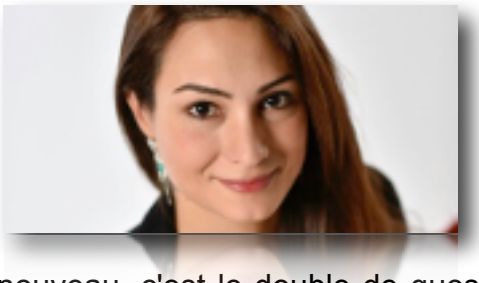
LA TRIBUNE

Par Cécile Monteil
08/07/2016

"La révolution Blockchain" : entre fantasme et réalité

La Blockchain, c'est la techno hype du moment. Les médias la proclament "nouvelle révolution technologique", les startups utilisant la Blockchain deviennent encore plus cool que celles qui travaillent sur le big data, et les grandes entreprises sont dans une course effrénée au partenariat avec ces dernières pour ne pas rater ce grand train. Mais au fait, c'est quoi la Blockchain ? Face à la confusion que suscitent de nombreux articles, le Dr Cécile Monteil a essayé de réunir les concepts clés de cette technologie au travers d'explications imagées.



Dr Cécile Monteil, urgentiste pédiatre, fondatrice de l'ONG Eppocrate et consultante pour la startup Stratumn. (Crédits : DR)

Lorsque l'on tente de s'informer sur le sujet, on se rend vite compte que la Blockchain, c'est complexe.

À chaque fois que l'on croit y comprendre quelque chose de nouveau, c'est le double de questions en plus et le doute sur ce que l'on avait compris la dernière fois.

Peut-être que le terme "Bitcoin" vous est plus familier ?

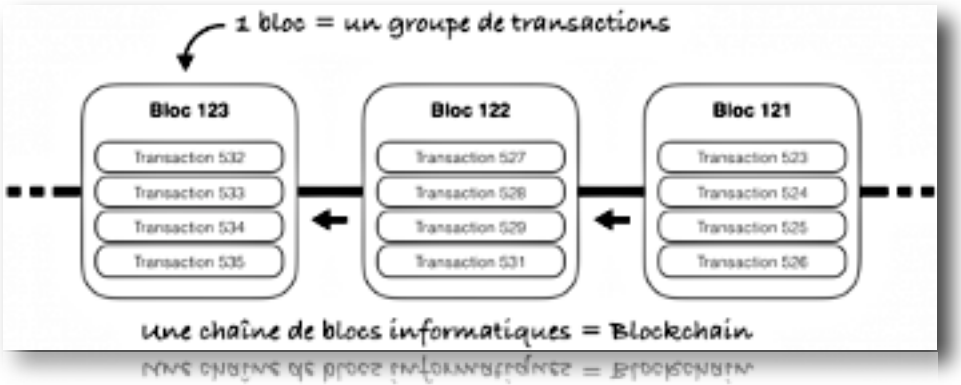
Cette monnaie digitale a beaucoup fait parler d'elle à ses débuts pour son utilisation dans le trafic de drogue ou le blanchiment d'argent. En effet, les malfaiteurs ne s'y étaient pas mépris en pariant sur la robustesse, la fiabilité et la sécurité de cette monnaie.

Quel rapport avec la Blockchain ?

Elle est la technologie sous-jacente permettant l'existence de la crypto-monnaie. Si le Bitcoin était la première application imaginée par son créateur, Satoshi Nakamoto, toujours inconnu aujourd'hui, la Blockchain est un outil technologique qui permet en fait de nombreuses autres applications, quel que soit le domaine (financier, juridique, médical, etc.).

Mais qu'est-ce que la Blockchain Bitcoin ?

Imaginez la Blockchain comme un grand cahier. Ce cahier est un registre public où sont consignés des échanges : les transactions. Chacun peut, ligne après ligne, y inscrire ses transactions et les horodater à l'aide d'un stylo indélébile. Ce cahier étant disposé dans un endroit accessible à tous, chacun peut le consulter à sa guise.



Ces transactions sont transparentes (visibles par tous) mais anonymes. En effet, pour réaliser leurs transactions, les personnes utilisent des "adresses bitcoins", sortes d'adresses email non nominatives et publiques, mais ne permettant pas de remonter vers les propriétaires.

En réalité, la Blockchain est un système informatique qui plutôt que de ressembler à un cahier, ressemble à une "chaîne de blocs" informatique ou "Blockchain" en anglais, répondant à des règles de fonctionnement cryptographiques.

