 2017[7].

Néanmoins, étant donné la législation en vigeur et prospective concernant son marché (primaire) de l'identité numérique[8], les experts qui gravitent autour de l'identité décentralisée sont confrontés, à court terme, à certaines difficultés de traduction. Par voie de conséquence, ces difficultés d'expression se transforment en difficultés de compréhension du sujet. En définitive, un modèle dont la qualification est trop vague peine à s'imposer, c'est-à-dire à être adopté.

Victime de son succès, ce nouveau paradigme doit trouver une certaine stabilité et récurrence lors de sa mobilisation par les acteurs francophones de ce marché en cours de structuration. A cet effet, nous proposerons quelques premières[9] recommandations de traduction dans la **Table 1**.

Comme pour toute technologie novatrice, les approches techniques, terminologiques, voire philosophiques, sont nombreuses et évolutives. La notion d'identité décentralisée n'échappe pas à ce principe : certains auteurs distinguent les notions « d'identité décentralisée » et « d'identité auto-souveraine », respectivement traduit de l'anglais « decentralized identity » et « self sovereign identity (SSI) »[10].

Selon le rapport « Blockchain and Digital Identity »[11], les termes d'identité décentralisée et d'identité auto-souveraine diffèrent en matière de degré de contrôle par l'utilisateur : *« Il est possible d'aller plus loin dans la décentralisation de l'identité en donnant aux utilisateurs le contrôle non seulement de leurs identifiants mais aussi des données qui leur sont associées. C'est le cœur de ce que l'on appelle la self sovereign identity (SSI) »*. Ainsi, une distinction de fond et de forme est effectuée dans ce rapport officiel, qui constitue ainsi un point de départ pertinent dans cette analyse. D'autres chercheurs tendent à confirmer cette hypothèse de différenciation de degré : *« L'identité auto-souveraine (SSI) est un nom contesté qui est souvent utilisé pour promouvoir divers projets d'identité numérique décentralisée. »*[12].

Bien qu'une majorité des chercheurs recourent massivement à l'acronyme « SSI » pour désigner le concept d'identité décentralisée, son utilisation n'est pas idéal. En effet, il est déjà largement utilisé dans le secteur informatique francophone pour désigner la « sécurité des systèmes d'information (SSI) ».

Désormais, il s'agit de déterminer quels sont les concepts fondateurs que toute personne doit nécessairement mobiliser et évoquer pour aborder la notion d'identité décentralisée. Ces derniers sont au nombre de six :

(a) l'expression générique « decentralized identity » qui permet d'introduire *in globo* ce concept, **(b)** la formulation « self sovereign identity » qui désigne son application théorique et strictement centrée sur l'utilisateur (avec un total contrôle des utilisateurs sur leur identité), **(c)** les termes de « decentralized identifier(s) - DID » et **(d)** « verifiable(s) credential(s) – VC » qui permettent d'évoquer les standards cryptographiques à la base des échanges et de l'interropérabilité desdits attributs d'identité évoqués, **(e)** et enfin, les termes « blockchain technology(ies) » et **(f)** « Digital Wallet » qui représentent respectivement, (e) les piliers techniques qui permettent - aux fournisseurs d'identité, utilisateurs et/ou services en ligne - d'enregistrer et d'horodater des preuves numériques d'attributs d'identité au sein d'une blockchain, puis (f), d'intéragir (c'est-à-dire d'émettre, partager, révoquer) ces preuves (via un Digital wallet).

II/ Proposition résumée d'une taxonomie pour l'identité décentralisée

Selon leurs sens et finalités, plusieurs traductions francophones peuvent être dérivées de ces termes anglophones[13]. A l'heure actuelle, les auteurs français et anglais ne s'accordent pas encore sur un terme univoque[14] pour mentionner le concept d'identité décentralisée. Ainsi, la traduction de ses composantes est plurielle, tant en anglais qu'en français (Cf. **Table 1**) : « identité décentralisée » pour « decentralized identity », « identité auto-souveraine, identité en propre, […] auto-portée, […] auto administrée » pour « Self Sovereign Identity », etc.

Cette richesse des traductions possibles implique pourtant une certaine complexité pour déterminer quels termes et traductions sont les plus adéquats afin de rendre compte de cette nouvelle réalité de l'identité numérique. L'enjeux est de traduire de façon juste et pérenne ces divers termes (Cf. **Table 1**), dont les sens et définitions respectifs seront probablement sujets à de futures évolutions.

Ainsi, il appartient à la diversité des acteurs actuels de cet écosystème naissant (développeurs, institutions publiques et privées, entreprises, associations, professeurs des écoles et des universités) d'entamer une recherche d'harmonisation de ces traductions et de leurs sens.

Dans la continuité des propos précédents, une proposition de taxonomie francophone sous la forme d'un tableau récapitulatif est suggéré. Ce dernier intègre les six éléments précités nécessaire pour une solution d'identité décentralisée.

