

Les blockchains : une invention qui n'a pas dix ans

Description

[Les usages des bases de données distribuées de type *blockchain*](#)

[Breveter l'open source](#)

[Les ICO](#)

[Piratage et arnaques](#)

[Des régulations tâtonnantes](#)

[Internet et blockchains](#)

Si en chimie, « *rien ne se perd, rien ne se crée : tout se transforme* »¹, en informatique, tout se copie. Tout du moins jusqu'en 2008. Qu'une suite de 0 et de 1 puisse être copiée est d'ailleurs le fondement même des technologies de l'information et de la communication. Or, comme l'écrivent Adli Takkal Bataille et Jacques Favier dans *Bitcoin, la monnaie acéphale*², pour la première fois depuis l'invention de l'informatique, « *le protocole Bitcoin a réussi à créer un bien numérique non reproductible* ».

Le protocole Bitcoin a réussi à créer un bien numérique non reproductible
Adli Takkal Bataille et Jacques Favier

Lorsque Satoshi Nakamoto, pseudonyme d'une personne ou d'un groupe, publie en novembre 2008 l'article fondateur « *Bitcoin : un système de paiement électronique pair-à-pair* », il propose « *une solution au problème de la double dépense* ». En effet, le problème majeur d'une monnaie électronique, qui par définition peut-être recopiée, consiste à s'assurer qu'une personne ne dépensera pas deux fois la même somme d'argent. Avec l'invention du Bitcoin, pour la première fois, la propriété d'un bien numérique peut être transférée sans être dupliquée ni passer par un registre centralisé.

Ce que décrit exactement Satoshi Nakamoto est « *un réseau [qui] horodate les transactions en les hachant en une chaîne continue de « preuves-de-travail », formant un enregistrement de données qui ne peut pas être changé sans avoir à refaire la « preuve-de-travail »* ». Ce que l'on appelle communément aujourd'hui *blockchain* correspond en réalité à la combinaison de plusieurs technologies : un protocole de réseau pair-à-pair, le minage par la preuve de travail, la cryptographie asymétrique et, enfin, une *blockchain* ou plus précisément une « *base de données distribuée de type blockchain* ».

Explications : avoir un compte Bitcoin requiert au préalable de télécharger sur un ordinateur ou sur un smartphone un « porte-monnaie » appelé aussi *wallet*. Ce porte-monnaie permet à un utilisateur de générer des adresses *bitcoin*. Chaque adresse, par exemple 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa, est en

réalité une paire de clés cryptographiques composée d'une clé privée et d'une clé publique. Pour recevoir des *bitcoins*, un utilisateur fournira une adresse, générée à partir de sa clé publique, et qu'il renouvellera, idéalement, à chaque transaction. Tandis que pour envoyer des *bitcoins* à l'adresse du destinataire, il signera la transaction avec sa clé privée.

Pour la première fois, la propriété d'un bien numérique peut être transférée sans être dupliquée ni passer par un registre centralisé

La signature et la vérification des transactions en *bitcoins* reposent sur la cryptographie asymétrique, c'est-à-dire que la clé privée permet de vérifier l'authenticité d'une signature à partir de la clé publique, l'inverse étant bien évidemment impossible. L'ensemble des transactions en *bitcoins* consiste ainsi à débiter certains comptes pour en créditer d'autres. Ces transactions sont enregistrées dans des fichiers que l'on appelle des blocs. Un bloc représente l'équivalent de dix minutes de transactions, et comporte le « résumé » du bloc précédent. Pour garantir l'intégrité des blocs, enchaînés chronologiquement les uns après les autres, depuis la première transaction en *bitcoin*, effectuée en 2009, le système utilise des « fonctions de *hash* ». Une fonction de *hash* est une fonction mathématique qui transforme n'importe quel contenu sous la forme d'un nombre hexadécimal.

Par exemple, le titre « La revue européenne des médias et du numérique » *hashé* donne « EDD559832CFB3B135BFAD11A0EB68D34F1C77D252140EAE01D8D3FE8EE0FBEDE ». Mais « la revue européenne des médias et du numérique », sans majuscule au début, donne « C39398ED08D75CC4CAA03D7FA223B3193E6212F1026021D0B1328760E5E8403C ». À la moindre modification du contenu, le nombre *hashé* devient totalement différent. Il est possible de *hasher* une phrase ou un mot de passe, tout comme *L'Iliade et l'Odyssee in extenso*. L'intérêt d'une fonction de *hashage* est qu'elle ne s'applique que dans un sens : le *hash* obtenu ne permet ainsi pas de remonter au contenu d'origine, en revanche il suffit de *hasher* à nouveau ce contenu pour vérifier que le *hash* en résultant est identique, preuve qu'aucune modification n'est intervenue. Les blocs du Bitcoin sont ainsi *hashés* et permettent d'avoir la garantie qu'ils n'ont jamais été modifiés depuis la première transaction.

Comme son nom l'indique, la *blockchain* est un enchaînement de blocs, chacun contenant le *hash* des blocs précédents, qui regroupe des transactions. Cette *blockchain* est synchronisée et stockée dans tous les ordinateurs de ceux qui l'utilisent. C'est une monnaie électronique décentralisée. Chaque ordinateur possédant une copie de la *blockchain* est appelé un « nœud » du réseau et vérifie en permanence l'intégrité de celle-ci.

