L'identité numérique : un usage de la blockchain au profit du citoyen

Synthèse

Djellil Bouzidi,
Coordonnateur du pôle Économie de Terra Nova
Thibaud Frossard,
Expert Économie numérique, Terra Nova
Michael Mainelli,
Professeur émérite, Gresham College (Londres) et fondateur de l'initiative Long Finance
Simon Matet,
Expert Nouvelles Technologies, Terra Nova

24 septembre 2018

À mesure que nous développons notre présence en ligne et notre activité numérique, en naviguant sur le réseau, en faisant des achats en ligne, en créant des comptes sur les réseaux sociaux... nous avons besoin de nous identifier. Les comptes que nous créons à cette occasion peuvent être fictifs ou protégés par des pseudonymes. Mais, dans le cadre de transactions commerciales, de services rendus entre particuliers ou de démarches administratives officielles, il importe de pouvoir attester de son identité tout en maîtrisant au mieux les informations que nous transmettons à cette occasion.

Dans ce contexte, une large réflexion se développe sur les outils de notre « identité numérique ». La situation actuelle la plus fréquente conduit chacun de nous à gérer des dizaines d'identifiants et plusieurs adresses électroniques, avec des risques de piratage voire d'usurpation d'identité élevés. Pour faciliter et sécuriser des usages aussi répandus et désormais indispensables à la vie quotidienne, la puissance publique doit prendre en compte ce nouveau sujet de l'identité numérique – qui renouvelle un aspect de sa souveraineté qui s'est toujours affirmée à travers la maîtrise de l'état civil.

Des initiatives existent déjà permettant de rassembler dans un identifiant unique et sécurisé différentes certifications administratives : carte d'identité, passeport, permis de conduire, affiliation à la Sécurité sociale, caisse de retraites, etc. Le gain de temps, de simplification, de sécurité... peut être considérable pour l'État mais aussi pour la compétitivité générale de l'économie. À l'image de ce qui se fait déjà en Estonie, une citoyenneté numérique globale peut ainsi se mettre en place. Pourtant, la méfiance vis-à-vis d'un outil aussi puissant est aussi légitime. Elle s'est d'ailleurs déjà manifestée dans le passé à l'égard de projets d'interconnexion des fichiers administratifs et a donné naissance à des normes de protection des libertés individuelles supervisées par un organisme indépendant, la Commission nationale informatique et libertés (Cnil). Peut-on pourtant aller plus loin ?

Le développement de la technologie « blockchain » offre l'opportunité de surmonter la contradiction entre la protection des libertés individuelles et les opportunités des nouvelles technologies. En effet, la blockchain peut se révéler utile pour aider les citoyens à garder le contrôle de leurs données, un facteur clé dans l'acceptation et l'adoption de systèmes d'identité numérique nationaux. En tant que système décentralisé de certification, la blockchain pourrait servir à construire un système d'identification numérique sans avoir à confier à l'État la gestion et la conservation d'un gigantesque registre numérique des citoyens. Selon les choix technologiques retenus, l'usage de blockchain entraînera une responsabilisation accrue des citoyens.

Aussi, nous recommandons d'éprouver la technologie en y recourant le plus souvent possible, notamment pour le rapprochement décentralisé de bases de données publiques, ou en lançant, dans des collectivités locales pilotes, des expérimentations de solutions plus globales, avant d'envisager un déploiement général en France.

SOMMAIRE

INTRODUCTION

La blockchain... Depuis quelques années, en lien avec l'envolée record des valorisations des cryptomonnaies, le mot est sur les lèvres de tous les acteurs privés comme publics. Devenu le « *buzzword* » de l'année – pour reprendre la terminologie du quotidien britannique *The Guardian*[1] –, l'usage des blockchains est l'objet de toutes les convoitises. Certains y voient l'équivalent d'Internet[2] en termes de potentiel de développement. D'autres, à l'image de l'économiste Nicolas Bouzou, appellent même la France à en faire sa priorité au détriment d'autres technologies comme l'intelligence artificielle. Enfin, notre ministre de l'Économie et des Finances, Bruno Le Maire, l'a promis dans une récente tribune[3] : « Nous ne raterons pas la révolution de la blockchain ! » Mais de quoi parle-t-on exactement ?

Les blockchains sont des bases de données, des registres partagés, qui permettent à des personnes physiques ou morales de valider, d'enregistrer et de suivre des transactions à travers un réseau décentralisé d'ordinateurs[4]. Le caractère « mutuel » des blockchains les protège du risque de monopole pouvant survenir sur une base de données centralisée. Avec pour objectif principal de se passer de toute autorité centrale, trois rôles principaux semblent pouvoir être assurés par cette technologie : la certification, l'identification et le paiement de transactions. Ce dernier point a d'ailleurs fait beaucoup de bruit avec l'une des rares utilisations fondatrices et reconnues des blockchains : les cryptomonnaies et, en particulier, le fameux Bitcoin. Nous n'y reviendrons pas ici.

L'usage des blockchains pour l'identification et la certification représente une nouvelle piste de travail puisque la technologie permet la création de registres incorruptibles et de confiance, deux caractéristiques clés de tout système d'identité. Nous proposons d'explorer, dans cette note, les capacités de la France à utiliser les possibilités offertes par la technologie blockchain afin de fournir et sécuriser l'identité numérique de ses citoyens.

En effet, l'identité numérique, avant d'être un actif économique crucial et à protéger, est surtout un élément régalien et clé de l'ordre public. En effet, l'histoire de l'État moderne se

[1] *The Guardian*, « Blockchain is this year's buzzword – but can it outlive the hype? «, 30 janvier 2018.
[2] Pour être plus précis, du protocole TCP/IP qui sert de base à Internet. Voir l'article de *Harvard Business Review* (2017), « The Truth About Blockchain ».
[3] *Numerama*, tribune : « Cryptoactifs, blockchain & ICO : comment la France veut rester à la pointe », par Bruno Le Maire, 19 mars 2018.
[4] Voir Michael Mainelli « Blockchains Will Help Us Prove Our Identities In a Digital World «, *Harvard Business Review (*2017).

confond pour une large part avec sa capacité à identifier, compter et contrôler les individus présents sur son territoire. L'identité numérique est l'extension moderne et naturelle de l'identité physique. Pour toute une série de raisons liées à l'ordre public (patrimoniales, successorales, matrimoniales, sécuritaires, policières, sociales, etc.), il importe que les identités soient incontestables et vérifiables. Cela conditionne la capacité de l'État à reconnaître ses ressortissants et sujets, et, partant, la capacité des ressortissants et sujets à bénéficier de toute une série de droits. Dans les démocraties libérales, ce contrôle des identités physiques s'est accru et perfectionné, parfois à l'encontre des libertés publiques, mais surtout en accompagnant leur développement.

Or, si nos identités numériques sont, aujourd'hui, régulièrement sollicitées, et le seront probablement demain toujours plus, elles sont désormais presque aussi importantes que nos identités physiques et toujours aussi difficiles à prouver ! Il n'existe toujours pas de standard reconnu au niveau mondial qui permettrait à chacun d'effectuer ses achats et démarches administratives en prouvant simplement qu'il est bien celui qu'il prétend être. Ainsi, il existe 1,4 milliard de sites Internet dans le monde, et l'e-commerce a représenté quelque 2 300 milliards de dollars de chiffre d'affaires au niveau mondial en 2017[5]. Pourtant, chaque site utilise plus ou moins des règles d'identification qui lui sont propres. Il en va de même pour de nombreux services publics. Un citoyen passe en moyenne 1 h 22 par jour sur les seuls réseaux sociaux[6]. Ces derniers possèdent dès lors une constellation d'informations sur chaque utilisateur et deviennent des fournisseurs d'identité numérique. Certains gouvernements, à l'instar des États-Unis, demandent d'ailleurs aujourd'hui aux passagers entrant sur leur sol de révéler leurs identifiants sur les réseaux sociaux. Peut-on toutefois compter sur cette identité numérique dans chaque situation ? Les gouvernements ont-ils un rôle à jouer pour reprendre l'initiative sur cette construction de l'identité par des acteurs transnationaux privés ?

