Thèse 10 : Blockchains (des dossiers transparents, redondants et sécurisés)

Si les *blockchains* ont fait les gros titres des médias, peu de gens savent comment cela marche vraiment ou quels en seront les usages probables dans la société de demain.

Nous proposons dans ce chapitre de revenir aux sources de la blockchain pour en comprendre les fonctionnalités et de décrire des applications vraisemblables voire "probables" qu'il est possible d'en tirer pour le domaine de la santé.

Les blockchains sont des technologies informatiques qui organisent la confiance en matière d'enregistrements, de transmissions et de stockages de transactions (et par extension de contrats et de dossiers). Elles ont pour caractéristiques d'être transparentes, sécurisées et d'être distribuées (c'est-à-dire de fonctionner sans organe central de contrôle, sans tiers de confiance.

Une blockchain est une base de données qui contient l'historique horodaté de tous les enregistrements qui retracent les échanges (des transactions au sens large) effectués entre ses différents utilisateurs (les parties prenantes). Cette base de données est certifiée par des nœuds de stockage distribués.

Il existe des blockchains publiques ouvertes à tous et des blockchains privées, dont l'accès et l'utilisation sont limités à des "parties prenantes" habilitées.

Une blockchain publique peut donc être assimilée à un grand registre public, anonyme et infalsifiable, une sorte de très grand livre que tout le

monde peut lire librement et gratuitement et sur lequel seuls quelques-uns peuvent écrire mais que personne ne peut effacer, falsifier ou détruire.

Une blockchain privée fonctionne de la même manière mais avec un accès réservé aux seules personnes ou institutions autorisées.

Pourquoi les blockchains ?

Les premières blockchains datent de 2008. Elles ont été développées à l'origine pour la monnaie numérique : le bitcoin. D'abord présentées par Satoshi Nakamoto (pseudonyme du ou des développeurs du bitcoin), la blockchain désigne en fait l'architecture de fonctionnement informatique sous-jacente.

Si blockchain et bitcoin ont été élaborés simultanément, aujourd'hui on dénombre de multiples initiatives qui promeuvent, toujours sous les mêmes principes, des applications dans des domaines divers comme le *trading* des grains et céréales, la gestion des droits d'auteur ou le vote électronique. On est bien loin du champ initial de la monnaie numérique et c'est là une indication du potentiel de déploiement des blockchains.

La blockchain apparaît clairement comme un formidable cheval de Troie de la désintermédiation. En se substituant aux " tiers de confiance " elle remet profondément en cause des professions dont c'est, au moins partiellement, la raison d'être : avocats, notaires, agents immobiliers, établissements financiers, mais aussi des plateformes de transport (tel Uber) ou d'hébergement (tel Airbnb), et bien d'autres encore.

On peut donc facilement comprendre qu'à l'avenir, bon nombre d'entreprises et d'administrations publiques utiliseront la technologie des

blockchains pour de nombreuses situations des contrats à ventes multiples aux registres d'État).

Comment cela marche-t-il ?

Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les nœuds du réseau appelés les "mineurs" selon des techniques qui dépendent du type de blockchain. Initialement, dans la blockchain du bitcoin, cette technique est appelée le "Proof of Work" (preuve de travail) et consiste en la résolution de processus algorithmiques. Une fois le bloc validé, il est daté et ajouté à la chaîne des autres blocs. La transaction est alors visible pour les deux partenaires mais aussi pour l'ensemble du réseau des parties prenantes autorisées.

Ce processus prend un certain temps selon la typologie blockchain utilisée (plusieurs minutes pour le Bitcoin à quelques secondes pour l'Ether qui utilise la technique du "Proof of Stake", la preuve de participation).

Quel futur pour les blockchains ?

Le caractère décentralisé de la blockchain, sa sécurité (cryptographie) et sa transparence (accessible à tous) promettent donc des applications à des domaines très variés.

On peut classer l'utilisation de la blockchain en cinq catégories :

• Les applications pour le transfert d'actifs (domaine financier principalement mais aussi : titres de propriété, contrats sur les matières premières, etc.)

• Les applications de la blockchain en tant que registre : elle assure ainsi une meilleure traçabilité des produits et des actifs (registre d'état civil, registre foncier, actes notariés, etc.).

• Les procédures de vote ou de sondage (votation, élection, référendum, etc.)

• Les contrats "intelligents" : il s'agit de programmes autonomes qui exécutent automatiquement une fois démarrés les conditions et les termes d'un contrat sans nécessiter d'intervention humaine (électricité et smart grid, etc.).