Les nouveaux blocs sont créés par certains nœuds du réseau appelés les mineurs. Ils mettent à la disposition du système leur puissance de calcul pour résoudre un problème mathématique complexe dont le principe est de trouver un nombre *hashé*. Comme il est impossible de retrouver le contenu original à partir du *hash*, l'ensemble des ordinateurs qui « minent » calcule toutes les possibilités pour arriver au résultat. Cette opération, appelée validation par « preuve de travail » (*proof-of-work*), ne peut être obtenue que par la

réalisation d'une tâche fortement consommatrice en énergie et en puissance de calcul.

Le système est conçu de telle sorte qu'il faudrait contrôler plus de 50 % de la puissance de calcul de tous les ordinateurs qui minent dans le monde pour arriver à modifier un bloc à l'insu de tous. C'est pour cette raison que, à ce jour, le Bitcoin et les *blockchains* n'ont jamais été piratées. La difficulté du minage est automatiquement ajustée en fonction du nombre d'ordinateurs en train de *hasher*, afin qu'un nouveau bloc soit généré en moyenne toutes les dix minutes. À chaque fois qu'un ordinateur trouve la bonne réponse, le bloc est créé et le mineur est rémunéré 12,5 *bitcoins*. C'est de cette façon qu'est programmée la création d'unités de compte *bitcoins*. Le protocole a été conçu pour que les *bitcoins* soient créés graduellement sans qu'une instance centrale s'en charge.

Il est également prévu dans le code informatique que plus la chaîne croît, plus il est difficile de miner des *bitcoins*, et plus la rémunération baisse. C'est pourquoi si, aux débuts du Bitcoin, des particuliers minaient sur leur ordinateur, la puissance de calcul nécessaire est aujourd'hui telle qu'ils sont supplantés par des entreprises qui font travailler des milliers de serveurs dans des entrepôts, notamment en Chine. Depuis janvier 2009, environ 16 millions de *bitcoins* ont été émis et seuls 21 millions seront générés en tout et pour tout, le dernier devant être produit en 2140.

Les bases de données distribuées de type *blockchain*
sont à la transaction ce que les protocoles
TCP et IP sont à la transmission d'information
via l'internet

Par extension, la « chaîne de blocs » peut être assimilée à un grand livre des comptes, public, anonyme et infalsifiable ([voir La rem n°37, p.67](#)). Il est d'ailleurs intéressant de noter que, pas une seule fois, le mot *blockchain* n'est cité dans le texte fondateur de Satoshi Nakamoto.

Les bases de données distribuées de type *blockchain* sont à la transaction ce que les protocoles TCP et IP sont à la transmission d'information via l'internet. Le code informatique de la plupart des *blockchains* publiques étant *open source*, quiconque possédant les compétences informatiques requises peut mettre en place une *blockchain*. Au-delà du Bitcoin, il existe aujourd'hui près de 1 150 registres distribués de type *blockchain* publique, dont la convertibilité en monnaie légale est assurée par des milliers de plates-formes de change à travers le monde. Lorsque les *blockchains* sont publiques, comme Bitcoin, Ether ou Monero, tout le monde, avec une connexion internet et un ordinateur, peut accéder à leurs services. Lorsqu'elles sont privées, leur utilisation est limitée à certains acteurs.

L'avènement du pair-à-pair pour certifier et enclencher automatiquement des transactions ouvre des perspectives inédites

À partir du protocole Bitcoin créé pour produire une base de données enregistrant l'ensemble des transactions opérées par ses utilisateurs, une déclinaison de la *blockchain* a été inventée en décembre 2013 par Vitalik Buterin. Baptisé Ethereum, ce protocole d'échanges décentralisés permet la création de « contrats intelligents ». Il utilise Solidity, un langage de programmation dit Turing-complet, parce qu'il permet de programmer l'ensemble des fonctions calculables au sens de Turing, à savoir quasiment toutes les fonctions que l'on connaît des langages de programmation modernes. Ces contrats intelligents permettent de vérifier et de mettre en application des accords mutuels qui sont enregistrés et consultables publiquement dans la *blockchain* d'Ethereum. L'intérêt de ces contrats est qu'ils sont autonomes, répliqués dans tous les nœuds de la *blockchain*, et que leur exécution ne passe pas par un tiers de confiance pour en garantir la validité.

L'avènement du pair-à-pair, non plus simplement pour transmettre et recevoir des informations mais également pour certifier et enclencher automatiquement des transactions, ouvre des perspectives inédites aux utilisateurs d'internet : particuliers, entreprises et États.

Les usages des bases de données distribuées de type *blockchain*

Il n'aura fallu que quelques années pour que de nombreuses entreprises s'emparent de cette invention et appliquent à divers domaines, outre la banque, ce que le Bitcoin réinvente pour la monnaie : passer d'un fonctionnement centralisé à une organisation décentralisée. Chacune de ces entreprises déploie des services basés sur un registre distribué dont la promesse, à l'instar de la cryptomonnaie, repose sur l'élimination des tiers de confiance historiques (notaire, administration, société de gestion de droit d'auteur...). L'utopie dont est porteur ce modèle de base de données peut s'étendre à tous les domaines nécessitant un organe central ou un tiers de confiance, mais également à toute activité pour laquelle des échanges entre de multiples acteurs induisent de nombreux contrôles, des problèmes de logistique, de lourdeur administrative et parfois de corruption.

