Blockchain et santé: cas d'application et premiers questionnements juridiques.

Isabelle Poirot-Mazères

Séminaire IFERISS-IMH : Blockchain et Santé : Perspectives d'applications et enjeux juridiques Intervention du 12 Octobre 2018

Blockchain et Santé : Cas d'application et premiers questionnements juridiques

Isabelle Poirot-Mazères,
Professeur de droit public

Institut Maurice Hauriou | Université Toulouse 1 Capitole | IFERISS

A l'origine corrélée aux crypto-monnaies, la blockchain en déborde désormais le cadre. Elle apparaît en particulier comme l'une des technologies les plus susceptibles d'accompagner les mutations du système de santé en apportant plus de fluidité, de sécurité et de flexibilité dans la gestion et le partage des données de santé. De quoi s'agit-il ? Selon la définition retenue par *Blockchain France*, elle est une « technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ». Par extension, c'est une base de données transparente, immuable, sécurisée et distribuée: au lieu d'être conservée par une institution dédiée, elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Elle est considérée à cet égard comme profondément disruptive en ce qu'elle induit un transfert de confiance des utilisateurs. On passe d'un modèle de confiance placé en des entreprises, des institutions publiques ou des fonctions réglementées (tiers de confiance) à un modèle où la confiance est mise dans un protocole (« *code is law* ») et dans une communauté décentralisée qui adhère à celui-ci.

Quel intérêt peut présenter une telle technologie dans le domaine de la santé et quel plus apporte-t-elle à un système déjà fortement encadré et protégé ? Si les spécialistes s'accordent à reconnaître qu'elle est de nature à en modifier les transferts d'informations et de données dans un avenir proche, les applications sont pour l'instant embryonnaires et l'on peine non seulement à mesurer l'ampleur effective des transformations qu'elle porte mais aussi à imaginer comment elle pourra s'inscrire dans des processus organisationnels de grande ampleur comme ceux du système de santé. L'ambition est donc pour l'instant modeste et les approches ponctuelles. Il apparaît ainsi que la technologie blockchain n'est pas destinée à se substituer en santé aux systèmes d'information ou de partage de données existants mais à les conforter ou à pallier leurs insuffisances.

En effet, par ses caractéristiques, elle répond à certains défis posés par l'utilisation des données en santé. La santé est d'abord un domaine où les acteurs sont nombreux, qui ne se font pas forcément confiance et dont les intérêts sont souvent divergents (patients, professionnels, compagnies d'assurances, fournisseurs de service, industriels…), et auxquels elle va permettre d'échanger de la « valeur » dans un cadre transparent et sécurisé. A cet égard, nous y reviendrons, elle peut être structurée pour restituer au patient la maîtrise de ses données de santé, lui permettre de participer au processus de leur valorisation et en décider la rétribution, ce qui n'est pas le cas aujourd'hui. Par ailleurs, le secteur est à la fois un producteur massif et un utilisateur dépendant des données de santé, et leur collecte, leur traitement, leur partage y revêtent une importance cruciale. Or cette importance de la donnée et de ses usages possibles suscitent des menaces diverses (avec des exigences corollaires en termes de sécurité et de confidentialité), de revendications croissantes (maîtrise des données personnelles par les patients, demandes des chercheurs ou des industriels) et de critiques récurrentes, notamment relatives aux problèmes d'interopérabilité (données cloisonnées dans différents systèmes indépendants les uns des autres, gestion « en silos », données encore peu standardisées). Enfin, les contraintes sont partout les mêmes dans le système de santé, exprimées similairement par les différents acteurs : nécessité de prouver ou garantir des identités (celles des patients, des professionnels, des tiers de confiance), de contrôler les accès aux dossiers médicaux ou le déroulement des protocoles de recherche, de permettre les transferts sécurisés des informations, d'encadrer les procédures de remboursement ou d'octroi de prestations sociales… La blockchain, est-il souligné, « au travers de sa conception, de ses principes de fonctionnement et des avantages qu'elle offre sur les transactions de données (partage transparent de toutes les transactions, sécurité, confidentialité grâce à la cryptographie, traçabilité avec le chaînage historisé et irrépudiable des blocs de transactions, absence de recours à une autorité centrale…) »[1], permet de répondre à des contraintes.

