



La technologie Blockchain ou une invention contre-pouvoir

Fiche pratique publié le 16/03/2021, vu 1311 fois, Auteur : [La zone du droit](#)

En 2019, internet a soufflé ses trente bougies. Il s'agit d'une grande invention sans précédent que le monde ait connu. Il y a de quoi à être en admiration quand on voit comment internet a transformé le monde.

En 2019, internet a soufflé ses trente bougies. Il s'agit d'une grande invention sans précédent que le monde ait connu. Il y a de quoi à être en admiration quand on voit comment internet a transformé le monde. Le web et ses ramifications se sont étendus dans toute la sphère de notre quotidien.

De plus en plus de machines communiquent entre elles. Les progrès sont si rapides que même les spécialistes n'arrivent plus à suivre la cadence.

Les données sont la ressource la plus prestigieuse de cette nouvelle ère du numérique. Des milliers d'appareils sont connectés entre eux et collectent d'énormes données.

Les données sont devenues également des ressources inestimables et l'accès au big data aboutit au développement de nouvelles technologies.

Google par exemple dépend des données que ses utilisateurs mettent à sa disposition souvent même sans le savoir. Internet se caractérise par la situation de monopole qui s'est installée ces dernières années.

Mais qui en a vraiment le contrôle ? La technologie Blockchain offre aux personnes concernées la possibilité de contrôler leurs propres données. Force est de constater que les hommes collaborent de moins en moins avec leurs semblables, préférant se tourner de plus en plus vers la technologie.

« La Blockchain » a été inventée en 2008 par un homme ou une femme ou un groupe de personnes sous le nom Satoshi Nakamoto. Personne ne sait qui se cache derrière ce nom. La Blockchain ou technique de registre partagé (Distributed Ledger Technology, DLT) est une technologie reposant sur la technique du consensus et destinée à remplacer tous les tiers de confiance. La Blockchain est un système communautaire en vrai. La base de données, distribuée, partagée et cryptée sert de répertoire d'informations public irréversible et incorruptible.

La Blockchain est susceptible de nombreuses applications dans tous les domaines même si le secteur financier et bancaire est privilégié aujourd'hui. Elle a donc une fonction de conservation de données ou de documents ; c'est une plateforme permettant des transactions, des transmissions ; elle peut être le support de smart contracts.

À l'origine de la création, il y a la méfiance des consommateurs dans les banques suite à la crise des « subprimes ». L'idée a alors germé de développer un système permettant de se passer des banques et plus généralement de tous les tiers de confiance.

En outre, le premier réseau au monde utilisant la Blockchain est le « Bitcoin » créé en 2009. Il fonctionne sans interruption depuis. Le bitcoin est une crypto monnaie qui ne dépend pas d'une banque centrale. Cet argent virtuel sert de moyen de paiement sous la forme de « Tokens » et peut faire l'objet de transaction entre utilisateurs. Pour l'heure, il est à noter que peu de gens comprennent la technologie Blockchain.

De plus, le principe de la Blockchain est que chacun des participants reçoit copie des données échangées, ce qui lui permet de savoir quelle transaction a eu lieu.

Les cryptomonnaies et la technologie Blockchain constituent dès lors un contre-pouvoir face « aux dérives des gouvernements et des banques centrales ». La Blockchain est un système communautaire en vrai.

l) La Blockchain : une technologie dépourvue d'un organe central

En 2015, la Blockchain reçoit du très sérieux journal *The Economist* son diplôme de respectabilité en étant présentée comme « Une machine à confiance » (« The Trust Machine », 31.10.2015, *The Economist*). Cette nouvelle technologie permet d'échanger de la valeur sans tiers de confiance.

Le site web « *Blockchain France* » présente la Blockchain comme une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

C'est également une technologie disruptive qui se donne pour ambition de supprimer les tiers de confiance. Il s'agit des organismes habilités à mettre en œuvre des signatures électroniques à permettre l'échange de biens, l'échange d'informations sur Internet. Il peut aussi s'agir d'organismes assurant la sécurisation des transactions de biens comme des paiements. Sont par exemple des tiers de confiance, l'État, les notaires, les chambres de compensation, les plateformes telles Paypal, les plateformes collaboratives, les banques, les assureurs.

Pour ses initiateurs, il s'agit de limiter le pouvoir des institutions existantes. On fait confiance sans se rencontrer. La confiance, c'est l'ambition des promoteurs qui ne doit reposer que sur la seule technologie. La technologie a ainsi été désignée sous le nom évocateur de trust machine.

Toutes les applications envisagées par la Blockchain visent en réalité à remettre en cause les institutions en place quelles qu'elles soient y compris les juges.