En France, de nombreuses expérimentations, plus ou moins réussies, ont été menées sur le sujet dans les dernières décennies. La France accuse toutefois un certain retard sur les sujets d'identité numérique par rapport à ses voisins européens. Cela a des conséquences sur son économie et sa capacité à améliorer son service public. Selon l'indice relatif à l'économie et à la société numériques[7], la France se classe, sur les sujets plus généraux de

[5] Source : https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/
[6] Hootsuite - We are Social, « Le Digital en France en 2018 ».
[7] Source: https://ec.europa.eu/digital-single-market/desi

performance numérique, à la 16e position sur 28, avec un score légèrement inférieur à la moyenne, et 13e en matière de services publics numériques. La dématérialisation progressive des démarches administratives, engagement fort du président de la République, ne pourra être réalisée sans une identité numérique rénovée. Forte de ces conclusions, une mission interministérielle sur l'identité numérique a été lancée en janvier 2018. L'objectif affiché par le gouvernement est d'obtenir un nouveau service ouvert au public à la rentrée 2019. Avec quels outils peut-on construire une nouvelle attestation des identités à l'âge numérique ? Pourrait-on le faire rapidement ? Comment le faire en préservant la liberté et la responsabilité de chacun d'entre nous ?

1. L'IDENTITÉ NUMÉRIQUE EST UN NOUVEAU DEFI À RELEVER POUR HISSER LA FRANCE AU RANG DES GRANDES NATIONS NUMÉRIQUES

Le concept d'identité numérique recouvre, selon les spécialistes, des réalités diverses. Nous désignerons, dans la suite de cette note, par identité numérique toute solution qui permet de certifier l'identité d'un utilisateur et de partager en ligne des données personnelles certifiées de manière simple.

1.1. L'IDENTITÉ NUMÉRIQUE EN FRANCE EST MULTIPLE ET DISPERSÉE ENTRE DES ACTEURS PUBLICS ET PRIVÉS

En France, l'histoire de l'identité numérique a été fortement marquée par de grands projets portés par la puissance publique. Il s'agissait majoritairement de solutions visant à unifier l'identité numérique des citoyens pour simplifier leur gestion administrative.

Dans un premier temps, la question fut abordée sous l'angle de l'identifiant de suivi unique. Le débat prit de l'ampleur publiquement à partir de 1974[8] avec la publication par *Le Monde* d'un article de Philippe Boucher intitulé « Safari ou la chasse aux Français ». À une époque où l'informatique était encore relativement peu répandue, le projet Safari – pour Système automatisé pour les fichiers administratifs et le répertoire des individus –, initié par l'Insee dès 1971 et soutenu par le ministère de l'Intérieur, consistait à agréger l'ensemble des données administratives des Français sur un ordinateur. Un numéro unique aurait pu servir

[8] Ertzscheid O., chapitre 1 – « Les logiques identitaires », in *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies,* 2013.

de clé d'identification numérique. Dans le cas de Safari, le numéro Insee (désormais connu sous l'appellation Nirpp[9]) avait été retenu. Le projet comportait à la fois une numérisation des fichiers sur bandes magnétiques et une interconnexion entre les bases de données de différentes administrations et organismes (fichiers de police, de Sécurité sociale, bancaires, etc.). Le programme et le relatif secret qui l'entourait ont suscité l'inquiétude de l'opinion publique et, en conséquence, un débat politique en pleine année d'élection présidentielle. Le projet Safari fut rapidement rejeté pour protéger les libertés individuelles. Cette affaire débouchera quelques années plus tard sur la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi est à l'origine de la Cnil[10], première autorité administrative indépendante en France[11].

Depuis, la centralisation – ou *a minima* l'interconnexion entre – des bases de données publiques revient régulièrement dans l'actualité avec plus ou moins de succès et d'écho médiatique. Au final, il n'existe toujours pas d'identifiant unique de connexion vis-à-vis de la puissance publique en France, et les liaisons entre chacune des bases de données publiques demeurent surveillées. Pour le citoyen, cela se traduit par une multiplicité d'identités numériques. Chaque citoyen dispose d'une identité numérique vis-à-vis de l'administration fiscale, d'une autre identité numérique vis-à-vis de la Sécurité sociale, etc. Cette absence d'unité n'est pas nécessairement un problème, elle permet aux diverses composantes de son identité numérique d'être mieux protégées. La multiplicité des bases de données permet d'éviter la perte massive de données personnelles en cas de piratage de l'une d'entre elles. Ainsi, aux États-Unis, les données d'identité de 145 millions d'Américains, dont leur numéro de sécurité sociale[12], ont fuité de la société Equifax (société d'évaluation et de notation de crédit)[13] et de sa base de données. Cependant, la pluralité des identités numériques contraint chaque entité à disposer de plus de données que nécessaires à son fonctionnement, en opposition au principe de « minimisation des données » dans la lignée duquel s'inscrit le

[9] Nirpp signifie : numéro d'inscription au répertoire des personnes physiques. Il est mieux connu sous la désignation : numéro de Sécurité Sociale.

[10] Cnil signifie Commission nationale de l'informatique et des libertés.

[11] Les missions de la Cnil sont définis dans l'article 11 de la loi susnommée.

[12] Le numéro de sécurité sociale aux États-Unis joue le rôle d'un « mot de passe » secret en l'absence de système national d'identité. Il est ainsi possible de contracter des emprunts ou de récupérer des impôts prélevés à la source en excès grâce à celui-ci.

[13] Voir https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

récent RGPD (Règlement général pour la protection des données)[14] adopté au niveau européen.

À ces identités numériques publiques se sont progressivement ajoutées des identités numériques privées. Certains acteurs privés ont ainsi voulu créer de grands agrégateurs d'identités à l'image des versions initiales de Microsoft Passport. Avec l'avènement des réseaux sociaux, le sujet a encore pris de l'ampleur. Chacun laisse sur ses profils Facebook, Twitter, etc., une quantité d'informations, que ce soit en les inscrivant lui-même lors de son inscription et au fur et à mesure de son usage, ou, plus subrepticement, en consultant des sites partenaires qui font appel à des services du réseau social.

1.2. LE PARADIGME DU TYPE OPENID EST ENTRÉ DANS LES MŒURS

Les identités numériques ainsi acquises par rapport à la puissance publique ou à des organismes privés sont utiles pour ces organisations, mais peuvent constituer des preuves d'identité pour de futurs échanges avec des tiers. Pour de nombreux tiers, il est en effet nécessaire de savoir qui souhaite s'inscrire à une application et s'il est vraiment celui qu'il prétend être.

Ainsi, en pratique, une demande d'identification nécessite généralement l'interaction entre trois parties. La première est la *personne*[15] qui cherche à prouver son identité ou l'authenticité de données personnelles. La seconde est *le fournisseur d'identité*, c'est-à-dire l'autorité ou l'entité qui certifie l'identité de la *personne* ou certifie le document émis. Comme évoqué, la *personne* détient de multiples identités numériques qui possèdent chacune des informations distinctes sur lui et font plus ou moins le lien avec son identité physique. Autrement dit, il y a une *personne* mais plusieurs *fournisseurs d'identité* possibles. Il existe aussi bien évidemment des *fournisseurs d'identité* physique comme la préfecture pour la délivrance d'une carte d'identité. La troisième partie est *le fournisseur de service ou requérant*. Il peut s'agir d'une tierce personne physique ou morale qui souhaite vérifier la véracité d'une identité ou d'un document (une administration, une banque, un assureur, un site Internet, etc.). Les *fournisseurs d'identité* agissent comme des tiers de confiance envers des tiers *requérants*.

[14] Voir par exemple, à ce titre, dans le règlement l'article 5.1.c : « Les données à caractère personnel doivent être : adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données). »

[15] Il peut très bien s'agir d'une personne physique (par exemple un citoyen) ou d'une personne morale (par exemple une entreprise).