D'ores et déjà, au regard des projets en cours, quelques domaines sont privilégiés[2] : d'abord dans la *supply chain* pharmaceutique, la blockchain, grâce à sa transparence et son inaltérabilité, peut améliorer la traçabilité et les vérifications d'authenticité des médicaments, des ordonnances médicales voire des brevets ; dans la recherche, elle peut être un outil pour renforcer la transparence des essais et la collaboration entre chercheurs ; et surtout, comme registre patient distribué, elle est désormais envisagée, grâce à l'IA, comme la technologie susceptible tout à la fois de potentialiser l'exploitation des données de santé et de redonner la main au patient : à cet égard, certains projets

[1] Jean-Yves DUGARDIN, « Blockchain : Une technologie disruptive pour le secteur de la Santé ? », 4 mai 2018, www.orange-business.com/fr/blogs/blockchain-technologie-disruptive-pour-secteur-sante-partie-1
[2] Voir par exemple, BLOCKCHAIN PARTNER, Etudes « Panorama juridique des enjeux juridiques de la blockchain » et « Blockchain et Santé », mars 2016.

s'attachent au recueil des données en vie réelle via les dossiers patient numériques et les objets connectés (projet Embleema) en vue d'améliorer la pharmacovigilance et d'accélérer les mises sur le marché ; d'autres visent de façon plus générale, à une mise en commun de bases de données issus de divers acteurs et à une rationalisation de leur utilisation, garantissant partage et intégrité des données à l'image du projet Substra (plateforme *open source*, sécurisée et éthique qui permet aux fournisseurs de données, comme les hôpitaux ou les centres de recherche, de valoriser leurs informations et de les utiliser à des fins de recherches médicales, avec pour objectif notamment de cibler les thérapies de manière personnalisée, dans un cadre protecteur de la confidentialité des données).

-Vers un nouveau modèle d'exploitation des données ? Une remarque préalable s'impose pour comprendre ce qui devraient constituer les linéaments des dispositifs blockchains en santé. Trois modèles de blockchains sont possibles en fonction de l'accès permis à la chaîne et la participation aux blocs : le premier type, le plus connu et commenté est celui des blockchains publiques, accessibles à tous, chacun pouvant effectuer une transaction, participer à la validation des blocs ou obtenir une copie de la blockchain. Les deux autres catégories sont dites « de permission » ou « permissionnées » : d'une part, les blockchains « de consensus » ou « de consortium » qui délimitent les personnes pouvant participer au processus d'approbation ou effectuer des transactions et pour lesquelles sont précisées d'emblée par les participants les règles de validation des transactions ; et d'autre part, les blockchains « privées » placées sous le contrôle d'un acteur qui assure seul le contrôle de la participation et de la validation. Cette dernière modalité n'a plus grand-chose de l'ADN de la blockchain, à savoir la décentralisation et la validation distribuée. Ce modèle entre sans difficulté dans les cadres juridiques préétablis d'un dispositif contrôlé par un intervenant et, comme le relève la CNIL, « il s'agit de simples bases de données distribuées 'classiques' ».

A l'analyse et au vu des projets en cours, il semble bien que le modèle qui devrait être celui du secteur de la santé, soit plutôt celui des blockchains de consortium entre acteurs choisis décidant de partager, au-delà de leurs intérêts divergents, des données et informations dans un cadre à la fois sécurisé, transparent et pérenne. Concrètement ici, s'agissant d'exploiter les données des patients, le modèle qui se dessine est celui dans lequel les composantes des dossiers ne sont pas toutes incluses directement dans la blockchain qui ne recueille que les transactions opérées sur celles-ci, *via* un code complexe (hash) faisant référence à une version précise du document original (stockage *off-chain*). Les données initiales, notamment les éléments trop lourds comme les images, sont ici appelées à rester dans les bases de données traditionnelles ou dans des systèmes de *cloud* comme elles le sont actuellement soit localement à l'hôpital ou auprès des hébergeurs agréés de données de santé (cf. les projets Embleema et Substra). Il n'est donc possible d'accéder à la donnée que par l'usage d'une clé

