DOCTRINE

PROSPECTIVES

La blockchain à l'aune de la feuille de route du numérique en santé

Perspectives de la blockchain à l'aune des objectifs nationaux de numérisation accélérée du secteur de la santé dans le cadre de la stratégie « Ma Santé 2022 » portée par le gouvernement.

Dans un article du magazine Capital publié sur son site internet le 15 avril 2019[1], Bruno Le Maire affirmait que « *le développement de l'écosystème blockchain est une priorité pour le gouvernement* ». Ces propos s'inscrivaient dans la droite ligne de l'adoption de la loi Pacte, du 22 mai 2019[2] qui a permis à la France de franchir de nouvelles étapes pour favoriser le développement de la blockchain, en mettant en place le cadre légal pour procéder à des investissements en jetons numériques (ICO émises en France). L'offre au public de jetons (Initial Coin Offering ou ICO) est une opération de levée de fonds par laquelle une société se finance au moyen d'une émission de jetons[3] (tokens), auxquels les investisseurs souscrivent essentiellement par un paiement en crypto-monnaie. Ce système repose sur la technologie informatique blockchain.

La loi Pacte a instauré un visa optionnel de l'AMF, qui pourra être sollicité par les porteurs de projets qui le souhaitent. En sollicitant un visa de l'AMF, ils s'engagent à respecter certaines règles et à donner certaines garanties, contrairement aux autres émetteurs.
Ces avancées législatives françaises sont en cohérence avec les efforts menés au niveau européen. Début 2018, la Commission européenne a confirmé une enveloppe destinée aux projets blockchain via son programme Horizon 2020.

La majorité des fonds ont été versés à des instituts de recherche, laboratoires et universités. Des entreprises nationales ou internationales en ont également bénéficié. Les projets qui ont reçu le plus de financement sont dans le secteur de la cybersécurité (26% du montant total alloué), suivi par l'IoT (22%) et la santé (19%)[4].

France Stratégie[5] définit la blockchain dans les termes suivants : « *Il s'agit d'une nouvelle façon de stocker de l'information, de la préserver sans modification, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables. Ces nouvelles données peuvent résulter de l'exécution d'une opération, d'une transaction ou de l'exécution « automatique* » d'un programme informatique. Elles sont inscrites sur l'équivalent d'un vaste registre « *distribué* », c'est-à-dire partagé par tous les membres du réseau, un système qui permet transparence et audibilité. »

Cette technologie présente des caractéristiques séduisantes dont les plus communes sont les suivantes exposées dans le même rapport.

Il s'agit d'un système :

- décentralisé. Chaque participant possède une copie constamment mise à jour du grand registre. Il n'y a pas de serveur central mais une gestion collaborative qui est en principe une protection contre les falsifications et autres attaques. Cette désintermédiation doit aussi être un facteur de baisse des coûts.
- transparent : le registre et donc l'historique des transactions est consultable en permanence par n'importe quel internaute (ou par tous les membres du réseau). Il est ainsi possible d'assurer la traçabilité intégrale d'un actif ou d'un produit ayant fait l'objet d'une transaction via une blockchain. Un participant intervient sous pseudonyme, mais toutes ses opérations sont traçables.
- fiable. La blockchain est infalsifiable et inviolable. Une fois enregistrées dans les blocs, les informations ne peuvent plus être modifiées ni supprimées. Le système décentralisé, en multipliant les copies, offre également une garantie contre le piratage.

Dans ce contexte, il est intéressant d'examiner la feuille de route du numérique en santé[6] présentée

par la ministre chargée de la Santé, le 25 avril 2019, dans le cadre de la stratégie « *Ma Santé 2022* » portée par le gouvernement actuel et de mettre en perspective les caractéristiques de la blockchain à l'aune des objectifs nationaux de numérisation accélérée du secteur de la santé.

Des usages nouveaux de la blockchain peuvent-ils être envisagés, par exemple dans le cadre de la création de nouveaux services nationaux à disposition des professionnels de la prise en charge et des usagers ? Cela nécessiterait-il de réguler l'usage de cette technologie, afin de donner aux acteurs de terrain des repères sur la confiance pouvant lui être accordée ?

La délégation du numérique en santé (DNS) mise en place par le décret du 20 décembre 2019[7], et son bras armé, l'agence du numérique en santé (ANS)[8] en lien avec les directions et autres acteurs concernés, est chargée de définir et de mettre en œuvre la stratégie du numérique en santé, notamment sur le volet de la sécurité des systèmes d'information manipulant des données de santé. La DNS doit proposer annuellement une feuille de route et identifier les moyens nécessaires à sa réalisation. Elle a d'ores et déjà renforcé dans le code de la santé publique par la loi n° 2019-774 du 24 juillet 2019[9] les dispositions consacrées à la sécurité et à l'interopérabilité des systèmes d'information de santé.

Elle a également inscrit dans la loi la création pour tous d'un espace numérique de santé (ENS)[10]. Créé dès la naissance pour chaque citoyen, cet espace accessible gratuitement sur différents supports, lui permettra de gérer ses données de santé et de participer à la construction de son parcours de santé en lien avec les différents professionnels, établissements et acteurs de santé. Il sera possible d'accéder via l'ENS notamment au Dossier médical partagé, au Dossier pharmaceutique ou encore à l'ensemble des données relatives au remboursement de ses dépenses de santé, messagerie sécurisée, agenda sécurisé, avec un portail d'accès à des applications référencées et des outils de télésanté. Comment ces applications seront intégrées à l'ENS ? La même question peut se poser pour le bouquet de services des professionnels de santé dont l'objectif est de leur éviter un accès à des applications dispersées et pas toutes fiables (action 16 de la feuille de route du numérique en santé).