Comme aux débuts de l'automobile, lorsque la France comptait 155 constructeurs en 1914, de nombreuses expérimentations en cours dans le monde témoignent de cet engouement pour les *blockchains*, dont l'intérêt et l'utilité des services proposés sont parfois relatifs. Selon le site blockchainfrance.net, les applications se classent en trois catégories :

- le transfert d'actifs, comme des monnaies électroniques, des titres, des actions ou des obligations ;
- la tenue d'un registre, garantissant son intégrité comme l'établissement d'un cadastre ou la certification de diplômes ;
- l'exécution automatique de programmes autonomes, appelés *smart contracts*.

Transfert d'actifs

Rappelons que l'article de Satoshi Nakamoto a été publié en pleine débâcle financière, deux ans après la

crise des *subprimes* aux États-Unis et au moment où, en septembre 2008, plusieurs établissements financiers américains entraient en cessation de paiement.

C'est dans ce contexte que le Bitcoin a été conçu comme un système permettant le transfert d'actifs à travers une monnaie électronique entièrement décentralisée dont les transactions sont validées et sécurisées par les utilisateurs eux-mêmes. D'abord confidentiel, il faudra attendre 2013 pour que la spéculation donne un coup de projecteur au Bitcoin, dont le cours, passé de 100 à 1 000 dollars en quelques semaines, attire les foudres et les critiques des professionnels de la banque et des experts de la finance qui furent, et sont encore nombreux, à prédire sa mort imminente. Au-delà de l'aspect sulfureux du Bitcoin souvent associé au *darknet* ([voir La rem n°33, p.63](#)), force est de constater que le transfert d'actif sans passer par un organe central trouve des applications de bon sens.

Le marché du transfert d'argent en est un bon exemple. Selon la Banque mondiale, ce marché va représenter 636 milliards de dollars en 2017. Les opérateurs de transfert, comme Western Union, prennent quelque 10 % de commission sur chaque transaction, et encore plus lorsque les transferts concernent l'Afrique, qui perd ainsi, selon l'ONG Overseas Development Institute, près de deux milliards de dollars par an. Le transfert d'argent entre particuliers *via* une *blockchain* ferait disparaître les commissions exorbitantes de ces intermédiaires. Par exemple, la fondation Stellar, organisme sans but lucratif créé en 2014 par Jed McCaleb, a pour but de développer un réseau de paiement transfrontalier à faible frais, accessible à tous et rapide. La cryptomonnaie émise par Stellar, appelée Lumen, est directement convertie en monnaie fiduciaire locale par des banques partenaires, la compensation ainsi que le règlement des transactions transitant par un réseau unique opéré par IBM. Alors qu'un transfert d'argent, assujéti à une commission calculée en pourcentage, passe par de nombreux intermédiaires et prend aujourd'hui plusieurs jours, une transaction entre particuliers *via* cette *blockchain* ne coûte que quelques centimes et est validée en quelques minutes. La plate-forme est actuellement limitée aux paiements transfrontaliers en livres britanniques et en dollars fidjiens, mais devrait à l'avenir concerner sept autres devises d'États du Pacifique Sud, notamment le dollar australien, le dollar néo-zélandais et le pa'anga des Tonga.

Les transactions sont validées et sécurisées par les utilisateurs
eux-mêmes

Le transfert d'actifs ne concerne pas uniquement les particuliers. Depuis l'automne 2015, les banques et les institutions financières considèrent les *blockchains* comme une opportunité pour économiser d'importants frais liés au transfert d'argent. R3 est à la fois une start-up américaine créée en septembre 2015 et un consortium regroupant neuf banques à son lancement, parmi lesquelles Barclays, Crédit Suisse, Goldman Sachs, JP Morgan (qui a depuis quitté le consortium) ou encore la Royal Bank of Scotland. Rejointes sans plus attendre par d'autres institutions financières dont la Société Générale, BNP Paribas ou encore Natixis, ce sont aujourd'hui quelque 80 établissements financiers du monde entier qui mènent de concert des travaux portant sur les *blockchains*. Il s'agit, non plus de *blockchains* publiques et ouvertes à tous, mais de *blockchains* privées, où les nœuds du réseau sont prédéterminés. Si la perspective de réduction des coûts

pour le secteur bancaire, jusqu'à 20 milliards de dollars par an, a fait rêver plus d'un directeur d'institution financière, des tensions liées à la gouvernance, la concurrence entre les acteurs et l'absence de résultat immédiatement opérationnel ont déjà provoqué le départ de certains. D'autres initiatives existent, par exemple celle d'UBS, Deutsche Bank, BNY Mellon et Santander, qui souhaitent lancer l'Utility Settlement Coin en 2018, dont le fonctionnement s'inspirerait de la *blockchain* Bitcoin. Mais « *il s'agit plutôt d'une nouvelle architecture IT permettant de faire de la compensation et du règlement plus rapidement* », explique Gonzague Grandval, cofondateur de Paymium.