privée via le patient concerné. En parallèle, le patient, acteur et participant, définit, grâce aux *smart contracts* -qui permettent l'exécution automatique des termes du contrat établi préalablement avec les autres participants de la blockchain - les personnes autorisées à accéder à ses informations (médecins, chercheurs, famille…), ce qui lui permet de se réapproprier ses données et d'en gérer l'accès, mais sans pouvoir les modifier ou les supprimer. L'un des avantages les plus couramment soulignés de la blockchain est ainsi de redonner au patient la maîtrise de ses données personnelles, de lui permettre de participer à leur valorisation via les partages et transferts de données, par exemple entre collecteurs de données et chercheurs ou laboratoires. L'essentiel, que conforte le RGPD, est de garantir le contrôle de l'individu sur ses données personnelles, pour contribuer à la recherche d'abord, mais aussi lorsqu'elles font l'objet d'une exploitation commerciale. Les projets émergent aux Etats-Unis, qui offrent des contreparties (en particulier sous forme de crypto monnaies) aux patients qui autorisent l'accès à leurs données.

Alors s'agit-il véritablement d'une révolution comme d'aucuns le soutiennent ? On peut l'imaginer voire l'anticiper sur le plan opérationnel ; en revanche, le caractère complètement inédit de la blockchain doit être nuancé en droit.

Des questionnements juridiques. Si la technologie blockchain reste encore entourée d'un certain flou, faute de cadre général et en attente de contentieux, elle est loin de baigner dans le vide juridique. S'appliquent en effet non seulement un embryon de règles dédiées[3] mais aussi les principes et règles de droit commun, qu'il s'agisse du droit civil des obligations (règles gouvernant le consentement, les contrats, les régimes de responsabilité, ou le régimes des droits de la personne ou des biens), du droit du numérique comme les règles concernant la signature électronique ou relatives à la protection des données personnelles (Règlement général sur la protection des données n° 2016/679, et loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles), ou des règles du droit de la santé (droits des patients, encadrement des recherches, droit de la génétique…). Restent évidemment bien des questionnements appelant précisions. Plusieurs points retiennent l'attention en lien avec la décentralisation, l'anonymat et l'immutabilité des contenus de la blockchain[4]. Nous n'envisagerons ici que le cas des blockchains « permissionnées », qui sont susceptibles de se développer en santé.

[3] Singulièrement dans le secteur financier: ordonnance 2016-520 du 28 avril 2016 relative aux bons de caisse; ordonnance 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers; loi PACTE, art.26. Sur la définition, cf « Vocabulaire de l'informatique (listes de termes, expressions et définitions adoptés) » : « mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification », JORF, 23 mai 2017.

[4] CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », 24 septembre 2018 ; « Blockchain : une révolution juridique ? », Revue Lamy, n°129, septembre 2017, p.34 et s. ; Mathieu

Immutabilité. Les informations véhiculées par l'intermédiaire de cette technologie sont fiables mais aussi infalsifiables et immuables, autant de qualités qui doivent être rendues compatibles avec les exigences du RGPD relatives au droit à la rectification et le droit à l'oubli. Quelques réponses sont d'ores et déjà avancées. S'agissant de la rectification, dans le contexte d'une blockchain dans laquelle les données ne sont pas stockées directement et auxquelles on ne peut accéder que par l'intermédiaire de la personne propriétaire *via* sa clé privée, celle-ci pourra toujours réaliser ou autoriser cette modification. De façon générale, la gouvernance de la blockchain devra prévoir une telle faculté de rectification sur le plan opérationnel. Pour le droit à l'oubli, est proposée la solution technique de la « neutralisation » des informations en cause qui, faute d'être effacées, seraient rendues inaccessibles[5].

Autre question, la sécurité de la technique. Tous les éléments de sécurité des traitements évoqués dans l'article 32 sont par nature respectés par l'implémentation de la blockchain permissionnée. Toutefois, conçue pour être à l'abri de toute corruption et garantir l'inviolabilité des transactions qu'elle gère, elle ne garantit pas pour autant l'infaillibilité de son contexte : la question de la sécurité est renvoyée « à la périphérie et aux interfaces de la blockchain ». Si les données qui y entrent sont falsifiées, corrompues ou de mauvaise qualité, « les transactions qu'elle gèrera le seront tout autant »[6]. Par ailleurs, le dispositif fonctionne à partir d'un jeu clé publique/clé privée mais un doute persiste sur la sécurité à reconnaître à des clés privées de signature sans autorité de certification identifiée (notamment au titre du Règlement européen eIDAS pour l'identification et la signature électronique). Enfin, on ne peut jamais exclure l'éventualité d'une cyberattaque d'un bloc de la chaîne susceptible de contaminer les suivants. A cet égard, la CNIL préconise, au sujet des blockchains permissionnées, de s'assurer d'au moins 51% des mineurs (quels qu'ils soient) afin d'empêcher toute coalition de nature à détenir la majorité des pouvoirs.