• Les projets à interventions multiples (suivi de grands chantiers, et bien sûr, le suivi médical entre protocole médical et dossier patient, on y reviendra).

Si l'on y réfléchit, les champs d'application sont impressionnants: finance, assurance, santé, énergie, transport, urbanisme, etc. De façon générale, les blockchains avec leurs systèmes informatiques distribués pourraient se substituer à la plupart des contrats centralisés impliquant "un tiers de confiance".

Bien évidemment, toutes les promesses de développement à venir ne sont pas exemptes de défis et de limites que ce soit économiques, juridiques, écologiques ou encore de gouvernance.

BLOCKCHAIN et DOSSIER MÉDICAL

La technologie des blockchains convient bien à tout système de partage de données restreint aux parties prenantes d'un processus. Le diagnostic, le traitement et le suivi médical de patients regroupés ou non dans le dossier médical pourraient tout à fait être pratiqués au moyen

d'une blockchain. Dans certains hôpitaux américains comme la Mayo Clinic, le Massachusetts General Hospital ou à Cleveland, cela est déjà expérimenté.

Analysons maintenant quelques enjeux d'une telle technologie.

1.- Chaîne de la valeur des actes médicaux

Les actes médicaux sont liés les uns aux autres dans la vie d'un patient, mais ils ne le sont pas forcément de manière formelle. Si les vaccinations sont répertoriées dans un carnet, ce dernier n'est pas toujours informatisé. La forme blockchain serait très adaptée à ce type d'usage. Car, ne l'oublions pas, l'enchaînement en "block" apporte sécurité et transparence aux différentes parties prenantes tout en évitant les doublons et les oublis. Ainsi la chaîne de la valeur des actes médicaux pourrait être à l'avenir renforcée par l'usage d'une telle technique en termes de productivité (par exemple plus de doublons dans les analyses et les examens) mais aussi en termes d'accidents avec un meilleur contrôle sur tous les actes médicaux entrepris ou à entreprendre.

2.- Les données enregistrées par les "medical devices"

Pour certaines situations il est même possible d'envisager une automatisation du processus blockchain, par exemple dans le cas des "medical devices" embarqués sur le corps humain comme les pacemakers ou autres dispositifs (pompe à insuline par exemple). Ces dispositifs électroniques devraient pouvoir être liés à un software de type blockchain pour augmenter la sécurité et la traçabilité mais aussi pour diminuer les erreurs et les oublis. Un enregistrement systématique, automatique et fiable renforcerait la pratique médicale.

3.- Protocole de confiance et chaîne de la connaissance

Le premier avantage de la blockchain est le rapport de confiance qu'elle produit. Sa structure codée empêche toute manipulation fausse ou malveillante mais elle oblige aussi les intervenants (parties prenantes du protocole) à davantage de précision en adoptant un peu de retenue dans leurs commentaires et leurs appréciations. Un langage, voire une rhétorique propre aux blockchains, pourrait ainsi apparaître et déboucher sur de nouvelles formes de connaissance, celle du récit des processus de traitement par exemple.

4.- Mise en œuvre d'une blockchain

La mise en œuvre d'une blockchain peut se faire pour le dossier médical ou indépendamment de celui-ci. En effet, des éléments du dossier médical comme les processus de diagnostic, d'opération ou de traitement se prêteraient parfaitement à la création de blockchain indépendante et spécifique car dans un dossier médical certains éléments n'ont pas une utilité significative pour être enchaînés. Les blockchains devraient être en principe réservées à des situations où plusieurs parties prenantes interviennent ensemble ou à tour de rôle dans un processus général complexe, des situations qui requièrent une gestion intelligente du risque.

Reprenons ici ce que l'on entend par dossier médical[1]. C'est un ensemble de documents (physiques ou informatisés) retraçant des épisodes qui ont affecté la santé du patient : lettres, notes, comptes-rendus, résultats d'examens de laboratoire, imagerie médicale, etc. Le dossier médical doit être soigneusement conservé pour la continuité des soins (il doit donc pouvoir être transmis au successeur du médecin de

[1] Extraits provenant de la définition donnée par Wikipédia

famille ou suivre le patient) pour répondre aux futures demandes d'accès des patients et même apporter certaines preuves en cas de recherche de responsabilités. Le passage progressif à la fin du XX^{e} siècle des dossiers papier aux dossiers numérisés ainsi que l'évolution des pratiques d'archivage et d'enregistrement, soulèvent des difficultés en termes de technique (durée de vie et fiabilité des supports numériques, sécurisation des données) et d'éthique médicale : confidentialité, dossiers dont la gestion est en partie sous-traitée dans d'autres pays ou par des entreprises privées, etc.