Cela permet à ces derniers d'éviter de ré-identifier la *personne* au gré de plusieurs procédures impliquant parfois des contacts réels (envoi d'une copie de sa pièce d'identité, d'un mot de passe temporaire par courrier, etc.). Dans le cas d'environnement numérique, ces types d'échanges ont connu un fort succès avec l'adoption à grande échelle par des acteurs comme Google ou Microsoft d'OpenID, un protocole mettant en œuvre ce paradigme.

C'est notamment le principe sous-jacent à Facebook Connect lancé à partir de 2009. De nombreux sites ou applications proposent de se « connecter via Facebook ». Pour l'utilisateur, cette fonctionnalité permet de gagner beaucoup de temps et simplifie grandement son expérience. Il n'a, par exemple, pas besoin de posséder de multiples mots de passe et, pour certains, cela lui évite de recréer un carnet d'adresses ou un portefeuille de photographies. Le système est extrêmement simple d'utilisation puisqu'il suffit d'avoir une session Facebook ouverte pour créer en un clic un compte chez le tiers. Pour le site partenaire, outre une simplification de l'expérience-client, il est possible d'avoir accès à diverses informations plus ou moins vérifiées sur l'utilisateur par le réseau social. Facebook Connect joue le rôle de *fournisseur d'identité*.

L'identité numérique de Facebook n'est cependant utilisable que pour des tiers demandant une vérification d'identité non critique. Le réseau social n'établit en effet pour le moment aucun lien entre l'identité physique et l'identité numérique de ses utilisateurs. Lors de l'inscription sur le réseau social, personne ne contrôle si je suis bien la personne que je prétends être en vérifiant ma pièce d'identité papier, par exemple. C'est l'une des raisons pour lesquelles il n'est pas rare de voir des cas d'usurpation d'identité sur le réseau[16]. Depuis 2014, le réseau précise toutefois dans ses standards d'utilisation qu'il faut se présenter sous son vrai nom et sa vraie identité. Suite à des signalements, des comptes sont parfois bloqués, et l'utilisateur doit, à ce moment, envoyer une copie d'un titre d'identité pour obtenir le déblocage. On le voit ici, le lien entre identité physique et identité numérique se renforce mais demeure à ce jour limité. En accord avec les politiques « Know Your Customer » (KYC)[17], il n'apparaît donc pas possible pour le moment d'utiliser Facebook Connect pour ouvrir un compte bancaire ou acheter des titres sur les marchés financiers. De même, pour des raisons évidentes de souveraineté numérique, il paraît difficilement acceptable, et imprudent, pour

[16] Voir à ce titre par exemple la prise de position récente du député Philippe Huppé pour demander une plus grande réactivité face à des usurpations d'identité sur les réseaux sociaux (questions au gouvernement le 27 mars 2018).
[17] En accord avec les politiques Know Your Customer, il est demandé à un certain nombre d'institutions financières de savoir qui sont leurs clients pour lutter contre le blanchiment ou le financement du terrorisme.

un gouvernement d'utiliser Facebook Connect comme *fournisseur d'identité* pour des usages administratifs.

En réponse et sur le même modèle, la Dinsic[18] a mis en place dès 2014 le dispositif France Connect. Il permet à des utilisateurs de s'identifier via un compte auprès d'un « fournisseur d'identité » pour accéder à des services proposés par de multiples tiers. Les « fournisseurs d'identité » sont aujourd'hui au nombre de quatre : le site gouvernemental de l'administration fiscale Impots.gouv.fr, Loggin de La Poste, Ameli de l'Assurance maladie et Mobile Connect d'Orange. Sur le modèle de Facebook Connect, ces sites permettent de se connecter à des sites tiers sans besoin de vérification d'identité, par exemple sur Télépoints pour la vérification du nombre de points sur son permis de conduire. Il n'y a pas de centralisation des bases de données : le fournisseur d'identité ne fait que confirmer l'identité de la personne et, s'il transfère des données, le consentement de l'usager est demandé. Il est même impossible pour le fournisseur d'identité de savoir à quel usage les données transférées sont utilisées. Chaque fournisseur d'identité applique son propre protocole de vérification. Dans le cas de La Poste, l'IDentité Numérique s'obtient par exemple en remplissant ses informations personnelles, en confirmant son numéro de téléphone via un SMS, puis par une vérification physique des données déclarées lors de l'inscription par un facteur. Aujourd'hui, France Connect compte quelque 4,7 millions d'utilisateurs et permet de se connecter à près de 600 sites partenaires.

1.3. LES NOUVEAUX DÉFIS DE L'IDENTITÉ NUMÉRIQUE

Dans ses engagements de campagne, le président de la République, Emmanuel Macron, a annoncé plusieurs grands programmes nécessitant une identité numérique commode et sécurisée. C'est, par exemple, le cas de la proposition visant à réaliser 100 % des démarches administratives en ligne d'ici à 2022[19]. Ainsi, aussi de la proposition de création d'un État-plateforme, d'un « compte citoyen en ligne » qui agrègerait tous les droits ou encore du développement souhaité de la télémédecine.

[18] La Dinsic est la Direction interministérielle du numérique et du système d'information et de communication de l'État.
[19] À l'exception logique de la première délivrance de documents d'identité officiels.

Le lien entre identités physique et numérique, l'exemple des cartes d'identité électroniques

Pour assurer le lien entre identité physique et identité numérique, il existe de multiples solutions. Nous en utilisons de nombreuses au quotidien parfois sans même le savoir. Le traditionnel login-mot de passe est le plus simple, il repose sur l'idée que seul celui qui l'enregistre le connaît mais il est de ce fait vulnérable à n'importe quel logiciel espion ou attaque par hameçonnage. D'autres authentifications sont possibles au moyen d'outils externes de façon à protéger les utilisateurs contre les vols de mot de passe. On parle alors d'identification à deux facteurs. Pour les paiements en ligne, certaines banques utilisent ainsi le téléphone portable et un code envoyé par SMS comme solution. La carte d'identité électronique pourrait constituer une autre solution d'identification sécurisée à deux facteurs en lui adjoignant une puce et un code PIN, par exemple.

De nombreux États mettent à disposition ce type de cartes à leurs résidents. Elles constituent des « tokens » d'identification, qui, reliés à un ordinateur, permettent d'assurer le lien entre le monde physique et le monde numérique. La solution est déjà implantée dans de nombreux pays européens et à travers le reste du monde. Des technologies biométriques (contrôle d'empreintes, etc.) peuvent être insérées dans les cartes. En cas de vol de la carte, cela constitue un degré de protection supplémentaire.

En France, un projet de carte d'identité électronique, associant une dimension biométrique, nommé Ines (Identité nationale électronique sécurisée), a été lancé en 2005. Le projet a été rejeté par l'opinion publique et n'a pas abouti. Le débat a repris lors du projet de loi de 2012 « Protection de l'identité » qui prévoyait notamment une puce d'identité numérique permettant d'accéder à des services de l'administration en ligne. Cette dernière disposition a cependant fait l'objet d'une censure du Conseil constitutionnel, repoussant encore le projet.

La France accuse aujourd'hui un retard sur les sujets d'identité numérique par rapport à de nombreux pays européens[20]. La multiplicité des identités numériques vis-à-vis des administrations (généralement des logins/mots de passe vulnérables), l'absence d'un token d'identification permettant d'assurer à tout instant le lien entre monde physique et monde numérique (carte d'identité numérique) ou encore la faible relation avec d'autres acteurs clés de la vie du citoyen (banques, assurances, etc.) sont autant de difficultés qui vont se poser pour hisser la France dans les rangs des grandes puissances digitales. Car une identité numérique certifiée est un atout pour le développement de l'économie et d'un écosystème numérique fort. C'est ce qu'a parfaitement compris l'Estonie. Dans ce pays, un protocole d'identification numérique reposant sur une carte d'identité numérique, disponible depuis 2001, a été adopté par près de 98 % des citoyens et permet d'accéder à divers services publics comme privés nécessitant une identification forte. L'Estonie repose aussi sur sa force digitale pour attirer des entreprises sur son territoire. En créant, en 2014, le statut de « e-résident », l'Estonie a d'ores et déjà permis à plus de 33 000 étrangers d'obtenir une identité numérique. Ce service permet en particulier de créer et d'assurer la gestion de son

[20] Voir encadré 1 sur la carte d'identité numérique et encadré 2 sur l'Estonie.

entreprise à distance. Sans solution crédible en France, la simplicité du système estonien pourrait amener des entrepreneurs français à se détourner de notre écosystème.