Sera-t-il fait recours à la blockchain ? Si le choix technologique de recourir à la blockchain était fait, aurait-il un impact juridique ? L'examen du cadre juridique actuel n'évoque pas pour l'instant ce sujet. Il est uniquement prévu l'obligation de respecter des référentiels de sécurité, d'interopérabilité, et d'engagements éthiques. Ces référentiels vont-ils évoluer afin de l'intégrer ?

Au-delà du cadre juridique propre aux données de santé, parler de la blockchain amène en effet à s'interroger sur la capacité à l'utiliser pour faire valoir des droits devant un juge. Un des atouts qui la caractérise réside dans le fait que le document électronique produit à l'appui de la blockchain pourrait avoir une plus grande force probante que le papier. Cependant, il resterait à convaincre le juge du degré de confiance dans le cadre d'un usage totalement dématérialisé. En l'état du droit, aucun texte ne détermine la portée juridique au sens probatoire des éléments inscrits sur un protocole technique. Dès lors qu'il ne fait pas partie des moyens de preuve actuellement reconnus au plan juridique, il appartient au juge de déterminer leur valeur probatoire, au vu des circonstances de l'espèce. La question qui émerge est alors la suivante : faut-il produire de nouvelles règles pour clarifier le positionnement et la valeur juridique de la blockchain dans notre droit ? et pour quels usages dans la santé ?
Dans le domaine de la santé, en raison de la particulière sensibilité des données produites, leur dématérialisation a fait l'objet, à l'occasion des dernières lois de santé qui se sont succédées à brève échéance ces dernières années, de dispositions législatives et réglementaires destinées à aider les acteurs à avoir confiance dans le numérique en santé. Parmi ces dispositions issues du cadre juridique du numérique en santé qui méritent d'être analysées (II), certaines pourraient servir à l'appui de nouveaux cas d'usage de la blockchain qui pourraient naître de la feuille de route nationale du numérique en santé (I), dans le contexte de la crise sanitaire actuelle particulièrement propice au recours aux nouvelles technologies.

EXAMEN DES CARACTÉRISTIQUES DE LA BLOCKCHAIN DANS LA PERSPECTIVE D'UN USAGE DANS LE DOMAINE DE LA SANTE

L'action 16 de la feuille de route du numérique en santé[11] est consacrée au projet de mettre à disposition des professionnels de santé un bouquet de services leur permettant d'accéder de manière sécurisée aussi bien aux services offerts par les acteurs publics (services socles nationaux ou régionaux, fournis par l'État, ses opérateurs et l'Assurance Maladie) qu'aux services proposés par les acteurs privés. Il est précisé que le bouquet de services s'appuiera sur les référentiels socles : Identifiant national de santé, référentiel des acteurs.
Ces référentiels socles sont les référentiels de sécurité et d'interopérabilité mentionnés à l'article L1110-4-1 et L1110-4-2 du code de la santé publique. Il n'est pas fait mention de la blockchain ni dans le bouquet de services ni dans les référentiels. Cela signifie-t-il qu'il n'existe aucune application possible ? Certains services existants, dont le DMP, semblent apporter un niveau de confiance dans la fiabilité du dispositif en présentant des caractéristiques similaires à celles de la blockchain. Le besoin d'évoluer vers cette technologie ne s'est pas fait ressentir semble-t-il. Ne serait-elle pas utile pour de nouveaux services ?

Bouquet de services et blockchain

Pour l'instant, il n'est pas fait usage à notre connaissance de la blockchain dans le Dossier médical partagé[12]. Anciennement dossier médical personnel, créé par la loi du 13 août 2004, renommé en 2016 Dossier médical partagé, sa gestion a été transférée de l'ASIP Santé à la Caisse nationale d'assurance maladie. Dans son mode de fonctionnement actuel, le DMP est conçu comme un système centralisé dans un but de protection des données de santé ainsi collectées.

S'il n'y a pas d'usage envisagé de la blockchain à ce jour dans le DMP d'après les communications faites à son sujet, son modèle centralisé de gestion pourrait évoluer sans nécessairement remettre en cause la gouvernance au niveau national de cet outil. En effet, on peut considérer que le DMP présente des caractéristiques qui, pour certaines d'entre elles, peuvent amener à réfléchir à l'usage de la blockchain. Nous en mettrons trois en avant :

- son fonctionnement nécessite un accès à tous les professionnels et établissements qui doivent l'alimenter ;
- la maîtrise par la personne concernée sur ses données : le DMP donne aux patients un droit de regard inédit sur leurs données de santé. Ces derniers peuvent accéder rapidement et en toute sécurité aux informations les concernant et ils ont la capacité de les compléter par des informations utiles (anciennes pathologies ou éventuelles allergies par exemple) mais aussi de pouvoir décider des professionnels de santé autorisés à y accéder ;
- la transparence : caractéristique notable, ce système national de données de santé est organisé depuis sa création pour permettre l'accès aux traces des « *actions réalisées sur le dossier médical partagé, quel qu'en soit l'auteur, au titulaire du dossier, au médecin traitant, aux professionnels de santé dont l'auteur des informations faisant l'objet de ces traces* » (article R1111-31 du code de la santé publique) ;

l'interopérabilité entendue ici comme la capacité à autoriser que deux systèmes différents se reconnaissent et puissent opérer des transactions. Pour pouvoir s'interfacer avec le DMP, il faut que l'éditeur respecte les conditions contractuellement définies. En outre, les logiciels doivent au préalable être autorisés par le Centre national de dépôt et d'agrément (CNDA). Le processus d'autorisation vise à s'assurer de la conformité d'un logiciel aux spécifications définies dans le guide d'intégration des logiciels de professionnels de santé, afin de garantir l'interopérabilité et la sécurité du service. La DMP-Compatibilité peut être complète (toutes les interfaces) ou partielle.