Ces évolutions technologiques et les nouvelles voies qu'elles ouvrent en matière de transactions constitueraient avant tout une réponse à la défiance qui vise les tiers de confiance en général et les états en particulier, lesquels sont les sources du droit moderne.

Que ce soit sur internet ou même dans d'autres structures sociales, les intermédiaires sapent le réel pouvoir démocratique car ce sont eux les opérateurs privés qui déterminent nos relations les uns aux autres. Ils détiennent le contrôle absolu sur les données et informations échangées entre les utilisateurs du réseau.

Il est donc de notre intérêt à tous de supprimer ces intermédiaires ou du moins de limiter leur influence dès lors qu'une technologie meilleure existe comme la Blockchain.

Par ailleurs, les transactions sur le réseau bitcoin sont vérifiées et validées par les agents du réseau eux-mêmes et cela rend superflu les intermédiaires centralisés tels que les banques.

Aussi, plusieurs transactions ainsi que la signature d'un contrat ou d'un virement monétaire sont regroupés en un bloc et enregistrés dans un registre virtuel. Un procédé cryptographique complexe fait d'algorithmes relie ces blocs les uns aux autres : c'est la fameuse « chaîne de bloc ». La particularité, c'est que toute la chaîne est enregistrée sur tous les ordinateurs des participants au réseau et pas uniquement sur une instance centrale tel le serveur d'une banque.

Toutes les données sont accessibles de façon décentralisée. Avec une Blockchain, quasiment tout ce qui se passe dans nos vies peut être considéré comme une transaction (un mariage, l'envoi d'un colis, le paiement d'un billet de train etc.). Ces événements sous la forme de transaction peuvent être gérés et enregistrés sur une Blockchain. Le principe de la Blockchain empêche toute manipulation a posteriori.

Sur un réseau Blockchain les transactions peuvent être automatisées grâce à un programme appelé « smart contract » ou « contrat intelligent ». Il vérifie que certaines conditions sont remplies et procède directement à la transaction.

De plus, la Blockchain est antinomique à l'État. En effet, elle déstabilise les fondements de son autorité, en ce que la règle du consensus remplace l'idée d'une décision centralisée au moment de la formation de chacun de ses blocs à la dernière étape du minage.

Enfin et surtout, la Blockchain bouleverse la manière dont la confiance est générée : traditionnellement adossée aux institutions depuis l'apparition des monnaies fiduciaires, elle s'en émancipe grâce à la fiabilité technique – cryptographie asymétrique et architectures informatiques distribuées – et aux conséquences psychologiques engendrées par la technologie – on peut la modifier par la volonté.

II) Une technologie transparente, sécurisée et à l'abri des tiers de confiance selon les utilisateurs

L'intelligence artificielle est un « ensemble de systèmes qui font preuve d'un comportement intelligent en analysant l'environnement et en permettant des mesures avec un certain degré d'autonomie pour atteindre des objectifs précis ».

L'algorithme, la Blockchain sont animés par une sorte d'intelligence :

- humaine : qui permet de les développer
- Artificielle : intelligence

En 2008, la Blockchain est née dans un contexte qui n'est pas anodin : celui de la plus grande crise financière que le monde ait connu depuis 1929, une crise suscitant la défiance envers les habituels tiers de confiance que sont les états ou les banques.

La Blockchain peut donc être définie comme « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ».

Il est en effet aujourd'hui possible d'obtenir un niveau de confiance au moins aussi fort uniquement grâce à cette technologie.

Dans ce contexte, les concurrents du droit officiel-étatique tels que les Blockchains peuvent prospérer, offrant une transparence totale et une désintermédiation permettant de ne plus s'appuyer sur des tiers de confiance. Le pouvoir appartient désormais aux utilisateurs et aux consommateurs, qui profitent de processus simplifiés et d'une haute qualité de l'information fournie. Cela est favorable à la stabilité et à la sécurité des transactions.

Ordinairement, la confiance est la croyance ou la foi dans la fiabilité d'une personne ou d'un système. Cette confiance reposait jusqu'à présent sur l'association de la technique, de l'organisation et du droit. Avec les Blockchains, on s'en remet entièrement à la technologie. C'est ainsi que les « smart contracts » permettent à deux partenaires de nouer une relation commerciale sans se connaître et sans tutelle d'une autorité centrale. Le système en lui-même garantit la validité et l'honnêteté de la transaction. La confiance ne dépend plus des hommes mais des machines - « The Trust Machine », comme l'a titré *The Economist* au sujet des Blockchains.

La crise de confiance actuelle touche en particulier le secteur bancaire et il n'est guère étonnant que le bitcoin et l'ether, qui sont des cryptomonnaies reposant sur la technologie Blockchain, donnent lieu à de véritables systèmes monétaires indépendants et parallèles par rapport aux systèmes monétaires étatiques et bancaires.