L'Estonie, une nation digitale

Tel qu'indiqué sur le site e-estonia.com, chaque Estonien dispose d'une identité digitale émise par le gouvernement. Tout citoyen peut ainsi signer électroniquement un document ou accéder en ligne à un service administratif. 98 % des Estoniens disposent d'une carte d'identité dite ID-Card permettant d'accéder de manière sécurisée à l'ensemble des services administratifs numériques offerts par l'Estonie. Ainsi, cette carte peut être utilisée pour voter électroniquement, pour utiliser son compte bancaire, pour bénéficier des services de santé, etc. De fait, plus de 500 millions de signatures digitales ont déjà été enregistrées.

Cette avancée technologique de l'Estonie est une réaction aux cyber-attaques dont le pays a été la cible en 2007. Le gouvernement estonien a décidé d'utiliser la blockchain pour gérer les échanges de données entre les administrations et les consigner de façon infalsifiable. La blockchain est utilisée dans des situations où plusieurs parties prenantes doivent partager des informations autorisées l'une avec l'autre sans un tiers central. En conséquence, le système estonien fournit à ses citoyens une expérience administrative unifiée, transparente, sécurisée et satisfaisante.

L'Union européenne s'inscrit en moteur sur la question de l'identité numérique. Outre le RGPD déjà évoqué, le règlement eIDAS du 23 juillet 2014 entend renforcer l'interopérabilité des services d'identification électronique et de confiance ainsi que l'échange de documents électroniques entre les différents États membres. Ce règlement fixe à ce titre les règles de sécurité et de vérification applicables aux différents types d'identité numérique[21]. Surtout, il insiste sur la reconnaissance mutuelle des moyens d'identification électronique[22] : chaque pays devra accepter les identités numériques – dûment délivrées selon les principes fixés par eIDAS – des autres États membres. Cette reconnaissance deviendra obligatoire à compter du 29 septembre 2018. C'est un nouveau défi pour la France qui rend urgent de mettre en place nos propres standards rapidement pour influencer les autres pays et s'inscrire comme un moteur du numérique en Europe, permettant en conséquence de ne pas « subir » les standards de nos voisins.

[21] Voir l'article 8 du règlement eIDAS sur les niveaux de garantie « faible », « substantiel » et « élevé ».

[22] Conformément à l'article 6 du règlement eIDAS, « lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée en vertu du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne [...] ».

Le gouvernement a pris conscience de ces lacunes et entend doter la France d'une identité numérique rénovée. Une mission interministérielle sur l'identité numérique a été lancée en janvier 2018 sous l'impulsion de Gérard Collomb, ministre de l'Intérieur, Nicole Belloubet, garde des Sceaux et ministre de la Justice et Mounir Mahjoubi, secrétaire d'État chargé du numérique. « L'objectif à atteindre consiste à développer pour l'ensemble des citoyens, des étrangers en situation régulière et des entreprises un parcours d'identification numérique fluide[23]. » L'objectif affiché par le gouvernement est d'obtenir un nouveau service ouvert au public d'ici à la rentrée 2019.

Au regard de l'histoire de l'identité numérique en France et des grands défis contemporains évoqués, six grandes caractéristiques apparaissent cruciales quant à ce nouveau système.

1. Être utilisable par des acteurs publics comme privés : la puissance publique est un acteur clé, tant dans le développement des solutions que dans leur utilisation, mais des acteurs comme des institutions financières, des écoles privées délivrant des diplômes ou des institutions étrangères sont toutes légitimes à fournir des données signées en leur nom que l'utilisateur peut vouloir rendre facilement accessibles à des tiers via son identité numérique.

2. Permettre le transfert de données ciblées entre fournisseurs d'identité uniquement sous le contrôle de l'utilisateur : l'utilisateur doit rester maître de ses données. Si un tiers requérant souhaite accéder aux données de l'utilisateur, celui-ci doit pouvoir comprendre clairement ce qui est transféré et donner ou non son accord. Aucun acteur ne doit avoir accès à des données d'un utilisateur par le système d'identité numérique sans le consentement du titulaire de l'identité concernée.

3. Permettre à tout moment d'établir un lien entre les identités numérique et physique : l'identité numérique doit être constamment accessible, permettre la vérification de l'identité physique de l'usager au moment les plus critiques (réalisation d'une dépense importante, vote, etc.) et résister à des tentatives de blocage par des pirates.

4. Permettre l'ajout par l'utilisateur de données certifiées par des tierces parties non référencées : l'utilisateur peut souhaiter vouloir ajouter de multiples

[23] Lettre de mission du 5 janvier 2018.

données obtenues au cours de sa vie. Il peut, par exemple, s'agir d'un diplôme obtenu dans une université étrangère que l'utilisateur pourrait vouloir transmettre à de futurs employeurs. Une fois ajoutée dans son identité numérique et certifiée par un acteur du système, l'utilisateur peut les partager au même titre que des données fournies par l'administration.

5. Assurer une traçabilité complète des données et des demandes et autorisations de chaque requérant.

6. Assurer la sécurité des données même face à une cyber-attaque ou un gouvernement liberticide : l'utilisateur doit avoir confiance dans la confidentialité et l'intégrité du système quand bien même un gouvernement serait tenté de l'attaquer.

2. LES NOUVELLES TECHNOLOGIES DE DÉCENTRALISATION DE TYPE « BLOCKCHAIN » PEUVENT RENDRE AU CITOYEN SON IDENTITÉ TOUT EN EN AMÉLIORANT LA SÉCURITÉ DES DONNÉES

2.1. LES TECHNOLOGIES « BLOCKCHAIN » PERMETTENT LA CRÉATION DE REGISTRES DÉCENTRALISÉS INFALSIFIABLES

Depuis une dizaine d'années est apparue une technologie permettant de concevoir des bases de données sécurisées et infalsifiables sans avoir recours à un acteur de confiance central : la blockchain. Si les technologies de blockchain sont nombreuses, le principe reste le même : les données (la *blockchain*, « chaîne de blocs », au sens littéral) sont recopiées sur une multitude de serveurs, les « nœuds » de la blockchain, et leur authenticité est assurée par un procédé cryptographique.

Historiquement, sur les blockchains les plus connues comme Bitcoin ou Ethereum, le procédé garantissant l'authenticité d'une blockchain est la preuve par le travail (« *proof of work* »)[24]. À chaque étape de la vie de la blockchain, des opérateurs (appelés « mineurs ») se saisissent de modifications demandées par des utilisateurs (des transactions, par exemple). Il est possible de vérifier que les modifications sont opérées par une personne légitime en comparant la signature électronique de la modification avec les propriétaires de

[24] Le protocole décrit correspond peu ou prou à celui utilisé par le Bitcoin. Il existe cependant autant de protocoles que de blockchains.

l'information modifiée, qui est stockée dans la chaîne des blocs précédents[25]. Pour créer un nouveau bloc, les mineurs apposent à la liste des transactions une trace du précédent bloc (nommé « hash », voir encadré sur le chiffrement), la date et l'heure du moment (horodatage), et la solution d'un problème mathématique complexe à partir de ces données. Il est ainsi facile pour quiconque de vérifier l'authenticité et la datation des données : il suffit de remonter de bloc en bloc les modifications et de vérifier à chaque étape que chaque modification inscrite est conforme aux règles de la blockchain (par exemple que l'adresse ayant envoyé des Bitcoins possédaient bien ces Bitcoins). À l'inverse, le coût important de la création de chaque nouveau bloc dissuade de polluer la chaîne avec des blocs illicites où une transaction illégale serait inscrite.