Tous ces objectifs nécessitent de s'assurer, d'une part, de la confiance que l'on peut avoir, d'une part, dans les personnes ou les machines qui accèdent au DMP et, d'autre part, de l'absence de modification des données qui sont conservées dans le DMP.

L'usage de la Blockchain pourrait également être utile dans le cadre de la mise en œuvre des nouveaux services nationaux. A titre d'exemple, le bouquet de services défini à l'action 16 de la feuille de route du numérique en santé est présenté comme devant permettre à terme « *de simplifier l'exercice des professionnels de santé, en miroir de l'Espace Numérique de Santé. Il aura pour vocation principale de faciliter l'accès à l'ensemble des outils dont un professionnel a besoin dans son exercice quotidien, sans qu'il ait à se ré-identifier à chaque changement d'outil. Un médecin pourra par exemple accéder au portail de suivi d'un patient utilisant une application de suivi du diabète sans sortir de son univers logiciel. Ceci passe par une interopérabilité accrue entre les différents outils numériques. Le bouquet de services permettra également aux professionnels de mieux connaître l'offre de services numériques publique et privée disponible. Ce bouquet de services numériques doit répondre à différents types de besoins, via une offre ouverte et modulable pouvant prendre différentes formes: un catalogue de services accessibles à partir des logiciels métiers par appel contextuel ou par intégration forte (API), mais aussi un portail web incluant une interface utilisateur et proposant un ensemble minimal de services " clés en main ". Cette évolution doit permettre aux offreurs de services de passer d'une offre construite en silo à une offre ouverte permettant l'intégration de services en provenance de tiers.* »

L'objectif du bouquet services est de simplifier la vie au quotidien des professionnels qui ne devront plus avoir besoin de se reconnecter pour passer d'un service à l'autre. A ce jour, il est prévu que l'accès unifié sera sécurisé par un dispositif qui permettra l'identification, l'authentification et les habilitations des acteurs de santé.

Ces mesures de sécurité sont formalisées dans les référentiels dits socles. Il s'agit des référentiels de sécurité et d'interopérabilité mentionné à l'article L1110-4-1 du code de la santé publique. La Blockchain y trouve -t-elle sa place ?

Référentiels de sécurité du secteur de la santé et blockchain

La loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (dite loi de Santé) a modifié l'article L.1110-4-1 du code de la santé publique, qui prévoit les référentiels de sécurité et d'interopérabilité dans le secteur de la santé.

La loi a précisé le champ des acteurs tenus de respecter l'obligation de conformité de leur système d'information utilisés pour traitement des données de santé à caractère personnel, aux référentiels d'interopérabilité et de sécurité. Il s'agit des catégories d'acteurs suivants :

- les professionnels de santé et les personnes exerçant sous leur autorité, les établissements et services de santé, le service de santé des armées et tout organisme participant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le code de la santé publique ;
- les professionnels des secteurs médico-social et social et les établissements ou services des secteurs médico-social et social mentionnés à l'article L.312-1 du code de l'action sociale et des familles ;
- les organismes d'assurance maladie, ayant pour finalité principale de contribuer directement à la prévention ou au suivi du parcours de soins des patients.

L'article L. 1110-4-1 précité précise en outre le mécanisme d'élaboration des référentiels, qui s'effectue en concertation avec les représentants des secteurs susvisés. Il rappelle que les référentiels doivent être approuvés par arrêtés du ministre chargé de la Santé. L'avis de la Cnil n'est plus imposé par le texte.

A ce jour, les référentiels de sécurité sont regroupés au sein de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S). La PGSSI-S se compose de 2 types de documents :

- des référentiels, pour fixer et décrire les exigences de sécurité des systèmes d'information portant sur : l'identification et l'authentification des acteurs de santé et médico-sociaux ; l'identification des patients (INS) et usagers du système de santé ; l'imputabilité (gestion de preuve et traçabilité) ; la force probante des documents de santé.
- des guides, pour accompagner les acteurs de santé, décrivant les bonnes pratiques organisationnelles et techniques, à appliquer (par exemple : guide d'élaboration et de mise en œuvre d'une politique de sécurité de système d'information, destruction sécurisée de données, etc.).

La sécurité des systèmes nationaux s'appuie sur ces référentiels parmi lesquels figurent ceux qui portent sur l'identification et l'authentification des acteurs. Pourquoi mettre en évidence ces deux thèmes ? Parce qu'ils ne sont pas sans lien avec les modalités de fonctionnement de la blockchain, par exemple dans le cadre d'une blockchain publique, avec possibilité d'intervention le cas échéant des pouvoirs publics pour gérer l'identification de façon centralisée.

Le référentiel d'identification des professionnels contient les données clés d'identification fiables et univoques de l'ensemble des professionnels qui ont besoin d'accéder, d'échanger ou de partager des données de santé au titre de soins, de coordination ou de régulation des services. Ces données d'identification sont enregistrées et certifiées par des tiers de confiance (actuellement, ce rôle est assumé par les ordres professionnels, les agences régionales de santé, le service santé des armées) désignés en tant qu'autorité d'enregistrement par les textes. L'identification d'un utilisateur est le début de la chaîne de confiance. L'authentification consiste à apporter la preuve de son identité. Elle permet aux services numériques de s'assurer de l'identité d'un professionnel au moyen d'éléments de preuve qu'il possède. Pour bénéficier d'une authentification, un professionnel doit disposer d'un identifiant.