Dans le futur

On comprendra aisément qu'accéder en ligne à son dossier médical sera à l'avenir une réalité pour tous les citoyens. En effet, ces derniers devraient pouvoir accéder à toutes les données les concernant qui leur permettront de mieux se prendre en charge du point de vue de leur santé. Cela paraît utile s'agissant des patients souffrant d'affections chroniques qui auront accès à leurs résultats de laboratoire, leur rapport d'examens et surtout les recommandations de spécialistes et apprendront ainsi à mieux se comporter et se soigner. Si l'on veut que les patients puissent s'impliquer dans la prise en charge de leurs affections, ils doivent pouvoir accéder aux données et informations et surtout aux recommandations.

Questions ouvertes

Les blockchains questionnent le processus des soins médicaux. Beaucoup de questions restent ouvertes. Un tour d'horizon s'impose ici. Les points qui suivent ne prétendent pas à l'exhaustivité.

1.- Des contrats liés mais sans "tiers garants" ?

La force des blockchains réside dans ce que le patient accède par lui-même aux données qui le concernent et n'a donc plus besoin d'intermédiaires (tiers garants) pour cette tâche. Ainsi le passage (aujourd'hui souvent obligé) par un médecin "traitant" (anciennement le médecin de famille) pour valider des actes médicaux accomplis par d'autres soignants, pourrait dans bien des cas être supprimé. Au bout du compte se profile une économie non négligeable pour le système de santé en même temps qu'une meilleure coordination du système de soins par l'accès partagé à toute l'information disponible.

2.- Des smart contrats émetteurs de protocoles ?

Demain, les technologies du Deep Learning autoriseront la programmation d'algorithmes auto-apprenants capables d'effectuer non seulement des transactions sans l'intervention humaine mais aussi de se corriger, de s'améliorer tout au long des différentes transactions. Les algorithmes seront de façon croissante en mesure d'apprendre de leurs erreurs et tendront vers une intervention optimale ! Cette technologie sera particulièrement adéquate lorsqu'un savoir spécifique fait défaut dans un lieu donné ou n'est pas disponible à un moment donné.

A moyen terme, et selon les domaines, le recours à ces processus intelligents et automatisés pourrait s'avérer puissant.

3.- Des contrats mais aussi des registres étatiques en question ?

L'Etat est souvent le garant (tiers garant) des enregistrements privés tels que : propriétés foncières, actes de naissance, actes de mariage ou enregistrement de biens commerciaux. Ces registres tenus par les administrations publiques sont aujourd'hui légion. Demain, le code informatique des blockchains pourrait virtuellement tous les remplacer.

Ainsi la composante étatique propre à l'enregistrement pourrait à terme être remplacée par les blockchains. Parallèlement, on peut s'attendre à ce que les transactions de "pair à pair" soient appelées à connaître des développements très importants. De nouveaux services Internet (apps et sites web) seront alors développés pour prendre en charge et faciliter ces transactions de "pair à pair". Ne faut-il pas imaginer dès lors que les assurances privées offriront des services d'assistance juridique et de soutien en cas de conflit et de litige juridique ?

4.- Un cas délicat : le dossier patient

En principe, le dossier patient pourrait être facilement transformé en blockchain. Il deviendrait ainsi une base de données décentralisée, transparente, traçable, sécurisée, optimisée (à l'abri des erreurs, doublons ou oublis). En attendant ce jour, il est plus que certain que les protocoles des actes médicaux notamment de diagnostic, d'opérations ou de traitements seront les premiers à être mis en blockchain, car ce sont d'abord eux qui nécessiteront des actes de confiance, de sécurité, de transparence, de traçabilité et de partage. Les actes médicaux seront ainsi garantis par une forme de vérification partagée et inscrite dans le code.

Le dossier patient en blockchain balayera l'opacité actuelle de la santé. La transparence ouvre la discussion sur les processus complets de traitement pour les patients et leurs proches. Il faut donc s'attendre à l'avenir à enregistrer des processus davantage que des actes. Le protocole sera code. Dans le régime de la blockchain, en quelque sorte, c'est le code qui organise de nouvelles modalités de confiance, c'est le code lui-même qui fait office de "tiers de confiance".

L'enregistrement continu et documenté des relations médicales est également de nature à favoriser la discussion entre patients. Les réseaux sociaux joueront à plein leurs effets d'amplificateurs avec pour conséquence que le domaine de la santé sera beaucoup plus qu'aujourd'hui ouvert à l'intelligence collective. Ceci ne pourra pas aller dans un premier temps sans contreparties négatives avec évidemment les risques propres à l'ouverture et au partage.