Il existe aujourd'hui d'autres technologies de blockchain, moins coûteuses en puissance de calcul et en énergie. Il existe aussi une quantité de variantes du protocole décrit ci-dessus. Le principe central reste toutefois le même : une chaîne de modifications partant d'un état initial qu'il est possible d'auditer de bout en bout, en vérifiant que chaque modification est bien légitime. Mieux encore, il est possible d'inscrire des « smart contrats » dans la blockchain. Il s'agit d'instructions exécutées par les nœuds de la blockchain lorsque certaines conditions sont remplies. Ceux-ci reposent sur le même principe qu'une modification simple : il est possible d'auditer la blockchain en vérifiant que les smart contracts ont bien été exécutés au bon moment. Aucun nœud n'a intérêt à créer un nouveau bloc ne respectant pas le contrat inscrit à l'étape précédente, puisque celui-ci serait immédiatement analysé et rejeté par les autres nœuds.

Pour l'identité numérique, ces technologies offrent la promesse d'un registre décentralisé et infalsifiable. Naturellement, il n'est pas question de partager publiquement un registre de données d'identité lisibles par tous. Mais il est envisageable de concevoir des systèmes reposant sur le partage de données certifiées authentiques par une autorité, chiffrées par leur propriétaire et rendues ineffaçables et infalsifiables en les recopiant sur une multitude de serveurs sécurisés.

[25] Dans le cas du Bitcoin par exemple, à une signature électronique infalsifiable est associé un nombre de Bitcoins. Les mineurs vérifient donc que la transaction soit signée par une signature ayant suffisamment de Bitcoins à son nom. Voir l'encadré chiffrement au sujet des signatures électroniques.

Chiffrement

Chiffrements symétriques et asymétriques

La cryptographie est indissociable des technologies blockchain et de l'identité numérique. Il existe deux grandes catégories d'algorithmes de chiffrement : les chiffrements symétriques et asymétriques.

Le chiffrement symétrique utilise une unique clé de chiffrement pour coder et décoder des données. Par exemple, la technique naïve de remplacer chaque lettre dans un message par un symbole est un algorithme de chiffrement symétrique : il suffit de connaître la correspondance entre les lettres et symbole pour chiffrer et déchiffrer.

À l'inverse, il existe des méthodes asymétriques utilisant deux clés de chiffrement. Tout message chiffré avec la première clé n'est déchiffrable qu'avec la seconde clé, et inversement. L'une des clés est qualifiée de clé publique et est connue de tous, l'autre, de clé privée et est secrète. Ces protocoles sont omniprésents en ligne, et c'est grâce à ceux-ci qu'il est possible d'envoyer des coordonnées bancaires chiffrées à un site de commerce en ligne : chacun connaît la clé publique du site et peut lui envoyer des messages confidentiels mais personne, sauf l'exploitant du site, ne connaît la clé privée, ce qui empêche de déchiffrer des messages envoyés par d'autres au même site.

Fonctions de hachage

Les fonctions de hachage sont une troisième catégorie d'algorithmes importante pour l'identité numérique à laquelle nous faisons référence. Ces fonctions produisent, à partir de données, une trace, nommée « hash ». Le hash est généralement court et identifie, de façon presque unique, les données hachées. Les fonctions de hachage utilisées en cryptographie génèrent des hash à partir desquels il est impossible de retrouver des informations sur les données ou de trouver deux jeux de données différentes donnant le même hash. Ainsi, on peut concevoir de partager des hash de permis de conduire certifiés authentiques sur une blockchain visible par tous. Impossible pour un pirate de retrouver les permis à partir des hash et de voler des identités, mais la personne peut prouver que son permis est authentique en montrant simplement que son hash est présent sur la blockchain des hash de permis authentiques.

Signatures électroniques

À partir des deux briques précédemment décrites, hachage et cryptographie asymétrique, il est possible de construire des signatures électroniques sécurisées. Une autorité certificatrice hache un document dont elle veut certifier l'authenticité et chiffre le hash avec sa clé privée. L'ensemble document + hash chiffré constitue le document signé. Il est possible pour n'importe qui de déchiffrer le hash avec la clé publique de l'autorité certificatrice. En le comparant avec le hash du document, on peut ainsi s'assurer que le document présenté comme authentique n'a pas été modifié depuis la certification par l'autorité.

Au regard des six caractéristiques évoquées dans le cahier des charges de l'identité numérique, la blockchain permet de satisfaire spécifiquement et avec une forte valeur ajoutée les points 5 (traçabilité) et 6 (sécurité) en cas de rupture de confiance envers l'administrateur de la solution d'identité numérique.

Ainsi, cette technologie permettrait de « rendre » aux citoyens les données qui leurs appartiennent (au moins en partie) de façon sécurisée et transparente. En tant que détenteur ultime des données relatives à son identité, chaque citoyen peut dès lors décider ou non (dans un second temps) de les échanger.

2.2. LES TECHNOLOGIES DE BLOCKCHAIN PEUVENT RENDRE ACCEPTABLE UNE IDENTITÉ NUMÉRIQUE PLUS AMBITIEUSE EN LA LAISSANT AUX MAINS DES CITOYENS

La France est à un carrefour technologique concernant l'identité numérique. Les différentes solutions techniques envisageables ne sont pas nécessairement exclusives et peuvent fonctionner de pair. Le système France Connect peut, à terme, se montrer suffisant pour fournir à toute personne physique ou morale un moyen simple de prouver son identité et partager des données en ligne avec un niveau de sécurité raisonnable. Les quatre premières caractéristiques listées ci-dessus sont à la portée d'un système centralisé sur le modèle de France Connect, même si le dispositif est aujourd'hui encore en développement et devra faire l'objet d'adaptation. Par exemple, le lien continu entre identité numérique et identité physique pourra être renforcé par l'ajout d'une carte d'identité numérique au système, avec ou sans biométrie. L'arrivée de fournisseurs d'identité privés, en particulier pour le transfert de données certifiées, est également réalisable, la Poste participant d'ailleurs déjà au projet, même si la question de la rémunération des fournisseurs d'identité privés reste ouverte. Il en va de même de documents externes non référencés : ils pourraient, par exemple, être vérifiés par des tiers physiques spécialisés dans l'audit de ce genre de pièces pour une mise en ligne définitive chez un fournisseur d'identité donné.

Néanmoins, il demeure que l'architecture centralisée dans laquelle différents services de l'État ou organismes privés détiennent les données et se les échangent peut être plus difficilement compatible avec les deux exigences de traçabilité ou de sécurité. Certes, il n'existe ni base de données centralisées ni échange s'opérant sans le consentement de chaque citoyen, mais ces derniers reposent toujours sur un tiers, l'État, dans lequel les citoyens doivent avoir pleinement confiance. Ce système risque donc de se heurter à terme aux mêmes inquiétudes que celles exprimées par la société civile lors des précédentes initiatives liées à l'identité numérique**.** Quels que soient les gains en termes d'efficacité ou de simplicité, les citoyens ne semblent pas prêts à centraliser leurs données les plus sensibles, comme leurs informations médicales, en se reposant entièrement sur la sécurité et l'intégrité du tiers central, c'est-à-dire la puissance publique, ou *a minima* dans les instances de contrôle de celui-ci comme la Cnil.

C'est ici que la blockchain peut être utile, comme nous l'avons déjà évoqué. Il ne s'agit bien évidemment pas de remettre en cause le bien-fondé de la confiance envers ces acteurs tiers. En interrogeant l'opportunité d'avoir recours à une solution décentralisée par la blockchain,

le débat reste ouvert quant à la mise en place de garde-fous supplémentaires à l'âge des piratages informatiques et des affaires d'espionnages massifs par des services de renseignement. En particulier, un tel système, bien construit, sera à même de résister à l'attaque du système informatique d'une administration ou à l'arrivée au pouvoir de personnalités politiques moins respectueuses des libertés individuelles. Laissé aux mains des citoyens, ce système serait potentiellement à même de se voir confier des données plus vastes et plus sensibles qu'un équivalent centralisé[26]. *A minima*, il serait ainsi possible, avec à chaque fois l'accord de chaque citoyen, de fusionner différentes données le concernant puisqu'il en resterait maître en toutes circonstances et qu'elles resteraient inaccessibles sans son accord.