L'actuel référentiel consacré à l'authentification[13] prévoit l'authentification directe des professionnels en s'appuyant sur les solutions existantes (carte de professionnel de santé (CPS), OneTime Password (mot de passe à usage unique (OTP),...) et des solutions complémentaires ou alternatives adaptées aux usages en mobilité (e-CPS, Time-Based One-Time Password (TOTP)...). Une nouvelle version du référentiel est attendue pour que les moyens d'authentification des professionnels par les services numériques de santé soient présentés de façon harmonisée avec les niveaux inscrits dans le règlement electronic IDentification, Authentication and trust Services (eIDAS). Elle inclura des moyens d'authentification indirects.

A ce jour, le référentiel d'authentification préconise des moyens d'authentification à l'appui de cartes et certificats fournis par l'Infrastructures de gestion de clés santé (IGC Santé). Une IGC, Infrastructure de gestion de clef (IGC) - ou « *Public Key Infrastructure* » en anglais - est un système assurant la gestion de certificats électroniques au sein d'une communauté d'utilisateurs. Une IGC est notamment composée d'au moins une autorité de certification, et peut comprendre au moins une autorité d'enregistrement chargée de vérifier les données d'identification des utilisateurs de certificat électronique, et de contrôler les droits liés à l'utilisation des certificats électroniques conformément à la politique de certification. L'IGC Santé est une infrastructure de gestion de clés cryptographiques (IGC) opérée par l'Agence des systèmes d'information partagés de santé (ASIP-Santé) devenue Agence du numérique en santé (ANS), à l'appui de l'Imprimerie nationale[14].

Les certificats émis par l'ANS permettent d'identifier les acteurs du secteur, personnes physiques et organisations. Ils attestent également de la qualité des pratiques de gestion des clés publiques mises en œuvre par ces autorités. Ils peuvent être révoqués en cas de défaillance.
Dans la blockchain, le principe d'authentification d'un utilisateur consiste à lui faire signer un message avec sa clef privée. Le fournisseur de service va vérifier la signature du challenge grâce à la clef publique de l'utilisateur, qui est stockée dans la blockchain. Cela ressemble au mécanisme d'authentification par certificat, à la différence qu'il n'y a plus de point central comme dans l'IGC mais un réseau décentralisé.

Dans sa version actuelle, le référentiel d'authentification ne fait donc pas mention de la blockchain. Mais il s'appuie sur l'IGC qui par nature fonctionne sur un système de registre permettant d'avoir des informations publiques comme la liste des certificats révoqués et d'autres informations privées conservées par un tiers de confiance.

Selon le rapport établi par le think tank Terra Nova[15] de 2018 consacré à l'usage de la blockchain pour l'identité numérique du citoyen, « *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 . [...] 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* ».

Il est intéressant de réfléchir à ce modèle pour identifier et authentifier les professionnels de santé, en tenant compte des modalités d'exercice très diversifiées qui sont les leurs et nécessitent par conséquent d'intégrer dans la réflexion les personnes morales au sein desquelles ils exercent.

La complexité d'englober l'ensemble de ces traits d'identité explique peut-être au moins partiellement les raisons pour lesquelles les efforts se sont à ce jour plutôt centrés sur le citoyen, également usager du système de sa santé.

La Direction interministérielle du numérique ex- DINSIC[16] a mis en place depuis 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. Le service vise les particuliers (déjà disponible), les agent publics (en cours) et les entreprises (à partir de 2020).

Dans le domaine de la santé, il est prévu la mise en place de différents niveaux de garantie « *pour assurer l'identification électronique aux services de santé en ligne, avec l'objectif, à terme, d'être de niveau de garantie « substantiel* » lorsque des données de santé à caractère personnel sont traitées ». L'application Carte Vitale (ApCV) est présentée comme un mécanisme de référence pour l'identification électronique. Les travaux devront être menés en lien avec la généralisation de l'utilisation de France Connect, condition indispensable pour permettre l'accès à une variété de fournisseurs d'identité et une fluidification des échanges de données entre les services. Il n'est pas à ce stade fait de référence dans ces projets à la technologie blockchain et à ses apports potentiels.

Il existe de nombreux cas d'usages pour lesquels le citoyen et usager du système de santé devrait avoir la capacité de s'assurer par lui-même de l'intégrité des données qu'il génère lui-même et de l'accès à ces données (par exemple, ses directives anticipées). La blockchain permet sur la base d'un système décentralisé de mettre tous les participants sur un pied d'égalité, sans qu'aucun d'entre eux ne puisse agir sans en informer ses pairs. La blockchain ne pourrait-elle pas être un moyen au service de ces fins ?

Ces chantiers nationaux de modernisation de la gestion de l'identité numérique dans tous les domaines d'activité dont la santé que ce soit celle des usagers comme celles des professionnels et des structures dans lesquelles ils exercent sont majeurs. Ils sont d'ores et déjà investis par les Gafa. Des initiatives d'autres acteurs privés se développent, comme Decentralized Identity Foundation et visent à créer un système d'identité décentralisé, indépendant d'une organisation centralisée - comme un registre gouvernemental - pour vérifier l'identité d'une personne. Dans un tel système, le stockage des données et la puissance de calcul doivent être autonomes - tout comme les identités sur le système lui-même.
Outre ses liens avec la certification des identités des personnes, la blockchain peut être également appréhendée au vu de ses caractéristiques intrinsèques à l'aune d'un autre type de référentiels du secteur de la santé, ceux relatifs à l'interopérabilité.

Référentiels d'interopérabilité du secteur de la santé et blockchain

Une des caractéristiques de la blockchain serait de faciliter l'interopérabilité des systèmes d'information. Dans le domaine de la santé, les conditions de son développement ont été largement renforcées par la dernière loi de santé précité de 2019. Il semble qu'il faille distinguer entre plusieurs formes d'interopérabilité.
Le législateur a modifié l'article L.1110-4-1 pour préciser, que les référentiels d'interopérabilité sont fondés sur des « *standards ouverts en vue de faciliter l'extraction, le partage et le traitement des données de santé dans le cadre de la coordination des parcours de soins, de l'amélioration de la qualité des soins et de l'efficience du système de santé ou à des fins de recherche clinique* ».