La finalité de cette liste - non exhaustive[15] - est de faire converger les traductions au plus proche de leurs réalités techniques et applicatives. Aussi, l'objectif est de les rendre, autant que possible, abordables et accessibles au grand public.

Conclusion

Cet article succinct n'a pas pour vocation de proposer un glossaire fixe et définitif (Cf. **Table 1**) pour l'identité décentralisée, mais bien de suggérer quelques fondements de réflexions qui puissent être réutilisés, approfondis ou améliorés pour l'écosystème francophone.

Dès lors et comme évoqué précédemment, il convient de prévenir tout amalgame entre les notions d'identité décentralisée et d'identité auto-souveraine, certes proches et pourtant différentes : une identité auto-souveraine est une identité décentralisée, cependant, une identité décentralisée ne constitue pas nécessairement une identité auto-souveraine.

En l'état actuel du développement et des connaissances du marché de l'identité décentralisée, il est préférable d'employer le terme générique « identité décentralisée » plutôt que « Self Sovereign Identity » pour évoquer ce phénomène. Cela permet entre autre de simplifier l'approche et les explications qui s'en suivent, au risque qu'une relative confusion avec la notion d'actifs numériques décentralisés soit possible[16].

Aussi, l'utilisation de ces termes (en anglais ou français) n'a pas la même portée, les mêmes effets, selon qu'ils soient mobilisés dans un cadre professionnel ou personnel. Dans le premier cas, une attention toute particulière au vocabulaire (professionnel) employé est attendue. Ce qui n'est pas le cas en toutes circonstances dans la seconde situation (personnelle).

Si certaines traductions peuvent être préférées à d'autres comme en témoigne la **Table 1**, nul doute que les traductions envisagées face à celles effectivement utilisées, co-existeront, jusqu'à ce qu'éventuellement, les unes prévales (de droit ou de fait) sur les autres.

***

Termes anglophones (1)	Traductions francophones possibles (2)	Traductions francophones recommandées (3)	Justifications (4)
« Decentralized identity »	« Identité décentralisée, distribuée ou désintermédiée »	« Identité numérique décentralisée ou distribuée »	Le terme « identité décentralisée » est préférable pour souligner la décentralisation du modèle d'identité numérique centralisé, jusqu'alors en place. Le terme « décentralisé » peut être substitué par « distribué » selon les approches techniques utilisées[17].
« Self Sovereign Identity – SSI »	« Identité auto-souveraine, en propre, auto-administrée ou autogérée »	« Identité numérique auto-souveraine »	Le terme « identité numérique auto-souveraine » est déjà largement introduit et utilisé par les experts francophones du secteur de l'identité numérique. Il permet facilement de comprendre deux notions fondamentales de l'identité décentralisée : celle d'autonomie et de souveraineté. Cependant, cette expression équivalente à celle de « SSI » renvoie à une expérience dans laquelle l'utilisateur gère son identité « de bout en bout », soit depuis l'émission de ses attributs ou assertions d'identité jusqu'à leurs partages ou encore révocation. En pratique, cette gestion intégrale n'est pas nécessairement applicable au modèle « d'identité décentralisée » dont il émane. Cette variante technologique et subtilité est importante afin d'éviter de substituer les termes « identité décentralisée » et« identité auto-souveraine », qui ne renvoient pas exactement aux mêmes réalités techniques et conceptuelles.
« Decentralized Identity Management System(s) »	« Decentralized Identity Management System(s) » « Système de gestion décentralisé/distribué de l'identité numérique » Idem L'expression « système de gestion décentralisé/distribué de l'identité » est similaire à des termes déjà utilisés pour une majorité de modèles de gestion centralisés de l'identité numérique : « système de gestion centralisée des accès et des identités » ou « Identity Access Management System - IAM) »	Idem	L'expression « système de gestion décentralisé/distribué de l'identité » est similaire à des termes déjà utilisés pour une majorité de modèles de gestion centralisés de l'identité numérique : « système de gestion centralisée des accès et des identités » ou « Identity Access Management System - IAM) »
« Decentralized identifier(s) (DID) »	« Identifiant décentralisé »	Idem	Dans ce cas précis, une traduction littérale et univoque est déjà unanimement utilisée par les experts de l'identité numérique en France.
« Verifiable(s) credential(s) (VC) »	« Justificatif vérifiable, attestation vérifiable, référence vérifiable, certificat vérifiable, assertion vérifiable, déclaration préétablie »	« Justificatif vérifiable », « attestation vérifiable », « déclaration d'identité préétablie »	La traduction du terme anglophone « Verifiable(s) credential(s) (VC) » est aujourd'hui celle qui fait le plus débat. De nombreux équivalents français sont possibles, bien que seulement quelques-uns correspondent à une réalité technique. C'est le cas pour le terme « justificatif vérifiable », qui désigne un simple renseignement à valeur probante faible ou moyenne qui est à disposition d'un utilisateur. Un degré plus élevé en matière de preuve de l'identité d'une personne consiste à utiliser l'expression « attestation vérifiable », qui suppose une approbation et un endossement préalable dudit « justificatif vérifiable » par un tiers de confiance (régalien par exemple). Finalement, l'expression « déclaration préétablie » pourrait uniquement et spécifiquement être utilisée dans le cadre de l'identité auto-souveraine, c'est-à-dire lorsqu'un utilisateur peut émettre seul ses attributs d'identité qui représentent alors des « déclarations d'identité préétablies ».
« Digital wallet »	« Portefeuille numérique, Portefeuille d'identité numérique, Mallette d'identité numérique »	« Portefeuille d'identité numérique ou Mallette d'identité numérique ».	Pour une utilisation professionnelle le terme de « Portefeuille d'identité numérique » semble plus adapté. Pour une explication accessible au grand public, la notion de « mallette d'identité numérique » est plus adéquate et permet de faire référence aux portefeuilles classiques qui contiennent de nombreux justificatifs et documents d'identité personnels.