2.3. LES PROMESSES DE L'IDENTITÉ BLOCKCHAINÉE : L'EXEMPLE DE LA BLOCKCHAIN DE DOCUMENTS CHIFFRÉS

Que devient le triptyque *personne / fournisseur d'identité / fournisseur de service* dans une nouvelle architecture blockchainée ? Beaucoup de solutions techniques différentes peuvent être envisagées : une idée pourrait être, par exemple, de déposer directement des documents authentifiés et chiffrés sur une blockchain[27].

Il est possible d'imaginer que le *fournisseur d'identité* signe électroniquement[28] un document numérique ou des données délivrées à la *personne*. Par la suite, le *fournisseur d'identité* peut d'ailleurs supprimer le document et la *personne* dépose une version chiffrée de ce document sur la blockchain. Seule la *personne* est à même d'autoriser ou non à un *fournisseur de service requérant* l'accès à chaque document ou aux données. Il n'a pas pour autant besoin de stocker ni de sécuriser lui-même ces données. Par exemple, un employé (*personne*) pourrait en un geste fournir à son employeur (*requérant*) tous ses diplômes, un document d'identité et un relevé d'identité bancaire sans avoir à stocker aucun de ces éléments lui-même ni avoir à demander l'accès à chaque *fournisseur d'identité* (les différentes institutions émettrices des diplômes, sa banque pour le relevé d'identité bancaire, la préfecture pour le document d'identité). Il récupérerait simplement sur la blockchain les documents demandés,

[26] En matière d'identité et compte tenu de tout ce que cela engage en termes d'ordre public, précisons que, quelle que soit la solution retenue, elle devrait garantir à l'État un accès à l'information essentielle et un contrôle sur ce qui ne relève pas de la vie privée proprement dite.

[27] D'autres solutions techniques sont bien entendu possibles et peuvent présenter d'autres avantages. Nous en rediscuterons dans la partie 2.4.

[28] Voir encadré sur le chiffrement.

les déchiffrerait et les fournirait à l'employeur qui pourrait alors vérifier grâce à la signature électronique de l'autorité certificatrice qu'ils sont authentiques et qu'ils appartiennent bien au futur employé. Une blockchain des clés publiques d'autorités certificatrices peut être mise en place pour faciliter la vérification des signatures. Seuls les documents demandés seront bien sûr transmis : d'autres documents (casier judiciaire, situation matrimoniale, dossier de santé, etc.) resteraient naturellement inaccessibles à l'employeur.

L'intérêt de la solution à choisir se mesure donc selon trois dimensions : coût, respect de la vie privée et contrôle *a posteriori*.

D'abord, en termes de coût, car dans cette architecture aucun acteur n'a besoin de stocker de manière extrêmement sécurisée et redondante les données. Chaque autorité certificatrice peut se dispenser de conserver des données sensibles et coûteuses à protéger efficacement. Cela présente notamment un avantage considérable pour les petits acteurs comme les mairies, les centres hospitaliers ou les médecins traitants. En France, l'Anssi contrôle les activités d'intérêt vital dont font partie certains fournisseurs d'identité qui pourraient être regroupés au sein de la blockchain. Dans la nouvelle architecture, seules quelques administrations régaliennes conservent les originaux des documents numériques, réduisant drastiquement les coûts des systèmes d'informations pour les autres acteurs. Un système à base de blockchain présente économiquement le même intérêt qu'une centralisation dans une base de données unique. Le nombre de systèmes d'informations à maintenir et sécuriser est ainsi réduit tout en améliorant l'interopérabilité des bases.

Cependant, contrairement à une solution centralisée, à l'évidence mal perçue par la société civile, une solution blockchainée présente un avantage clair en termes de vie privée et de sécurité des données. Dans cette architecture, aucun acteur mis à part la *personne* n'aurait accès à la totalité des documents. Par exemple, la préfecture en tant qu'autorité certificatrice aurait éventuellement accès aux documents d'identité qu'elle a certifiés – si elle en a gardé une copie – mais ne saurait rien, par exemple, du dossier médical de la *personne*, certifié par d'autres autorités. Crucialement, aucun acteur n'est en position d'empêcher l'accès aux autres documents : même le ***fournisseur d'identité*** initial ne peut revenir *a posteriori* sur sa signature si sa clé publique est stockée de façon irréversible et infalsifiable dans une blockchain. Cet avantage réel en termes de vie privée et de sécurité des données permettrait une identité numérique plus ambitieuse, fusionnant plus de données de nature plus sensible qu'une solution centralisée sans susciter des inquiétudes aussi fortes que les tentatives

précédentes évoquées plus haut, les citoyens restant alors maîtres de leur identité et des données qu'ils choisiraient ou non de transmettre.

Enfin, avec ce système décentralisé, il devient envisageable de demander aux administrations et aux tiers privés de ne conserver que le strict minimum. Ainsi, les petits détenteurs de données sensibles, les hôpitaux par exemple, pourraient ne pas conserver les données des patients et s'en remettre au système blockchainé, sans compromettre la vie privée de quiconque. À l'exception de cas très restreints et encadrés[29], les tiers n'ont aucune raison de partager des informations. Pour la Cnil, il devient plus aisé de vérifier que les données conservées sont bien le strict minimum, par exemple que les hôpitaux ne détiennent aucune donnée sur des patients déjà sortis, et qu'aucun dispositif de partage n'est mis en place à l'exception, par exemple, de dispositifs spécifiques et restreints. En cas d'infraction, la traçabilité et l'horodatage permis par la technologie blockchain pourront simplifier les procédures de contrôle de la Cnil.

2.4. LES DIFFICULTÉS DE MISE EN PLACE D'UNE IDENTITÉ BLOCKCHAINÉE

2.4.1. Le choix de la blockchain et sa publicité

La blockchain de documents chiffrés, présentée précédemment, ne constitue qu'un exemple parmi les multiples solutions potentielles. Dans le cas d'une blockchain d'identité, deux questions principales se posent :

A. que dépose-t-on sur la blockchain ?

B. qui assure le stockage décentralisé et valide les nouveaux blocs ?

Pour répondre à la question B, il est nécessaire d'introduire une distinction supplémentaire entre les blockchains : les blockchains publiques et les blockchains privées. Toute blockchain repose sur un certain nombre de nœuds capables de valider les nouveaux blocs. Dans le cas d'une blockchain publique, tout acteur qui le souhaite peut accéder au registre de la blockchain et valider des nouveaux blocs. Il n'y a pas de filtre, et chacun est libre d'y proposer une « transaction ». De même, il n'y a pas de présélection des mineurs, tout le monde « étant libre » de participer au protocole de validation des blocs. Les blockchains historiques comme Bitcoin ou Ethereum sont publiques. Dans le cas des blockchains privées, une présélection des acteurs peut être opérée à l'entrée. Ces blockchains sont majoritairement utilisées par

[29] Par exemple pour la lutte contre la fraude fiscale.

des regroupements d'acteurs privés. Il peut s'agir de blockchains de consortium où seuls des acteurs désignés peuvent proposer des transactions et valider des nœuds. Dans ces blockchains, les processus de validation peuvent être simplifiés et reposer sur le vote à la majorité simple d'acteurs, par exemple.