La tenue d'un registre

Les bases de données distribuées de type *blockchain* trouvent également, comme domaine de prédilection, la tenue d'un registre infalsifiable et transparent, par exemple, pour l'établissement d'un cadastre ou pour la certification des diplômes.

Au Honduras, le gouvernement a inscrit dans une *blockchain* publique l'intégralité des titres fonciers du territoire afin d'éviter l'appropriation unilatérale des terres par certains, et garantir aux yeux de tous que le cadastre ne soit pas modifié ou altéré. Au Ghana, une initiative similaire, menée par l'ONG Bitland, permet d'enregistrer les actes fonciers associés à des coordonnées GPS qui, une fois inscrits dans une *blockchain* appelée Bitshare, sont immuables sans un transfert de propriété en bonne et due forme. Depuis 2016 en Géorgie, l'initiative est directement portée par le gouvernement, avec le concours de l'entreprise Bitfury. Loin d'« uberiser » les notaires, ces initiatives prennent forme dans des pays où l'absence de cadastre et de services notariés, ainsi qu'un haut niveau de corruption, incitent des start-up à proposer ce genre de services ou les États eux-mêmes à mettre en place un cadastre inviolable.

Régulièrement dénoncée par les écoles et par les entreprises, la fraude au diplôme serait un fléau en constante progression. Pour ne citer qu'un seul cas tristement célèbre, Gilles Bernheim, grand rabbin de France, a reconnu avoir menti sur son CV, en 2015, en usurpant le titre d'agrégé de philosophie, mentionné dans toutes ses biographies. Des entreprises, comme Verifdiploma fondée en 2000, se sont lancées sur ce créneau d'authentification des diplômes et autres certificats d'un candidat. Une des solutions mises en œuvre par l'ESILV (École supérieure d'ingénieurs Léonard de Vinci) en partenariat avec la société Paymium en France, ou par l'École d'ingénieurs Holberton à San Francisco, aux États-Unis, avec la société Bitproof, a été d'enregistrer la signature de chaque diplôme dans la *blockchain* Bitcoin et de tenir ainsi à jour le registre de leurs diplômés.

L'exécution automatique de programmes autonomes, appelés *smart contracts*, est l'un des domaines les plus prometteurs

Il est, à la fois, extrêmement difficile de falsifier un tel registre, qui horodate par ordre chronologique l'ensemble des diplômes émis par l'école et très simple pour une entreprise de vérifier dans ce même registre si un candidat est bel et bien diplômé de ladite école. En France, le ministère de l'éducation

nationale et le rectorat devraient s'emparer du sujet au plus vite afin de moderniser le Répertoire national des certifications professionnelles (RNCP), registre des diplômes reconnus par l'État, ce qui permettrait de les distinguer facilement de ceux qui ne le sont pas. Serait en même temps créée une *blockchain* publique dans laquelle les écoles et les universités inscriraient leurs diplômés, cette base de données pouvant être consultée par tous les employeurs de France ou de l'étranger.

Les *smart contracts*

L'exécution automatique de programmes autonomes, appelés *smart contracts*, est l'un des domaines les plus prometteurs des bases de données distribuées de type *blockchain*. Il ne s'agit plus simplement de transfert d'actifs ou de la tenue d'un registre mais de rendre possible le développement d'organisations autonomes décentralisées. Dans chaque nœud du réseau Ethereum est installée une EVM (Ethereum Virtual Machine), dont l'objet est d'exécuter automatiquement les conditions et les termes de contrat, sans nécessiter d'intervention humaine, une fois lancés. Pour ne citer qu'un seul exemple, la mise en œuvre d'une organisation autonome décentralisée de transport entre particuliers permettrait à leurs utilisateurs – conducteurs et personnes souhaitant se déplacer – d'établir un contrat, sans passer par un tiers de confiance, et de garantir le paiement. De fait, à tous les services leaders du web, nouveaux intermédiaires des temps modernes, correspondent un ou plusieurs projets concurrents d'organisation autonome décentralisée. Ainsi, LaZooz ou Arcade City, services de transport entre particuliers, concurrenceraient Uber ou Blablacar. Storj rivaliserait dans les services de *cloud computing* avec DropBox. OpenBazaar deviendrait un site de petites annonces comme Craigslist. Slockit relie des objets physiques au réseau Ethereum afin d'interagir avec eux à travers des *smart contracts* : une serrure d'appartement connectée lui permettrait de concurrencer AirBnB.

Au-delà « d'uberiser » à leur tour les nouveaux intermédiaires du web, la diversité des applications mises en œuvre à travers ces organisations autonomes décentralisées semble sans limite. Dans le domaine de la logistique et de la traçabilité par exemple, la start-up Everledger utilise une *blockchain* pour combattre la fraude dans l'industrie du diamant. Des start-up ont déjà mis en place un système de vote, inviolable et infalsifiable. En France, laprimaire.org, initiative citoyenne organisée en dehors de tout parti politique traditionnel, a utilisé la plate-forme Ethereum pour organiser le vote de son candidat à l'élection présidentielle 2017. Ainsi a peut-être été inventé l'un des futurs outils politiques au service de la démocratie.