Cette Blockchain est un registre de transactions qui sont regroupées en "blocs" et ajoutées au fur et à mesure à la chaîne de blocs, formant ainsi la "Blockchain".

Ce fonctionnement est possible grâce un réseau de centaines de milliers d'ordinateurs, "les mineurs", qui vérifient à plusieurs et à l'aide de calculs cryptographiques la validité de chaque bloc de transaction ajouté à la Blockchain.

Bien sûr, le travail des mineurs n'est pas gratuit ! Pour chaque nouveau bloc de transaction validé, ils sont rémunérés en bitcoin par deux procédés différents. D'une part, par le montant total des frais de transactions associés aux transactions du bloc en question, et d'autre part, par un montant "récompense" pour le travail effectué, provenant du pool de bitcoins n'ayant pas encore été attribué.

Pas encore attribué ? Une digression sur Bitcoin s'impose.

Bitcoin, ce nouvel "or digital"

L'or est un métal précieux, qui a la valeur de ce que les humains veulent bien lui accorder. À l'origine, sur Terre, il existe une quantité finie d'or. Lors de la ruée vers l'or, il était facile de recueillir de l'or à l'aide d'une simple passoire dans un ruisseau, mais avec le temps, il est devenu de plus en plus difficile d'en trouver. Les mineurs ont alors dû partir travailler de plus en plus difficilement dans des mines. L'or devenant alors rare, son prix augmente avec le temps.

Bitcoin, c'est un peu de "l'or digital". En 2009, Satoshi Nakamoto a mis en ligne 21 millions de bitcoins, enfermés dans un "coffre-fort" digital. Plutôt qu'une pioche, ce sont des logiciels informatiques installés sur des ordinateurs appelés mineurs, qui réalisent des calculs cryptographiques afin de gagner ces bitcoins, tout en validant les fameux blocs de transactions ! Le taux de création des bitcoins est prédéfini par un algorithme de Satoshi pour être rapide au début (facile), puis de plus en plus lent (difficile) avec le temps. Le dernier bitcoin devrait approximativement être émis en 2140.

Bien sûr, si les mineurs gardaient tous les bitcoins pour eux, ils ne vaudraient rien. Ils les revendent donc en échange de monnaies courantes selon le prix du marché (environ 600 euros en juillet 2016).

Aujourd'hui, de très nombreux sites acceptent les paiements en bitcoin : on peut acheter des billets d'avion, commander ses repas à domicile, payer une chambre d'hôtel ou s'acheter des chaussettes en bitcoin.

Une technologie anti-piratage

L'un des concepts phares de la Blockchain est sa fiabilité et sécurité infaillible. Ceci repose sur deux éléments fondamentaux :

- **Le fonctionnement de la Blockchain est décentralisé.** Le réseau de "mineurs" travaille de façon simultanée afin de valider chaque nouvelle information ajoutée à la Blockchain. Cette validation est consensuelle au sein du réseau et ne dépend d'aucune autorité centrale. Il n'y a pas de "chef" de la Blockchain !

- **La base de données de la Blockchain (les transactions) est distribuée**, c'est-à-dire que chaque mineur en possède une copie intégrale sur son ordinateur et peut confronter sa copie à celle du réseau. Pour les utilisateurs, elle est consultable et téléchargeable gratuitement sur Internet.

Ces propriétés uniques font de la Blockchain un registre impossible à pirater. Il faudrait en effet corrompre plus de 50% du réseau pour modifier la base de données existante. La puissance informatique nécessaire serait colossale et totalement hors de portée de quelque organisation que ce soit (même pour Google !).

Le Super-pouvoir de la Blockchain Bitcoin

La Blockchain offre une fonctionnalité cruciale : intégrer un "message" à chaque transaction, qui fera partie intégrante de celle-ci, bénéficiant donc du même niveau de sécurité. Mais, ce message ne peut contenir que 80 caractères ; et 80 caractères, c'est encore moins qu'un tweet ! On ne va donc pas stocker dans la transaction toute l'information qui nous intéresse, et qui est en général très volumineuse, mais seulement une preuve de cette information. Comment ?

Choisissez l'information dont vous voulez garder une preuve : un contrat, des photos, une vidéo, un livre, etc. Hachez cette information dans un "hachoir" à Blockchain par un algorithme dédié: le SHA256. Et vous obtiendrez un code unique lié à l'information entrée : un "hash", empreinte digitale cryptée de votre document et inférieur à 80 caractères, donc facilement intégré dans ce fameux "message".