Le nouvel article L.1110-4-2 du code de la santé publique issu de la même loi prévoit la mise en place d'une procédure d'évaluation et de certification permettant d'attester la conformité d'un système d'information ou d'un service ou outil numérique en santé aux référentiels d'interopérabilité mentionnés à l'article L. 1110-4-1 précité. La procédure d'évaluation et de certification sera définie par décret en Conseil d'Etat. En pratique, pour les éditeurs, il est envisagé de leur mettre à disposition des outils de tests pour leur permettre de tester leurs produits. Les résultats de ces tests seront publiés. Ces nouvelles règles imposent aux éditeurs de distribuer des logiciels conformes aux référentiels d'interopérabilité.

Le cadre de référence est à ce jour principalement le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS). Il contient des spécifications qui permettent aux SIS d'échanger et partager des données de santé.

Aux côtés de l'obligation désormais inscrite dans la loi à l'article L1110-4-2 du CSP de se conformer à ce CI-SIS, d'autres modes d'interopérabilité sont également mis en avant.
L'action 16 de la feuille de route du numérique en santé prévoit en effet que « *le bouquet de services numériques doit répondre à différents types de besoins, via une offre ouverte et modulable pouvant prendre différentes formes : un catalogue de services accessibles à partir des logiciels métiers par appel contextuel ou par intégration forte (API), mais aussi un portail web incluant une interface utilisateur et proposant un ensemble minimal de services « clés en main* ».

Cette forme d'interopérabilité, entendue comme l'organisation d'accès aux services du portail via appels contextuels ou par interface interopérable, pourrait-elle bénéficier de la technologie de la blockchain ?
Si les systèmes nationaux déjà existants n'y recourent pas, les nouveaux services pourraient être réfléchis en intégrant les avantages de cette technologie, par exemple pour faciliter l'amarrage d'applications sur le bouquet de services ou encore à l'espace numérique de santé.

Examen de la place de la blockchain dans le cadre juridique du numérique en santé

Il ne s'agit pas ici de faire l'apologie de cette technologie mais d'examiner dans quelle mesure ce système décentralisé peut concourir à aider à la mise en œuvre des outils de la feuille de route : outil national peut ne pas être synonyme d'outil centralisé au moins sur le plan technique. Toute intégration de la blockchain dans le domaine de la santé nécessite en tout état de cause la prise en compte de ses faiblesses.

A l'analyse, l'usage de la blockchain dans le cadre de la mise en œuvre de projets inscrits dans la feuille de route soulève la question de ses qualités pour contribuer à dématérialiser dans des conditions juridiques et techniques satisfaisantes la donnée de santé à caractère personnel. Cette question doit être regardée à l'aune des règles de protection des données personnelles et également des règles propres aux données de santé déjà inscrites dans le code de la santé publique, dont celles relatives à la force probante des documents dématérialisés comportant des données de santé (1 et 2).

Pour autant, il ne nous semble pas nécessaire de l'encadrer par le recours à une loi. En effet, la blockchain n'est en soi qu'un moyen technique au service d'une fin. Aussi, il ne semble pas qu'il y ait lieu qu'elle fasse l'objet en elle-même d'un texte, au risque qu'il soit rendu obsolète en raison de l'évolutivité rapide de la technologie. Son usage dans le domaine de la santé se trouve en outre d'ores et déjà régulé au travers de grands principes inscrits dans la loi qui encadrent les données de santé. En sus des règles relatives au secret professionnel, est ainsi inscrit dans la loi le principe d'interdiction de cession des données de santé à titre onéreux. Concilier ces principes existants avec la nécessité de trouver un modèle économique compatible avec l'usage de la blockchain constitue un véritable enjeu (3).

Forces et faiblesses de la blockchain au vu du cadre juridique actuel

La blockchain comporte des faiblesses à intégrer « *by design* » dans les systèmes qui la mettraient en œuvre dans le domaine de la santé.

En effet, l'opportunité du recours à cette technologie devrait être examinée en tenant compte, d'une part, des enjeux écologiques, celle-ci étant à certains égards grande consommatrice d'énergie, et d'autre part, des exigences issues de la réglementation relative à la protection des données personnelles.

A cet égard, la Cnil a émis des recommandations relatives à l'usage de la blockchain selon lesquelles le principe commun à certaines de ces solutions est que la donnée en clair est stockée ailleurs que sur la blockchain (comme par exemple sur le système d'information du responsable de traitement) et que seule une information prouvant l'existence de la donnée y est stockée (engagement cryptographique, empreinte issue d'une fonction de hachage[17] à clé, etc.). La blockchain serait utilisée dans un rôle de certificateur.

On rappellera en outre qu'il n'est pas possible de revenir sur la modification apportée dans la blockchain. Il est donc recommandé de penser l'architecture du système en préservant la possibilité de modifier la donnée dans une base ad hoc, afin de respecter le droit des personnes concernées à l'égard de leurs données personnelles, en particulier le droit à l'oubli. A noter qu'une blockchain privée ou permissionnée[18] pourrait permettre de faire transiter les données en clair (sans le mécanisme de l'empreinte). Elle entraînerait cependant plus de risques pour la protection des données. Restent à prendre les mesures de sécurité qui s'imposent pour éviter par exemple le vol de la clé privée et bien entendu d'éviter toute faille dans la construction de la blockchain lors de sa conception.
D'une façon générale, le système qui permet de faire transiter les données en clair devra naturellement être conçu dans le respect des règles de sécurité et de confidentialité des données personnelles de santé. On soulignera que le fait de procéder au hachage des données personnelles de santé est une technique de pseudonymisation, qui ne permet pas de s'exonérer du respect des règles spécifiques aux données de santé, telles que l'hébergement des données de santé, si les conditions de leur application sont réunies par ailleurs.