Dans les domaines de la production d'énergie solaire, de l'assurance ou de la gestion des droits d'auteur, l'utilisation de *smart contracts* apporterait une transparence et une confiance, qui font parfois défaut, tout en inventant des services d'un genre inédit.

La production d'énergie solaire – Le *Solarcoin* est une monnaie électronique adossée à la production d'énergie solaire, créée par la Fondation SolarCoin en 2014. C'est un programme de récompense, à l'instar des *miles* des compagnies aériennes ou ferroviaires, qui vise à encourager la production d'énergie solaire photovoltaïque à travers le monde. Les détenteurs d'installations photovoltaïques peuvent être rémunérés en monnaie électronique sur la base d'un *Solarcoin* pour un mégawattheure produit. Cette monnaie peut ensuite être utilisée entre les partenaires du projet, comme le français ekWateur (prononcer équateur), premier

fournisseur d'énergie français à accepter le paiement de sa consommation d'énergie en *Solarcoins*. L'utilisation d'une *blockchain* permet de certifier l'origine de la production d'énergie solaire. « *Les panneaux photovoltaïques des participants sont munis de capteurs qui envoient dans la blockchain les informations sur les quantités d'électrons produites : quand, par quel panneau photovoltaïque de quel membre du réseau, et ce dernier reçoit les SolarCoins correspondants. Le tout est consultable par tous les participants. Il n'y a pas de serveur central ni d'autorité régulatrice, car dès lors qu'une personne intègre ce réseau, la blockchain se télécharge sur son ordinateur* ». Autre partenaire de la Fondation SolarCoin, Lumo est une plate-forme d'épargne participative consacrée aux énergies renouvelables, dont l'objectif est de populariser les *SolarCoins* et d'en multiplier le nombre de détenteurs : « *tous ceux qui auront participé au financement d'une centrale solaire recevront des SolarCoins* », explique Alex Raguet, cofondateur de Lumo.

Les assurances – Les assureurs s'intéressent également aux *smart contracts*, notamment dans le domaine de l'assurance dite paramétrique ou indicielle. Encouragé par la Banque mondiale pour couvrir les agriculteurs des pays en voie de développement, ce type de contrats d'assurance intelligents, également disponible sur les marchés matures, consiste à enclencher une indemnisation dès lors qu'une anomalie météorologique est constatée. Par exemple, un agriculteur souscrit une assurance stipulant qu'une indemnisation sera versée après 30 jours de sécheresse. Lorsque l'événement se produit, l'agriculteur est automatiquement indemnisé, sans avoir à faire de déclaration auprès de son assureur.

Axa Assurances a récemment lancé une offre de *smart contract* sur la *blockchain* d'Ethereum, visant à indemniser les retards d'avion de plus de deux heures. La souscription de l'offre s'effectue en ligne quinze jours avant le départ. Le contrat est relié aux bases de données de Flightstats, recensant le trafic aérien mondial. Dès qu'un vol a deux heures de retard, l'indemnisation de l'assuré est déclenchée automatiquement, sans que l'assureur ait de déclaration de sinistre à traiter. Actuellement testée sur les vols transatlantiques directs entre l'aéroport Paris Charles-de-Gaulle et les États-Unis, l'offre a vocation à s'étendre au reste du monde dès 2018.

En avril 2017, Spotify a annoncé avoir racheté la start-up Mediachain Labs, qui déploie une solution de *smart contracts*

Les droits d'auteur – La gestion des droits d'auteur est un casse-tête pour l'industrie musicale, tout particulièrement aux États-Unis où les services de *streaming* rencontrent de plus en plus de succès. Le suédois Spotify, leader mondial, est fréquemment attaqué pour non-respect du versement des droits d'auteur. Au terme d'une longue bataille judiciaire aux États-Unis, l'entreprise a finalement dû reverser en mars 2016 plus de vingt millions de dollars à la National Music Publishers' Association (NMPA), selon laquelle plus de 25 % des écoutes sur Spotify étaient « sans licence ». En avril 2017, Spotify a annoncé avoir racheté la start-up Mediachain Labs, qui déploie une solution de *smart contracts* sur la *blockchain* d'Ethereum, afin de gérer finement les droits d'auteur attachés à un artiste. Le service rendrait transparente l'attribution d'une œuvre écoutée sur la plate-forme à tel ou tel artiste et déclencherait automatiquement le

paiement des droits d'auteur.

Également en avril 2017, trois des plus importantes sociétés de gestion de droits d'auteur au monde, la Sacem (Société des auteurs compositeurs et éditeurs de musique), l'Ascap (American Society for Composers Authors and Publishers) et PRS for Music (Performing Right Society for Music) ont annoncé travailler ensemble à la mise en œuvre d'un prototype de « *gestion partagée des informations relatives aux droits d'auteur* ». Ce prototype s'appuie sur la *blockchain open source* du consortium privé Hyperledger, chapeauté par la Fondation Linux, qui réunit vingt-sept entreprises, notamment IBM, SAP, Fujitsu, GE, Hitachi et Huawei. Le prototype de gestion des droits d'auteur reposera sur le projet Hyperledger Fabric, auquel IBM a grandement contribué, et qui est un concurrent des *smart contracts* proposés par Ethereum. Cette *blockchain* privée permettra d'associer à chaque morceau une signature contenant les informations liées aux droits d'auteur et, à terme, de créer un « *registre mondial des droits d'auteur* ».