L'inclusion de technologie blockchain dans l'identité numérique peut associer de multiples combinaisons de solutions techniques reposant sur des réponses différentes aux questions A et B. Dans notre précédent exemple, nous avons proposé de déposer des documents certifiés et chiffrés (A). Pour restreindre la diffusion des documents, même chiffrés, les nœuds pourraient être limités à des acteurs présélectionnés – acteurs publics, acteurs certifiés ou même des instances européennes (B). Il s'agirait alors d'une blockchain privée, et les nouvelles accréditations pour le minage pourraient être données par un acteur-tiers de référence comme la Cnil. Une autre architecture possible pourrait consister en une blockchain publique contenant seulement des hash de documents. Cette blockchain publique permettrait uniquement d'assurer la traçabilité de documents qui pourraient, eux, être stockés sous forme chiffrée sur une blockchain privée reposant sur des nœuds de confiance.

L'usage de chaque type de blockchain peut présenter différents risques et avantages[30]. Par exemple, dans le cas de la blockchain de documents chiffrés, qu'adviendrait-il si l'accroissement de la puissance des ordinateurs et l'évolution des techniques cryptographiques permettaient de casser le chiffrement dans quelques années ?

[30] Voir à ce titre le tableau comparatif ci-après.

Avantages et risques des blockchains

	A - Que dépose-t-on sur la blockchain ?	B - Qui assure le stockage décentralisé et le « minage » de la blockchain ?	Inconvénients	Avantages
Blockchain de documents chiffrés	Les documents chiffrés directement	Blockchain publique	- Risque de piratage des documents si le chiffrement est cassé - Suppression des données assurée seulement par la suppression des clés de chiffrement - Éventuellement nécessaire de mettre en place une cryptomonnaie pour inciter les acteurs privés à participer	- Peu de perte des documents possibles, forte résilience aux attaques informatiques - Difficulté à supprimer des données sur la blockchain
		Blockchain privée	- Qui décide des serveurs autorisés ? - Plus grande centralisation suivant la diversité des participants	- Sécurité des données assurée même si le chiffrement est cassé - Possibilité de suppression des données chiffrées
Blockchain de hash	Les documents restent chez les fournisseurs d'identité ou chez les propriétaires des données. Il n'y a que les hash sur la blockchain	Blockchain publique	- Nécessite de stocker les documents ailleurs - Éventuellement nécessaire de mettre en place une cryptomonnaie pour inciter les acteurs privés à participer	- Impossibilité de casser le chiffrement de la blockchain pour voler les données - Possibilité de supprimer les documents chez les tiers
Solution hybride : blockchain privée de documents chiffrés et blockchain publique de hash et autorisations	Les documents chiffrés sont déposés sur la blockchain privée ; les hash, les clés publiques des autorités certificatrices et les règles d'accès sont gérées sur une blockchain publique	Hybride	- Éventuellement nécessaire de mettre en place une cryptomonnaie pour inciter les acteurs privés à participer à la blockchain publique	- Sécurité des données même si l'algorithme de chiffrement est cassé - Possibilité d'authentifier des documents même si les participants de la blockchain privée sont injoignables / bloqués par une attaque informatique - Délestage des fournisseurs des données dont ils n'ont pas expressément besoin

2.4.2. La difficile question de la clé privée

Par ailleurs, aussi fiables que soient les technologies de blockchain, elles reposent toutes sur un maillon crucial : la détention d'une clé secrète. Sans elle, il est impossible de lire ou d'apporter des modifications à la blockchain. Si celle-ci venait à tomber entre les mains d'un acteur malveillant, il pourrait usurper l'identité du propriétaire légitime et effectuer des transactions en son nom. Néanmoins, l'avantage de la solution blockchain est que la responsabilité d'une éventuelle perte de cette clé secrète incombe à l'individu, qui est de fait plus responsabilisé[31]. C'est la contrepartie naturelle d'une meilleure maîtrise de ses propres données. Aujourd'hui, les utilisateurs de blockchain recourent à plusieurs solutions pour sécuriser la clé, depuis un simple chiffrement de la clé au moyen d'un mot de passe à des systèmes plus baroques. Des nouveaux périphériques physiques spécifiquement prévus pour – théoriquement du moins – stocker une clé de manière sécurisée sont ainsi apparus ces dernières années. On remarque toutefois que les détenteurs de cryptomonnaie, principaux usagers des blockchains à l'heure actuelle, ont aussi recours à de simples feuilles de papier dans des coffres-forts.

De manière générale, aucune de ces méthodes ne donne entière satisfaction. Les exemples de portefeuilles de Bitcoins piratés sont légion, des particuliers aux plus gros sites Internet d'échange qui détiennent des cryptomonnaies pour le compte de tiers. Une technologie censée faire disparaître les tiers de confiance en garantissant cryptographiquement la sécurité d'une base de données est de fait, aujourd'hui, infiniment moins sécurisée que n'importe quelle banque en ligne. C'est gênant pour un actif à vocation plutôt spéculative comme le Bitcoin. C'est une limitation insurmontable si l'on prétend dématérialiser sur une blockchain des données médicales, par exemple.

Un système d'identité numérique par blockchain comme celui décrit plus haut nécessiterait que chaque personne physique ou morale puisse conserver à tout moment une clé privée de chiffrement. C'est elle qui permettrait d'apporter des modifications ou de nouveaux documents sur la blockchain ou de fournir l'accès à ses informations. Ainsi, comme évoqué plus haut, l'usage de cette technologie supposera dès lors une responsabilisation accrue du citoyen.

[31] Il faudrait toutefois prévoir un mécanisme de secours, à l'image de ceux qui existent lors du vol d'une carte bleue par exemple.

La puissance publique doit fournir aux citoyens les moyens de disposer d'une clé privée sécurisée. Si la forme exacte doit faire l'objet d'études techniques plus poussées, cette clé pourrait être un mot de passe stocké sur des périphériques de stockage sécurisés éventuellement biométriques ou du moins avec un code PIN. Cette clé privée sécurisée pourrait à ce titre être stockée sur des cartes d'identité électronique.

Suivant les données déposées sur la blockchain, il peut être nécessaire de prévoir des solutions pour les récupérer dans des situations plus ou moins dégradées, de la perte du support électronique à l'inconscience, voire au décès du propriétaire des données. De fait, des solutions reposant sur des tiers de confiance existent déjà pour gérer sans autorité centrale la perte de la clé. Au lieu de demander la réédition d'une clé à un organisme central – ce qui, encore une fois, nierait le caractère décentralisé du système – il est possible de concevoir des mécanismes où des tiers de confiance choisis par les utilisateurs permettent de retrouver une clé perdue.

2.4.3. Quelques exemples de solutions d'ores et déjà existantes

La question de l'identité numérique blockchainée a d'ores et déjà été abordée par des précurseurs, et des solutions, principalement privées, sont en développement. Ces dernières reproduisent certaines des fonctionnalités que nous proposons.

Civic par exemple est une solution d'identité numérique qui s'attaque au problème des règles de « Know Your Customer » (KYC). Le modèle est le suivant : l'utilisateur de Civic installe l'application sur son téléphone. Il envoie via cette application des documents d'identité comme un permis de conduire. Civic ou un de ses partenaires certifie l'authenticité du permis et stocke un « hash » de ce permis sur la blockchain. Civic n'a alors plus besoin de conserver le document d'origine et le supprime de ses serveurs. Lorsqu'une banque, par exemple, veut vérifier l'identité de l'utilisateur, celui-ci peut fournir son permis de conduire. La banque ne sait pas *a priori* si le permis n'est pas un faux, et le vérifier peut être coûteux ou compliqué. En revanche, si elle est cliente de Civic, elle peut vérifier qu'un hash du permis est bien sur la blockchain de Civic, s'assurant ainsi que la pièce est authentique. Civic prévoit à terme un écosystème autour d'un jeton, le CVC, récompensant des tiers qui valident les documents

d'utilisateurs[32]. Civic se positionnerait ainsi comme une plateforme d'échange entre fournisseurs et consommateurs d'identité. La différence par rapport au système décrit dans cette note est que Civic ne permet pas de stocker des documents d'identité de façon sécurisée, ce qui suppose que l'utilisateur en garde une copie et puisse facilement en faire refaire en cas de perte. Il ne permet donc pas à des petites institutions de s'affranchir de la charge de conserver les données. Par ailleurs, il s'agit évidemment d'un acteur privé utilisant la technologie du Bitcoin, ce qui n'est pas acceptable pour stocker et authentifier les données fiscales ou de santé des citoyens français.