Si la blockchain venait à avoir des applications dans le domaine de la santé à l'aune de la feuille de route du numérique en santé, il resterait

enfin à lui trouver une place dans le respect des règles contenues dans les référentiels de sécurité et d'interopérabilité mentionnés à l'article L. 1110-4-1 du code de la santé publique pour les motifs évoqués supra. Elle peut toutefois d'ores et déjà apparaître entre les lignes du projet de référentiel force probante.

Dans le domaine de la santé, la question de la fiabilité des documents de santé dématérialisés s'est posée et a été traitée en 2016 dans le cadre de la loi de modernisation de notre système de santé. La réflexion sur la qualité de la blockchain en tant que moyen de preuve doit être élargie aux autres moyens permettant de procéder à la dématérialisation des données de santé pour permettre le « *zéro papier* ».

Compatibilite avec les Principes régissant la force probante des documents de santé dématérialisés

Que ce soit avec l'aide d'un dispositif technique comme la blockchain ou avec d'autres moyens (certificats électroniques, cachets électroniques, etc.), tous les systèmes d'information de santé qui produisent des documents de santé dématérialisés doivent être conçus en intégrant les règles des articles L. 1111-25 à 31 du code de la santé publique, relatifs aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique.

Les données produites par l'ensemble des professionnels à l'occasion de leurs activités de prévention, de diagnostic, de soins, de compensation du handicap, de prévention de perte d'autonomie et de recherche, doivent être conservées pendant une durée longue, fixée par la loi dans certains cas, pour répondre à la nécessité d'assurer dans le temps la continuité et la qualité de la prise en charge des patients. Elles constituent en outre des éléments de preuve décisifs dans le cadre de contentieux de responsabilité médicale.

Tout en recourant aux outils technologiques permettant la dématérialisation des données de santé, les établissements et professionnels de santé conservent concomitamment les documents sur support papier jusqu'à l'expiration des délais réglementaires de conservation (notamment celui des dossiers patients prévu à l'article R1112-7 du code de la santé publique), afin de ne pas encourir de risques de mise en cause de leur responsabilité.

Les articles L1111-25 à 31 du code de la santé ont donc eu pour objectif de fixer et uniformiser les règles applicables à l'ensemble des acteurs produisant des données de santé, afin de fixer les conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique.

Il a été fait le choix de ne pas créer de règles spécifiques pour ces documents et d'appliquer expressément les seules dispositions du code civil relatives, d'une part, à la copie numérique et, d'autre part, à l'écrit électronique et la signature électronique. En effet, il ressortait de l'analyse de la jurisprudence administrative et des visas des textes régissant le secteur de la santé que les dispositions du code civil en la matière servaient régulièrement de référence au juge administratif. C'est le cas dans d'autres secteurs que le secteur de la santé, qui, bien que relevant du droit administratif, font application du code civil - par exemple, dans le cadre de la dématérialisation des marchés publics.

Ce choix a été conforté par le fait que les dispositions du code civil ont été complétées par des textes d'application conformes au règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur dit règlement « *eIADS* », qui ne prévoit pas de règles spécifiques ou dérogatoires pour le secteur de la santé.

L'article L. 1111-25 précité précise désormais que les règles s'appliquent à « *tous les documents comportant des données de santé à caractère personnel, produits, reçus ou conservés par un professionnel de santé, ou par tout professionnel ou organisme concourant à la prévention ou aux soins, ou par un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social pour l'exercice de leurs activités de prévention, de diagnostic, de soins, de compensation du handicap, de prévention de perte d'autonomie, ou de suivi social et médico-social* ».

Enfin, un référentiel reste à intervenir pour préciser les conditions de mise en œuvre de ces articles. Ce référentiel dit force probante pris en application de l'article L1111-31 du code de la santé publique a été mis à la concertation sur le site internet de l'ANS[19]. Il doit préciser les règles à respecter afin d'aider les responsables de traitement à identifier le degré de confiance pouvant être accordé au document dématérialisé comportant des données de santé.

Le projet de référentiel force probante indique que ses annexes identifient des paliers de mise en œuvre (ex : signature électronique simple, avancée, qualifiée), présentant des caractéristiques de sécurité plus ou moins avancées, mais induisant un niveau de complexité progressif de mise en œuvre et de déploiement.

Il appartient au responsable du système d'information de s'appuyer sur la classification des documents de santé [document de référence n°6] afin d'identifier le palier de mise en œuvre minimum adapté à chaque document. Il résulte de ce système de palier que la destruction des documents originaux ne sera pas possible dans tous les cas. Tout dépendra de la robustesse du dispositif de dématérialisation mis en place et des résultats de l'analyse de risques qu'il appartient au responsable du système d'information de réaliser. Ce dernier peut en outre mettre en œuvre des mesures

de sécurité complémentaires afin d'ajuster au mieux la sécurité de son système d'information en fonction du contexte et des enjeux propres aux documents concernés.

Le référentiel prévoit également le cas dans lequel il serait fait le choix par le responsable du système d'information de n'appliquer aucune des recommandations du référentiel (ce qui laisse interrogatif sur la valeur prescriptive de ce référentiel devant pourtant être approuvé par arrêté du ministre chargé de la Santé).

Quel que soit le palier retenu par le responsable de traitement, dès lors que les moyens mis en œuvre ne sont pas présumés fiables, il est préconisé de recourir à une convention de preuve.