Le 5 octobre 2009, date à laquelle est publié le premier taux de change *bitcoin*/dollar, un *bitcoin* vaut 0,001 dollar.

Le 21 octobre 2017, il vaut
6 100 dollars.

D'abord utilisée comme registre, la *blockchain* pourrait à terme être assortie de *smart contracts* utiles pour affecter très précisément les droits d'auteur à chaque œuvre. « *Un artiste pourra demander une rémunération pour une diffusion de sa musique à la radio, ne pas en demander aux boîtes de nuit et demander un prix moins élevé aux particuliers. Il pourrait aussi ne pas faire payer des sites de streaming qui ont une approche éthique. Enfin, la blockchain et les smart contracts permettent de différencier la répartition des droits : 5 % à tel musicien, 2 % à tel autre* » explique Clément Jeanneau, cofondateur de Blockchain France.

L'univers des *blockchains* laisse présager autant de perspectives qu'il relève déjà d'innombrables défis. La spéculation dont les cryptomonnaies font l'objet impressionne. Le 5 octobre 2009, date à laquelle est publié le premier taux de change *bitcoin*/dollar, un *bitcoin* vaut 0,001 dollar. Le 21 octobre 2017, il vaut 6 100 dollars. Inexistante en 2008, la capitalisation totale des cryptomonnaies avoisine, à l'heure où cet article est écrit, 173 milliards de dollars, et 4 milliards de dollars en valeur sont échangés quotidiennement sur les places de marché. À lui seul, le *bitcoin* représente la moitié de la valorisation totale des cryptomonnaies.

Breveter l'*open source*

Le fonctionnement de l'internet repose sur des logiciels et protocoles *open source*, comme TCP et IP. Le protocole Bitcoin est également *open source*. Cela n'empêche pas certains acteurs de déposer des demandes de brevets. Aux États-Unis, l'US Patent and Trademark Office (USPTO) a déjà enregistré 220 brevets entre 2013 et 2016. Les banques et les établissements financiers, comme Morgan Stanley, Accenture, Bank of America ou encore Goldman Sachs, comptent parmi les déposants les plus actifs. En 2016, l'Australien

Craig Wright s'est présenté comme étant le créateur du Bitcoin, sans toutefois en apporter la preuve irréfutable. Il a depuis constitué un portefeuille de demandes d'une centaine de brevets auprès de l'Office britannique de la propriété intellectuelle. Il semblerait que Craig Wright tente de breveter chaque élément de toute base de données distribuée. Il faudra attendre plusieurs années avant que ces brevets soient enregistrés ou rejetés.

Les ICO

Par nature accessibles à quiconque installe le logiciel Bitcoin sur son ordinateur ou son smartphone, les cryptomonnaies sont actuellement utilisées par des start-up pour lever des fonds, concurrençant les professionnels du capital-risque, au point de dépasser en valeur leur fonds d'amorçage. Si les introductions en Bourse, en anglais *Initial Public Offering (IPO)*, sont extrêmement réglementées et déterminent la cotation de titres de capital d'une entreprise sur un marché boursier, leur équivalent dans l'univers des cryptomonnaies, les *ICO (Initial Coin Offering)* ne le sont pas du tout. Une *ICO* correspond à une levée de fonds directement auprès des internautes qui échangent des *tokens*, actif numérique correspondant à un droit lié au service lancé, contre des cryptomonnaies, principalement des *bitcoins* et des *ethers*, soit l'équivalent de 14 millions de dollars en 2015, 222 millions en 2016 et plus de 1,2 milliard sur les six premiers mois de 2017, dont la moitié sur les 30 derniers jours de ce semestre, selon le bureau de recherche indépendant Autonomous. À lui seul, le projet Tezos, qui se place en concurrent de la *blockchain* d'Ethereum, a levé l'équivalent de 232 millions de dollars.

Piratage et arnaques

Les *smart contracts* développés sur Ethereum et les *ICO* ont fait l'objet d'importants détournements sans pour autant qu'une seule *blockchain* se soit déjà fait piratée. En juin 2016, une faille de sécurité dans une application construite sur Ethereum a provoqué le détournement de 50 millions de dollars ([voir La rem n°40, p.29](#)). Plusieurs *ICO* ont également fait l'objet de détournements, toujours spectaculaires, comme celle de CoinDash, le 17 juillet 2017. Un individu a piraté le site web de la société, le jour du lancement de l'*ICO* en remplaçant l'adresse Ethereum de CoinDash, à laquelle les intéressés étaient censés envoyer leur cryptomonnaie, par sa propre adresse Ethereum. Durant les trois premières minutes, le temps que les organisateurs se rendent compte du problème, 8 millions de dollars avaient été détournés.