Table 1
Tableau récapitulatif d'une taxonomie francophone minimaliste pour l'identité décentralisée

Notes

1 L'Art poétique (1674) de Nicolas Boileau-Despréaux, Chant I

2 T. Langlois-Berthelot. Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique. 2021. (hal-033145688)

3 T. Langlois-Berthelot. Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés. 50 experts vous expliquent la blockchain , IS EDITION, (à paraître en février 2022)

4 T. Langlois-Berthelot. La blockchain, un nouveau fondement pour la confiance numérique ? Observatoire d'IN Groupe, 2021, 5 pages⟩ (hal-03314567)

5 Op. Cit. Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés.

6 Auteur inconnu, What is "sovereign source authority" ? 2012, (Sur le blog moxytongue.com)

7 Špela Čučko, Muhamed Turkanović, Decentralized and Self-Sovereign Identity: Systematic Mapping Study, IEEE Access, 15 octobre 2021, *« If we consider overall growth, from 2017 to 2021, the number of [SSI related] papers grew by 96.7 pourcent »*

8 Op. Cit. Perspectives juridiques de l'émergence d'une identité décentralisée au service de droits numériques augmentés.

9 Glossaire de l'Université de Lille, élaboré conjointement en mars 2021 : Glossaire basique sur l'identité décentralisée

10 DSIUN de l'Université de Toulon, Modifié le 29 septembre 2020, La sécurité des systèmes d'information (SSI)

11 European Union Blockchain Observatory and Forum, page 24 sur 27, publié le 2 mai 2019, Blockchain and Digital Identity

12 J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen, Digital Identities and Verifiable Credentials, publié le 2 Septembre 2021, page 4 sur 11. (*« Outre la différenciation entre l'identité décentralisée et l'identité auto-souveraine, dans l'ensemble des recherches examinées, différents niveaux de décentralisation ont également été observés. »*)

13 Op. Cit. Decentralized and Self-Sovereign Identity: Systematic Mapping Study : (*« Outre la différenciation entre l'identité décentralisée et l'identité auto-souveraine, dans l'ensemble des recherches examinées, différents niveaux de décentralisation ont également été observés. »*)

14 Op. Cit. Decentralized and Self-Sovereign Identity: Systematic Mapping Study, page 9 sur 19 15/10/2021,(Carte de classification mettant l'accent sur la démarcation entre l'identité décentralisée et l'identité autosuffisante.)

15 D'autres éléments techniques du concept d'identité décentralisée sont volontairement exclus de ce tableau (*Verifiables Presentation, Trusted Lists, Revocation Lists*, etc.) afin de conserver une certaine exhaustivité et intelligibilité.

16 Ce qui n'est pas nécessairement une problématique dans la mesure où une recontextualisation permet de dissiper rapidement cette confusion (marché et finalités différents à court et moyen terme, etc.), qui provient en partie de l'utilisation sous-jacente de la technologie blockchain, dont l'une des caractéristiques principales est la décentralisation.

17 Dans un contexte où l'infrastructure numérique sous-jacente (par exemple une bockchain) est particulièrement ouverte et accessible, c'est-à-dire possédant un nombre important d'ordinateurs (nœuds), alors le terme d'identité décentralisée est préférable. En effet, cela correspond mieux à la réalité technique décrite : plus le nombre de nœuds du réseau est important, plus les données de ladite blockchain sont décentralisées et donc immuables. Inversement, si le registre électronique sous-jacent est peu décentralisé (soit avec nombre de nœuds limité), alors l'utilisation du terme « d'identité distribuée » prévaut sur celui « d'identité décentralisée ». Toutefois, dans les faits, les termes « distribué » et « décentralisé » sont généralement utilisés de façon interchangeable et équivalente.