Dans ce contexte, le juge pourra être amené à statuer sur la validité de la convention de preuve. Il n'est jamais lié par elle. La question va probablement se poser dans le cadre des services nationaux à destination des usagers mentionnés dans le cadre de la feuille de route du numérique en santé de l'introduction de l'usager dans celle-ci. En vertu de l'effet relatif des contrats, la convention de preuve ne peut pas être opposée à l'usager, elle ne vaut qu'entre les parties qui la concluent. Comment en étendre les effets à l'usager sans risquer d'être dans une situation asymétrique ? En effet, la convention de preuve ne doit pas créer d'asymétrie trop forte entre les parties, le juge pouvant considérer que les clauses sont alors abusives. La mise à disposition de la documentation technique imposée par l'article L.1111-31 du code de la santé publique peut contribuer à éviter ce risque, en permettant à chaque partie de prendre connaissance des modalités de fonctionnement du processus de dématérialisation.

Cependant, on en revient au sujet de l'identité numérique du citoyen, usager du système de santé, et devant maîtriser l'usage et le devenir de ses données au travers de systèmes dans lesquels il doit avoir suffisamment confiance.

Compatibilité avec le Principe d'Interdiction de céder les données de santé à titre onéreux

D'aucuns mettent en avant qu'un effet néfaste de la blockchain, en tant que dispositif décentralisé qui ne s'appuie plus sur un tiers de confiance, pourrait engendrer un risque de patrimonialisation des données de santé. Ce risque ne nous semble pas accru par ce dispositif mais il existe. En matière de données de santé à caractère personnel, la personne dispose déjà d'un droit d'accès à son dossier patient organisé par le code de la santé publique. Des outils nationaux sont ou seront à sa disposition pour renforcer l'effectivité de ce droit (en particulier au travers du DMP et de l'ENS).

Le renforcement des droits de la personne concernée sur ses données amène à soulever la question de la monétisation des données de santé en permettant de les rendre accessibles contre rémunération. La mise en œuvre de ces droits est effectivement facilitée par la technologie dont celle de la blockchain.

Il résulte que si les pouvoirs publics faisaient le choix de (re)donner à la personne concernée cette maîtrise sur ses données personnelles non plus seulement au travers de la reconnaissance de nouveaux droits sur ces dernières (droit à la portabilité, droit à l'effacement, etc.), mais en recourant à la blockchain, il faudrait prendre en compte dès la conception du dispositif la question du modèle économique.

La volonté du législateur français a été incontestablement d'éviter toute marchandisation des données de santé, qui sont une émanation du corps humain pour lequel l'indisponibilité est un principe essentiel du droit français en inscrivant un principe d'interdiction des données de santé à titre onéreux à l'article L. 1111-8 alinéa 4 du code de la santé publique : « *VII.-Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal.* » Au titre des règles communes d'exercice des professions médicales, on rappellera que la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'article L. 161-29 du code de la sécurité sociale sont interdites, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur. (Article L4113-7 du code de la santé publique).

Le recours à la blockchain doit donc se faire en tenant compte de ces principes. En outre, elle pourrait elle-même en faciliter le respect en étant conçue avec des restrictions adaptées.

La blockchain publique présente une architecture décentralisée, ouverte, chacun pouvant y accéder, y effectuer des transactions ou prendre part au consensus. Des variantes sont cependant possibles. Ainsi, par exemple, la blockchain publique peut faire appel à une architecture ouverte tout en introduisant :

- un « *validateur* » de transactions, pour contrôler les nœuds du réseau autorisés à valider les transactions ;
- ou un contrôle sur l'identité des intervenants pouvant être partie à une transaction.

Cette technologie de la blockchain pourrait être couplée avec le système classique de l'IGC présentée supra. En effet, le système de l'IGC pourrait porter les solutions d'identification, faisant ainsi le lien entre l'identité et le pseudonyme sur la blockchain. La blockchain serait alors en charge de tracer les accès aux données.

La maîtrise par l'individu de ses données personnelles via la blockchain semble ainsi pouvoir être encadrée par des moyens techniques. Une contrepartie financière ne peut être envisagée que dans un cadre éthique et juridique rénové.

CONCLUSION

Il semble que la blockchain ne se trouve pas bloquée aux frontières du secteur de la santé. Elle connaît d'ores et déjà quelques déclinaisons et pourrait faire l'objet de nouveaux cas d'usage sans nécessité d'une régulation normative dédiée, sous réserve d'être mise en œuvre « *by design* » dans le respect des principes fondamentaux relatifs à la protection des données personnelles et des règles particulières relatives aux données de santé et en tenant compte du modèle économique.

Comme pour tout autre moyen technique mis en œuvre pour numériser le domaine de la santé, il relève de la responsabilité des professionnels et des responsables des structures dans lesquelles ils exercent de prendre des mesures adaptées pour sécuriser leur usage, tant en amont, qu'en aval de leur mise en œuvre. La sécurité juridique est essentielle et doit également être prise en compte « *by design* ».

Il est en effet indispensable de prendre en compte l'ensemble du cadre juridique applicable aux documents de santé comportant des données à caractère personnel pour le cas d'usage métier concerné.

L'analyse juridique permettra également de sécuriser le projet en procédant à la formalisation dans des procédures et des contrats de la répartition des rôles de tous les acteurs intervenant dans la chaîne, dont les industriels. Ces derniers doivent s'engager à respecter les conditions de sécurité associées.

Il est également recommandé d'utiliser des dispositifs et des services déjà disponibles et labellisés. Dans le contexte du règlement européen « *eIDAS* » n° 910/2014 qui ne semble pas devoir évoluer pour intégrer la blockchain, l'Anssi pour la France, et les organes de contrôle européens équivalents, labellisent des services et outils capables de produire, signer et horodater des documents électroniques.