De tels flux monétaires n'ont pas manqué d'alerter les institutions financières chargées de la régulation des monnaies légales. En effet, l'absence de cadre réglementaire a laissé foisonner bon nombre d'arnaques, mais aussi des levées de fonds phénoménales au profit de sociétés n'ayant parfois rien proposé d'autre qu'une présentation Powerpoint et une vidéo d'autopromotion. Pour ne citer qu'un exemple, le projet Eros.Vision, qui se présentait comme l'« Uber de la prostitution », a pu bénéficier d'une importante médiatisation, y compris en France *via* le trimestriel *Usbek & Rica* et la radio BFM, et lever l'équivalent de 19 millions de dollars avant de disparaître quelques jours plus tard.

Des régulations tâtonnantes

Les cryptomonnaies sont par nature transfrontalières. Si des pays se sont emparés de la question, comme la Chine, les États-Unis, le Japon, la Corée du Sud, ainsi que certains pays européens, il n'en reste pas moins qu'ils alternent entre, d'un côté, une interdiction pure et simple des *ICO* et des places de marché ouvertes au public, et de l'autre, une absence totale de régulation. Le 1^{er} avril 2017, le Japon a reconnu le *bitcoin* comme instrument de paiement, tout en régulant, *via* la Department and Financial Services Agency (FSA), les places de marché ouvertes au public sur lesquelles s'effectue le change de ces monnaies électroniques en monnaies nationales.

La dévaluation du yuan ayant provoqué d'importants transferts d'argent vers les cryptomonnaies, la Chine a purement et simplement interdit les *ICO* et les places de marché le 1^{er} octobre 2017, sûrement pour pouvoir mettre en œuvre une régulation à l'échelle du pays. La Corée du Sud a fait la même annonce. En mars 2017, aux États-Unis, la SEC (Securities and Exchange Commission) a refusé à l'agence Winklevoss Bitcoin Trust, établie à Wilmington en Californie, l'autorisation de créer un fonds indiciel coté en Bourse en expliquant que « *le marché du bitcoin n'est pas suffisamment régulé pour faire face aux fraudes et aux cyberattaques, dont il a déjà été victime plusieurs fois depuis sa création, et l'absence d'une Banque centrale ou d'institution de référence en fait une proie idéale pour les spéculateurs et la formation de bulles* ». En réponse à une question posée par la Commission des affaires économiques et monétaires du Parlement européen, le président de la Banque centrale européenne, Mario Draghi, a déclaré en septembre 2017 « *qu'il n'était pas dans son pouvoir d'interdire ou réguler le bitcoin* ».

Il est intéressant de voir combien l'invention de l'internet et celle du Bitcoin se ressemblent à
bien des égards

En France, le Trésor public va proposer à l'automne 2017 un projet d'ordonnance pour faciliter la transmission de certains titres financiers « *au moyen de la technologie blockchain* », afin de leur garantir un cadre réglementaire. Les minibons (anciennement appelés « bons de caisse », instrument financier entre le prêt et l'obligation) associés à une *blockchain* bénéficient déjà d'une assise légale en droit français, à la suite de l'ordonnance du 28 avril 2016 prise en application de la loi Macron du 6 août 2015. Chaque État va ainsi s'assurer d'apporter ou non, selon le type de *blockchain*, un cadre réglementaire ou, à l'inverse, mettre en place un dispositif d'interdiction de ces registres distribués.

De même qu'il était impossible d'imaginer le développement des services offerts par l'internet à la naissance du réseau, il serait vain de parier sur les usages et services à naître des *blockchains*. Il est cependant intéressant de voir combien l'invention de l'internet et celle du Bitcoin se ressemblent à bien des égards. Tous deux sont indissociables d'un contexte politique et social sous tension et d'une effervescence idéologique qui se réclame d'une doctrine de liberté absolue. À la naissance de l'internet dans les années 1960 et 1970 correspond le contexte politique de la guerre du Vietnam, de l'assassinat de John Fitzgerald

Kennedy et du développement des mouvements pacifistes américains, au cours desquels de nombreux universitaires et chercheurs vont contribuer à réfléchir à de nouvelles utopies dans un climat de plus en plus libertaire. Quant au Bitcoin, son contexte géopolitique est celui de la plus grande crise financière que le monde ait connu depuis 1929, marqué par une perte de confiance envers les banques, les institutions et les États, dont les plans de sauvetage puis de relance et enfin d'austérité ont fait exploser les dettes publiques et aggravé encore davantage la progression du chômage comme l'accroissement des inégalités dans les pays matures.

L'internet et le Bitcoin n'ont pas été créés *ex nihilo*, ils sont au contraire l'aboutissement de recherches et de tâtonnements aux filiations diverses. Pour l'internet, ce sont des intérêts parfois très éloignés entre l'Armée, les États, les entrepreneurs et les chercheurs. Le réseau de réseaux est le fruit d'un assemblage d'innovations disparates, comme celle du Français Louis Pouzin qui, en inventant en France Clyclade, premier réseau à commutation de paquets, va permettre quelques années plus tard à Vinton Cerf de mettre au point les protocoles TCP/IP, au cœur du fonctionnement de l'internet. De la même manière, le Bitcoin s'inspire des travaux de cryptographie proposés dans les années 1990 par Haber et Stornetta, ou encore de Nick Szabo, informaticien, juriste et cryptographe, qui a proposé dès 2005 un système d'échange monétaire basé sur la validation par la preuve de travail, dont s'est probablement inspiré le [ou les] dénommé(s) Satoshi Nakamoto.