IDChain est une autre solution « blockchainée » d'identité numérique. Celle-ci repose sur deux blockchains, une, privée, contient les données chiffrées tandis que l'autre, publique, sert à gérer les autorisations et les paiements. Une institution peut donc stocker des informations sur ses clients dans la blockchain privée et vendre des droits de consultation dans la blockchain publique avec, là encore, un système de jetons similaire au Bitcoin. Cette solution ressemble en grande partie à la solution hybride que nous présentons, à un détail près : l'utilisateur dont les données sont vendues n'est mentionné nulle part dans le dispositif. De fait, celles-ci sont fournies par des institutions comme les banques et stockées sur la blockchain privée, *a priori* sans chiffrement ou avec une clé de chiffrement accessible à tous les participants de la blockchain privée. Si ce dernier aspect est inconcevable en France, l'utilisation de smart contracts sur une blockchain publique pour gérer les autorisations d'accès peut être une piste intéressante. Cela suppose toutefois qu'il soit possible de le faire en conservant un chiffrement des données par leur propriétaire légitime.

A contrario, certains projets proposent des solutions de blockchains de documents chiffrés centrées sur le propriétaire de l'identité qui fournit à des *fournisseurs d'identité* des documents à certifier. Celui-ci signe les documents et les inscrit chiffrés par une clé dans la blockchain. La clé est ensuite délivrée à l'utilisateur et supprimée des serveurs du *fournisseur d'identité*, assurant le contrôle de l'identité par l'utilisateur lui-même. Lorsque celui-ci cherche à prouver son identité à un requérant, il peut donner sélectivement accès à certaines données pendant un temps restreint au moyen de smart contracts. C'est ce type de modèle vers lequel nous proposons de tendre, à ceci près que dans un système d'identité numérique animé par

[32] Sur le modèle d'un certain nombre d'autres « *utility tokens* » (jetons utilitaires), ces jetons pourront ensuite être librement échangés sur un marché, leur valeur sous-jacente venant du fait qu'ils pourront être utilisés pour acheter les services de la plateforme, c'est-à-dire des services d'identification. Ce type de modèle économique n'a pas encore connu de véritable succès.

l'État, le *fournisseur d'identité* serait généralement l'administration ou l'acteur ayant produit le document certifié. Celui-ci n'en serait pas moins rendu clé en main à son juste propriétaire : le citoyen.

De nouvelles technologies blockchain d'identité numérique continuent à se développer, et des géants du numérique entendent aussi se repositionner sur le sujet[33]. Pour un usage généralisé à l'échelle d'un pays comme la France, il sera nécessaire de s'attacher à vérifier la capacité de passage à l'échelle de ces technologies. Avant d'envisager un déploiement complet, des expérimentations pourraient être réalisées.

2.5. LA BLOCKCHAIN POURRA ÊTRE INTRODUITE PROGRESSIVEMENT DANS UNE IDENTITÉ RENOVÉE ET ÊTRE EUROPÉENNE

Malgré leur pertinence, la relative urgence de mise en place d'une solution d'identité numérique améliorée à l'horizon 2019 ne laisse que peu de temps pour les analyses techniques et la mise en place d'une solution entièrement blockchainée. L'inclusion de technologies blockchain pourra venir dans un second temps et améliorer encore une identité numérique d'ores et déjà renforcée. Certaines briques technologiques, à l'image de la carte d'identité électronique numérique, peuvent être réutilisées dans le cadre d'une solution plus globale incluant l'utilisation de la blockchain.

D'ici là, des expérimentations ou des projets simples de blockchain pourront permettre d'éprouver la technologie. Il peut s'agir par exemple, dans un premier temps, d'utiliser une blockchain privée pour rapprocher de manière décentralisée des bases de données publiques. Outre que cela est intéressant du point de vue de l'identité numérique, cela permettra de continuer à faire monter en compétence les acteurs publics et les éventuels fournisseurs privés. À terme, et comme nous l'avons déjà évoqué, des lancements ciblés dans des collectivités locales pilotes d'expérimentation de solutions plus globales (par exemple la blockchain de documents chiffrés ou la blockchain hybride) seront peut-être nécessaires avant d'envisager un déploiement général en France.

Une autre possibilité, non exclusive d'ailleurs, est de repositionner le sujet de l'identité numérique au niveau européen. Comme le montre les exemples des règlements RGPD et eIDAS, l'Union européenne s'est déjà montrée motrice sur ces sujets. Pour regagner la

[33] Voir à ce titre les annonces de Microsoft sur l'identité numérique et la blockchain pour donner une identité numérique aux sans-papiers à l'échelle mondiale.

confiance des citoyens européens, de plus en plus défiants et tentés par les populismes de droite ou de gauche, un projet marquant pourrait être d'instituer une identité digitale au niveau européen en sus ou non de l'identité numérique de son pays membre.

Ceci permettrait de reconnecter les Européens avec l'Europe. L'usage quasi quotidien d'une identité numérique permettrait à tout citoyen de renforcer son sentiment d'appartenance en s'identifiant grâce à une clé européenne tout en gardant le contrôle de ses données[34]. En choisissant une solution blockchainée, l'Europe pourrait garantir aux citoyens européens une transparence et une fiabilité totales dans l'utilisation de leurs données tout en contribuant à bâtir la brique de base d'une Europe numérique. En se positionnant comme fournisseur d'identité numérique, l'Europe pourra d'ailleurs permettre aux États membres aux identités numériques les moins avancées de rattraper leur retard.

CONCLUSION

L'identité numérique est devenue un actif clé tant pour la souveraineté des États et des individus que pour leur développement économique. Les fournisseurs d'identité à la fois publics et privés sont nombreux. La simplification des procédures administratives, le marché numérique européen, la nécessaire question de souveraineté pour l'identité numérique rendent nécessaire l'amélioration du système public français d'identité numérique. Les pistes d'amélioration de l'identité numérique en France sont nombreuses et peuvent avoir recours ou non à la technologie blockchain. La blockchain est pertinente si les citoyens veulent reprendre contrôle de leurs données, un facteur clé dans l'acceptation et l'adoption de systèmes d'identité numérique nationaux. Elle peut permettre en sus de réduire les coûts, d'améliorer la protection de la vie privée, de simplifier le contrôle et l'audit des fournisseurs d'identité et des tiers requérants.

Il existe de multiples solutions techniques présentant des caractéristiques différentes : à ce titre, il est possible d'utiliser des solutions partiellement ou complètement basée sur la blockchain. Selon les choix technologiques retenus, l'usage de blockchain entraînera une responsabilisation accrue des citoyens, qui nous semble nécessaire et bienvenue. Si des

[34] Notons que le sentiment d'appartenance passe également et même surtout par des ancrages affectifs très différents : la langue, les épreuves historiques, les rituels.

solutions intégrées existent, leur usage à l'échelle d'un pays comme la France n'a jamais été éprouvée.

La relative urgence de mise en place d'une solution d'identité numérique améliorée à l'horizon 2019 ne laisse que peu de temps pour les analyses techniques et la mise en place de la solution. Nous proposons donc que les technologies blockchain puissent être ajoutées dans un second temps à une identité renforcée, certaines briques technologiques, comme la carte d'identité électronique numérique, pouvant être réutilisées dans le cadre d'une solution plus globale incluant l'utilisation de la blockchain. Aussi, nous recommandons d'éprouver la technologie en y recourant le plus souvent possible (notamment pour le rapprochement décentralisé de bases de données publiques) ou en lançant dans des collectivités locales pilotes des expérimentations de solutions plus globales, avant d'envisager un déploiement général en France. Enfin, nous proposons d'envisager également l'utilisation d'une telle solution à l'échelle européenne afin de reconnecter les citoyens avec l'Europe.