C'est donc ce "hash" qui sera stocké sur la Blockchain, et non les informations initiales. L'intérêt fondamental de la Blockchain, c'est de pouvoir stocker avec chaque transaction une preuve d'information, afin de pouvoir démontrer ultérieurement et à tout moment l'existence et le contenu de cette information originale à un instant donné.

Ce mécanisme porte souvent à confusion, et beaucoup imaginent aujourd'hui que la Blockchain peut stocker directement et de façon parfaitement sécurisée leurs données (par exemple stocker son dossier médical), ou que toutes les informations stockées sur la Blockchain seront visibles aux yeux de tous puisque le registre est librement accessible à tous. Vous saurez maintenant que cela relève (encore) du fantasme. Cependant, on pourrait imaginer une convergence entre plusieurs technologies pour arriver à ce résultat, il nous reste alors du pain sur la planche !

Concrètement, quelles en sont les applications ?

La Blockchain est avant tout un outil technologique, qui trouve sa place dans de nombreuses situations où garder une preuve irréfutable d'informations, sans avoir à en révéler le contenu se révèle utile. Voici quelques exemples "de la vraie vie" :

➤ Faciliter les tâches administratives

Marre de remplir, parapher et signer des tonnes de papier en double exemplaire ? La Blockchain est à votre service ! La société Docusign, en partenariat avec Visa, développe une preuve de concept pour que l'expérience client lors d'un leasing de voiture soit enfin agréable.

Le client n'aura qu'à s'asseoir au volant de sa voiture de prédilection et se laisser guider. Au moyen d'une tablette, il complétera son choix de kilométrage, d'assurance, ou encore de téléchargement de musique, puis renseignera ses informations bancaires. Après une signature électronique des documents, chaque preuve de l'existence ("hash") de ces derniers sera gravée dans la Blockchain afin de garantir leur authenticité à l'instant de la signature, et une copie des documents sera envoyé au client par mail. Il ne restera alors qu'à allumer le moteur de la voiture et prendre la route !

➤ La finance : les Marchés boursier

Nasdaq, le plus grand marché électronique d'actions au Monde l'avait dit : ils seront le premier marché boursier à essayer la Blockchain, et ils l'ont fait !

Leur 1er essai a été mené avec succès : garantir l'enregistrement de l'émission d'actions de la société Chain vers l'un de leur investisseur privé via "Nasdaq Linq", une plateforme basée sur la Blockchain.

La preuve de l'existence de la propriété des nouvelles actions émises a été tracée dans la Blockchain, sans aucun papier, et le délai de règlement de l'opération a été réduit de quelques jours à quelques minutes, un gain de temps significatif dans ce domaine !

➤ La santé : les essais cliniques

Tout le monde a eu vent de scandales où certains chercheurs, n'aboutissant pas au résultat espéré, ont traficoté les données d'essais cliniques (modification des objectifs en cours de route ou des données recueillies, invention de faux-patients, etc). Grâce à la Blockchain, chaque étape de l'essai clinique pourrait être tracée de façon cryptée et horodatée. Il deviendrait alors facile d'auditer et de vérifier l'intégrité des essais clinique et de leurs résultats.

Une preuve de concept a déjà été réalisée par une équipe de chercheurs à Oxford, qui a tracé dans la Blockchain les informations postées sur clinicaltrials.gov avant et après résultats, afin de vérifier si les objectifs et les informations concernant les études n'avaient pas été modifiés après la réalisation de l'étude.

Et en 2016, où en sommes-nous ?

La Blockchain détient un pouvoir disruptif majeur, apportant une nouvelle façon de réaliser des opérations avec plus de transparence, de fiabilité et de sécurité. En 2016, il est clair que nous n'en sommes qu'aux prémices. Alors que la Blockchain Bitcoin de Satoshi Nakamoto était unique au départ, son caractère open source est en train de faire fleurir d'autres Blockchains d'inspiration commune, mais possédant des propriétés différentes, s'attachant à résoudre des problèmes plus différents les uns que les autres.

Ce qu'il manque encore fondamentalement, ce sont les outils qui faciliteront l'utilisation de la (des) Blockchain(s), aujourd'hui très complexe. En attendant, restons attentifs aux résultats des nombreuses expérimentations d'utilisation de la Blockchain qui commencent à pointer le bout de leur nez, et observons la magie opérer !

Par Dr Cécile Monteil,
urgentiste pédiatre,
fondatrice de l'ONG Eppocrate
et consultante pour la startup Stratumn.