Il n'aura fallu que trente ans pour transformer profondément la pensée libertarienne de l'internet

Enfin, un autre dénominateur commun entre l'internet et les registres distribués de type *blockchain* repose sur leur architecture, tous deux ayant des protocoles *open source* et fonctionnant en pair-à-pair. Qui aurait pu imaginer le développement du réseau internet et de ses services comme le web, le *mail* ou le pair-à-pair, puis des plates-formes comme Facebook, Google ou Amazon. Il n'aura fallu que trente ans pour transformer profondément la pensée libertarienne de l'internet, et pour que le rêve initial de Norbert Wiener, J.C.R. Licklider, Robert Taylor et bien d'autres – créer un outil citoyen de participation active et de créativité décuplée par l'interaction – engendre dans le même temps une surveillance de masse où les données personnelles sont devenues le pétrole du XXI^e siècle. Et gare à ceux qui, vingt ans plus tard, tenteront de s'en réclamer encore, comme Aaron Swartz qui lutta pour « *la liberté d'internet et pour faire de la connaissance une donnée aussi largement et gratuitement accessible* ³ ». Il n'aura même pas fallu dix ans pour que cette même idéologie, au fondement du Bitcoin, soit reprise par le secteur financier, qu'une avalanche de dépôts de brevets prévoit d'en parasiter le développement à moyen terme, et que de nombreux États tentent de réguler les places de marché grand public. Pour autant, l'idéologie de rupture, dont sont porteuses les bases de données distribuées de type *blockchain*, s'inscrit dans des initiatives bien au-delà du secteur financier et du transfert d'actifs, par exemple dans les domaines de la traçabilité alimentaire, de l'industrie pharmaceutique, de la distribution d'énergie, de la certification d'identité et potentiellement, dans tous les domaines susceptibles de passer d'une autorité de confiance institutionnelle à une confiance distribuée à travers un réseau de pairs.

Il n'aura même pas fallu dix ans pour que cette même idéologie, au fondement du Bitcoin, soit reprise par le secteur financier

Les *blockchains* vont-elles « uberiser » Uber ? Permettront-elles au contraire de corriger les excès de l'uberisation ? Se substitueront-elles à l'organisation à la fois centralisée et pyramidale qui régit nos institutions ? Insuffleront-elles la volonté politique d'introduire de « l'horizontalité » comme instrument pour « faire appliquer les règles de droit là où la loi n'arrive pas, à elle seule, à protéger les droits fondamentaux des citoyens »³, mais également, pour assurer une transparence dans des chaînes de valeur complexes et souvent opaques parce qu'humaines et motivées par des intérêts parfois divergents ? À n'en pas douter, des méta-organisations inédites, décentralisées et autonomes, sont probablement en gestation parmi le millier d'initiatives dans le monde s'appuyant sur les bases de données distribuées de type *blockchain*. Et nul ne sait ce qu'il adviendra si ce n'est que, dorénavant, la boîte de Pandore est ouverte.

¹ Antoine-Laurent de Lavoisier.

² *Bitcoin, la monnaie acéphale*, Adli Takkal Bataille et Jacques Favier, CNRS Éditions, 2017.

³ *Abécédaire des architectures distribuées*, Cécile Méadel, Francesca Musiani (coord.), Presses des Mines, 2015.

Sources :

- *Les télécommunications entre bien public et marchandises*, Laurent Chemla, Éditions Charles LéopoldMayer, 2005.
- « La Blockchain, au-delà du Bitcoin », Goofy, framablog.org, 30 janvier 2016.
- « Introduction (non technique) à la « blockchain » », LinkedIn.com, Romain Roupheal, 1^{er} avril 2016.
- « Lumo intègre le projet blockchain ElectriCChain, distributeur de la monnaie « SolarCoin » », Delphine Sibony, Lumo-france.com, 2 juin 2016.
- « La Blockchain décryptée, les clefs d'une révolution », Blockchain France, Netexplo Observatory, mai 2016.
- « Quand le crowdfunding s'allie à l'énergie solaire et à la blockchain », Dominique Pialot, Latribune.fr, 9 juin 2016.
- « La Blockchain, ou la confiance distribuée », Yves Caseau, Serge Soudoplatoff, Fondation pour l'innovation politique, juin 2016.
- « Vote électronique : la blockchain à la rescousse ? », Louis Adam, ZDNet.fr, 22 mars 2017.
- « Pourquoi l'industrie musicale a besoin de la blockchain », Paul Loubière, Challenges.fr, 14 avril 2017.
- « La Blockchain au secours des droits musicaux », T.B., *Ecran total*, n° 1144, 8 mai 2017.
- « #Token Mania », Lex Sokolin, Autonomous Next, juillet 2017.
- « Assurance : les premières offres fondées sur la « blockchain » font leur apparition », Laurent

Thevenin, *Les Echos*, 19 septembre 2017.

- « Comprendre le Bitcoin et la Blockchain », Mathieu Nebra, Openclassrooms.com, consulté le 21 octobre 2017.
- « Comprendre Bitcoin », bitcoin.fr/faq/, consulté le 23 octobre 2017.

Categorie

1. Articles & chroniques

date créée

3 janvier 2018

Auteur

jacquesandrefines