Décentralisation. Registre partagé où toute décision est prise par consensus entre les participants, sans arbitre centralisé, la blockchain garde ses zones grises auxquelles le droit peut répondre. Sur les responsabilités juridiques en cas de dommages d'abord, qui devraient obéir aux règles de droit commun, dès lors qu'en seront identifiés les acteurs. Sur ce point, qui renvoie à la détermination du responsable de traitement, l'un des aspects de la blockchain les plus débattus, les lignes s'éclaircissent, tout au moins pour les blockchains privées ou de consortium, comme il s'en dessine

---

PESIN et Aurélie BAYLE, « Blockchain et RGPD », https://www.linkedin.com/pulse/blockchain-rgpd-mathieu-pesin/?originalSubdomain=fr.

[5] La CNIL relève que certaines techniques devraient permettre en ce sens de respecter les exigences du RGPD en coupant « l'accessibilité de la donnée en fonction du format choisi (engagement cryptographique, chiffrement, empreinte issue d'une fonction de hachage à clé…) ».

[6] Jean-Yves DUGARDIN, « Blockchain : Une technologie disruptive pour le secteur de la Santé ? – Partie 2 », https://www.orange-business.com/fr/blogs/blockchain-technologie-disruptive-pour-secteur-sante-partie-2

en santé. La détermination du responsable de traitement exigé par le RGPD devrait être relativement aisée dès lors que la gouvernance et les rôles respectifs de chaque participant identifié seront fixés par avance.

Ensuite, le transfert hors Union européenne des données personnelles, inhérent à la technologie, doit faire l'objet d'un éclairage des autorités compétentes, en particulier de la CNIL, et ponctuellement, d'un alignement sur les textes européens lors de la mise en œuvre d'une blockchain. Singulièrement, relèvent certains spécialistes, « dans le cadre de projets permissionnés, la localisation des traitements peut être maîtrisée dans la mesure où la structure du réseau blockchain peut, si besoin, être adaptée pour répondre aux exigences liées aux traitements transfrontaliers (création de *side-chains*, de *channels*, etc…) »[7].

D'autres questions émergent qui devront être clarifiées au gré des contentieux : celle de la valeur des *smarts contracts* (au regard des exigences du Code civil) : le *smart contract* n'est en effet qu'un logiciel dont l'usage doit s'inscrire dans un contrat préalable, avec autorité juridique, respectant les conditions classiques, notamment consentement et capacité des parties ou contenu licite et certain. Des incertitudes demeurent que les parties devront d'emblée régler ou le juge résoudre ex post, comme la confrontation des *smarts contracts* à la règle de l'article 1210 du Code civil selon laquelle « les engagements perpétuels sont prohibés ».

Enfin, certains débats sont réactivés par l'institution des blockchains au premier rang desquels ceux concernant le statut juridique et la libre disposition des données personnelles, dès lors que la technologie porte en elle, intrinsèquement, la valorisation des transactions comme du partage de celle-ci entre les patients et les utilisateurs, et pose la question, cruciale, de la contrepartie des opérations de minage.

Il importe d'ores et déjà de s'interroger sur la blockchain en santé, mais sans emballement ni réticence. Nous n'en sommes qu'aux prémices, à tous niveaux. Au vu des retards dans la standardisation des données de santé et des difficultés d'interopérabilité des SI, il faudra au secteur de la santé encore quelques années pour réunir les conditions d'une généralisation de cette technologie. Mais des applications comment à être expérimentées. D'où l'importance, ici comme ailleurs, d'avancer, de comprendre ce qu'il en est, de cerner ou d'adapter les règles juridiques protectrices des patients et ce, tout en marchant…

[7] Mathieu PESIN et Aurélie BAYLE, « Blockchain et RGPD », préc.