5.- Comment appréhender la relation "Code versus Loi" si tout est dans le code ?

Les nouvelles infrastructures de type blockchain établissent de fait un nouvel état mondial pour l'architecture des relations juridiques. En effet, si le code (informatique-blockchain) fait loi, alors la question de la fabrication de la loi tendra à se déplacer. Ce ne sera plus une autorité qui définira un code de conduite *a priori* mais des pratiques qui seront jugées *a posteriori.* Tout le dispositif pivote vers la jurisprudence, vers le jugement *a posteriori.* En d'autres termes, le code (blockchain) assurera *a priori* la fonction du *tiers de confiance* dans une première phase, puis en cas de litige, *a posteriori* la justice devra traiter des affaires non résolues dans une seconde phase. Il est raisonnable de penser que l'usage des blockchains entraînera une redistribution des rôles et des responsabilités.

6.- En quoi une société de type Blockchain changera les choses ?

On assiste à la naissance d'une société sans intermédiaire en première ligne. De ce fait, la société tendra à se réorganiser d'abord autour du citoyen "augmenté" (du fait de l'*empowerment*) puis autour du pilier de la justice, qui pourrait voir son rôle fortement accru. Les traditions et la coutume continentales de l'*a priori* vont perdre de leur poids. La montée

en force du courant de la "désintermédiation" ne va pas faiblir. Les exemples d'Uber, Airbnb, etc. ne sont que les prémisses d'une société du tout direct. En effet, l'action directe des citoyens (et des patients) va "déborder" le système traditionnel, comme les professionnels de l'intermédiation et risque même de remettre en question certaines pratiques d'expertise scientifique. La vérité peut changer de camp... car certains ne verront plus l'utilité des intermédiaires classiques dans la société à mesure que les utilisateurs se tourneront de manière croissante vers les nouveaux systèmes d'intermédiation technologique.

7.- La blockchain médicale et l'exemple des radiologues

Un article scientifique[2] paru dans le prestigieux "New England Journal of Medecine" fait depuis trembler le monde des radiologues. Ecrit par le docteur Ziad Obermeyer de la Harvard Medical School et son collègue Ezekiel Emanuel de l'Université de Pennsylvanie, il décrit comment les nouvelles techniques de l'intelligence artificielle en s'appuyant sur les Big Data et les Machines Learning, seront en mesure de remplacer à terme les médecins radiologues en fournissant analyses et diagnostics en temps réel et sans frais!

La radiologie qui aujourd'hui coûte beaucoup d'argent au système de santé, est une cible privilégiée des innovateurs du "Digital health". En effet, lorsque l'on souhaite pénétrer un métier, celui de la médecine en l'occurrence, autant commencer là où les marges sont généreuses. Investir le champ de la radiologie en offrant un service équivalent, voire meilleur, tout en cassant les coûts, risque de valoir aux acteurs qui porteront ces transformations de larges soutiens.

---

[2] NEJM, 29 septembre 2016, Vol. 375 :13, pp. 1,216-1,219.

L'analyse des images est le champ d'activité de prédilection pour les algorithmes auto-apprenants car ces derniers sont très performants dans la reconnaissance de forme. Le Suisse Reto Wyss de la start-up Vidi à Fribourg, en est d'ailleurs l'un des développeurs les plus talentueux. Mondialement connu, il fait lire et interpréter à ses algorithmes auto-apprenants à peu près n'importe quelle vidéo. Chercher une pièce défectueuse à la sortie d'une chaîne de production ou un globule blanc anormal au milieu de milliers d'autres bien formés, fait partie de ses prouesses. Dès lors analyser une radio peut devenir demain un jeu d'enfant !

Ces algorithmes ne sont pas de type système-expert comme jusqu'à aujourd'hui, car ils ne s'appuient pas sur une expertise préétablie et normalisée dans des bases de données. A l'inverse, ils ne cessent d'apprendre et de se perfectionner avec le flux constant de données massives provenant de milliers d'expériences. Plus ces algorithmes sont alimentés en données provenant de cas concrets, plus ils s'améliorent, ils finissent asymptotiquement par fonctionner parfaitement. Un horizon fatal pour l'expert humain dont les limites peuvent toujours être atteintes contrairement ces "machines".

Le "Machine Learning", nom donné à cette discipline de l'intelligence artificielle, n'a pas fini de transformer notre monde car dès le moment où l'on a besoin d'analyser et/ou interpréter des images numériques, nul ne pourra prétendre être meilleur ou plus rapide que ces machines "intelligentes" et virtuelles.