En droit interne, il est annoncé par la Direction du numérique en santé et l'Agence du numérique en santé de nouvelles versions des référentiels de sécurité et d'interopérabilité du secteur de la santé, mentionnés à l'article L. 1110-4-1 du code de la santé publique, et la mise à disposition de nouveaux outils tels que Pro Santé Connect[20].

Il sera intéressant d'apprécier dans quelle mesure la technologie de la blockchain trouvera, le cas échéant, une place dans l'environnement technologique et normatif du numérique en santé en pleine mutation. La dimension patrimoniale est enfin un sujet qui paraît devoir faire l'objet d'un débat éthique et juridique pour avancer sur ce sujet de société.

Florence EON-JAGUIN
Avocat
Cabinet Withlaw

Notes

(1) https://www.capital.fr/economie-politique/bruno-le-maire-le-developpement-de-lecosysteme-blockchain-est-une-priorite-pour-le-gouvernement-1335182

(2) Loi° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, n° 2619 (PACTE : Plan d'action pour la croissance et la transformation des entreprises)

(3) Pour rappel, le jeton (token dans le monde blockchain) désigne un actif numérique possédant une double propriété :Il est transmissible par un dispositif d'enregistrement électronique partagé (en d'autres termes, la Blockchain telle que définie par le législateur français). Il attribue à son détenteur des droits sur un bien ou un service détenu par l'émetteur du jeton

(4) Informations extraites de l'article Blockchain : où sont passés les 340 millions de l'Union européenne ? du 17/01/2020 publié sur le site internet du Journal du net https://www.journaldunet.com/economie/finance/1488084-blockchain-ou-sont-passes-les-340-millions-de-l-union-europeenne/

(5) Le groupe de travail présidé par Joëlle Toledano sous l'égide de France Stratégie a rendu un rapport sur les enjeux de la blockchain en juin 2018.

(6) https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf

(7) Décret n° 2019-1412 du 20 décembre 2019 portant diverses dispositions relatives à l'administration centrale des ministères chargés des affaires sociales qui institue, « auprès des ministres chargés de la santé, de l'action sociale et de la sécurité sociale, un délégué ministériel au numérique en santé. Il est nommé par décret, sur proposition de ces ministres. »

(8) Ex-ASIP Santé (Agence des Systèmes d'Information Partagés de Santé)

(9) Loi n° 2019-774 du 24 juillet 2019, relative à l'organisation et à la transformation du système de santé

(10) Extrait de l'article L1111-13-1 « I.-L'espace numérique de santé est ouvert automatiquement, sauf opposition de la personne ou de son représentant légal. La personne ou son représentant légal est informé de l'ouverture de l'espace numérique de santé, des conditions de fonctionnement de cet espace, de ses responsabilités en tant que gestionnaire de données de santé dans un espace numérique et des modalités de sa clôture en application du 3° du IV. La personne concernée ou son représentant légal est également informé des modalités d'exercice de son droit d'opposition préalablement à l'ouverture de l'espace numérique de santé. »

(11) https://esante.gouv.fr/sites/default/files/media_entity/documents/Dossier_virage_numerique_masante2022.pdf

(12) Articles L1111-14 à L. 1111-24 / Art. R. 1111-26 et suivants du code de la santé publique

(13) https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi_referentiel_authentification_v.2.0.pdf

(14) L'intégration dans le monopole de l'imprimerie nationale de la production des cartes de professionnels de santé (CPS) et des autres produits de certification diffusés par l'agence des systèmes d'information partagés (ASIP) santé (carte de personnel employé, carte de personnel autorisé, certificats logiciels, certificats serveurs) a pour base réglementaire le décret n° 2012-1117 du 2 octobre 2012.

(15) L'identité numérique : un usage de la blockchain au profit du citoyen, 24 septembre 2018

(16) La direction interministérielle du numérique (DINUM), créée par le décret du 25 octobre 2019, a pris la suite de la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC).

(17) Un hash est un nombre souvent hexadécimal calculé à partir d'une donnée. Il représente en quelque sorte une empreinte digitale servant à identifier la donnée initiale. Il existe plusieurs fonctions de hachage. Pour deux chaînes de données identiques, le même hash sera calculé alors que pour deux chaînes de données différentes il y aura deux hashs différents ; cela permet de vérifier si la donnée initiale n'a pas été modifiée.

(18) En pratique, plusieurs sortes de blockchain coexistent, mettant en œuvre des niveaux de permission différents pour les différentes catégories de participants. La Cnil utilise la classification suivante :
- les blockchains publiques sont accessibles à n'importe qui dans le monde. Toute personne peut effectuer une transaction, participer au processus de validation des blocs ou obtenir une copie de la blockchain ;
- les blockchains à permission ont des règles définissant quelles personnes peuvent participer au processus d'approbation ou même effectuer des transactions. Elles peuvent, selon les cas, être accessibles à tous ou être en accès limité ;
- les blockchains dites « privées » sont sous le contrôle d'un acteur qui assure seul le contrôle de la participation et de la validation. Selon certains experts, ces usages ne respectent pas les propriétés classiques de la blockchain, notamment la décentralisation et la validation distribuée. En tout état de cause, elles ne posent pas de question particulière de conformité au RGPD, il s'agit de simples bases de données distribuées « classiques ».

(19) Article L1111-31 : Les conditions d'application de la présente section [4 : Conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique], notamment pour déterminer le procédé de signature adapté à la nature du document, sont précisées par les référentiels définis à l'article L. 1110-4-1.

(20) Doctrine technique du numérique en santé, Janvier 2020