Ce sont jusqu'aux tiers de confiance de l'économie collaborative qui peuvent être touchés par les applications des Blockchains (Uber, Airbnb, eBay, Paypal, etc.). Aussi les Blockchains pourraient-elles bouleverser la nature même de l'organisation des sociétés actuelles, ce que n'ont pas fait Uber et ses semblables - qui se sont finalement contentés de remplacer des prédateurs capitalistes par d'autres prédateurs capitalistes.

Chacun possède aussi une méga-identité dont il est propriétaire. Il n'y a plus besoin de confier ses données à des tiers. L'une des promesses phares de la technologie Blockchain est de remplacer les tiers de confiance et d'assurer l'exécution plus fine et surtout automatique de certains contrats qui intéressent le monde des créateurs par exemple. La Blockchain peut être un outil dont se serviront les maisons d'édition ou les sociétés de gestion collective des droits, mais elle peut aussi devenir un outil qui remplace ces tiers de confiance dans une certaine mesure.

Les Blockchains sont sécurisées par différents mécanismes, notamment par des techniques cryptographiques avancées et des modèles mathématiques de comportement et de prise de décision. La technologie Blockchain est la structure de base de la plupart des systèmes de cryptomonnaie et empêche ce type de monnaie numérique d'être dupliqué ou détruit.

Les Blockchains s'appuient en grande partie sur la cryptographie pour assurer la sécurité de leurs données. Une fonction cryptographique extrêmement importante dans un tel contexte est celle du hachage. Le hachage est un processus par lequel un algorithme appelé fonction de hachage reçoit une entrée de données (de n'importe quelle taille) et renvoie une sortie déterminée contenant une valeur de longueur fixe.

La sécurité de la transaction est assurée par un réseau d'ordinateurs qui valident et certifient la transaction avant de l'inscrire de manière définitive dans un bloc. Une fois enregistrée, cette dernière devient infalsifiable et transparente, facilement vérifiable. Il s'agit donc d'un réseau distribué au sein duquel les transactions s'effectuent en pair à pair. La technologie de la Blockchain permet la sécurisation, la capitalisation, la traçabilité et la mesure des échanges entre

pairs.

La transparence s'étend également dans le temps car l'ensemble des informations est stocké sans limite de durée sur la Blockchain. Il est donc possible de connaître l'origine d'un versement par exemple, mais aussi de connaître les versements précédents l'ayant rendu possible, ainsi que les versements précédents les ayant rendus possibles etc.

Cette transparence, doublée d'une facilité d'accès (une connexion à Internet suffit) permet une vision complète des transactions réalisées sur une Blockchain et des données ou informations qui peuvent y être placées. La Blockchain permettrait ainsi d'améliorer la prestation de services du fait de l'automatisation, de l'immutabilité (des blocs de données composant la Blockchain) et des rapports en temps quasi-réel autorisés par les smart contracts, en particulier dans les domaines où une preuve d'identification est requise.

Enfin, si la technologie venait à remplacer certains tiers de confiance, il serait important qu'elle puisse être contrôlée. Or, il a été observé que les mineurs étaient le plus souvent chinois. Par ailleurs, il est difficile d'imaginer que toute la technologie soit entre les mains de quelques géants de l'informatique qui seront sans doute chinois et américains. Aussi, la principale difficulté que présente la Blockchain est son défaut de régulation et par conséquent de valeur juridique et d'opposabilité aux tiers.

Sources :

<https://Blockchainfrance.net/decouvrir-la-Blockchain/c-est-quoi-la-Blockchain/>

<https://Blockchainfrance.net/2018/05/22/comprendre-les-tokens/>

<https://Blockchainfrance.net/2016/01/28/applications-smart-contracts/>

<https://www.haas-avocats.com/data/Blockchain-machine-preuve/>

<https://www.zdnet.fr/blogs/social-media-club/la-Blockchain-va-t-elle-tuer-les-tiers-de-confiance-39865540.htm>

<https://www.contrepoints.org/2017/10/02/299965-cryptomonnaies-nouveau-contre-pouvoir>

<https://bitcoin.org/fr/>

<https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>

https://fntc numerique.com/upload/Communiqués_de_presse_pdfs/_Tribune_Blockchain_DEF.pdf

<http://www.hbrfrance.fr/chroniques-experts/2016/07/11628-open-innovation-co-creation-pourquoi-la-Blockchain-est-une-petite-revolution/>

https://www.lexis360.fr/Document/Blockchain_le_droit_et_la_technologie_Blockchain_une_approche_sec

<https://academy.binance.com/fr/articles/what-makes-a-Blockchain-secure>