l'École de Paris du management

Tout ce que vous devriez savoir sur les vrais usages de la *blockchain*

par

Thierry Rayna
Professeur de management de l'innovation à l'École polytechnique,
chercheur au laboratoire i3-CRG (UMR CNRS 9217)

En bref

Face à l'insondable mystère que sont pour lui les chaînes de blocs, le profane s'interroge. Qu'est-ce donc là que cette diablerie, concoctée par un Docteur Nakamoto, dont on débat de l'existence même, et qui déchaîne les passions des initiés ? Et quelle est cette technologie démiurgique dont on prétend qu'elle va renvoyer le système bancaire aux oubliettes, révolutionner les échanges et modifier les relations sociales ? La première vague d'exaltation passée, il est grand temps de dédramatiser l'objet. Loin des promesses de ses débuts, le système bitcoin dévoile ses faiblesses, son coût exorbitant et sa lourdeur, qui obèrent son utilité, en dehors de quelques cas précis. Ne méritant ni l'excès d'honneurs de ses débuts ni l'indignité à laquelle le vouent ses contempteurs, la *blockchain* requiert que l'on comprenne ses principes afin de mieux cerner ses limites et d'en maîtriser les enjeux et les risques.

Compte rendu rédigé par Pascal Lefebvre

Séminaire organisé grâce aux parrains de l'École de Paris du management :

Algoé [1] • Carewan [1] • Conseil régional d'Île-de-France • Danone • EDF • Else & Bang • ENGIE • FABERNOVEL • Fondation Roger Godino • Groupe BPCE • Groupe Caisse des Dépôts • Groupe OCP • GRTgaz • HRA Pharma [2] • IdVectoR [2] • IPAG Business School • L'Oréal • La Fabrique de l'industrie • MINES ParisTech • RATP • Renault-Nissan Consulting • SNCF • Thales • UIMM • Ylios [1]

1. pour le séminaire Vie des affaires
2. pour le séminaire Management de l'innovation

Exposé de Thierry Rayna

Je suis professeur à l'École polytechnique et chercheur au sein du Centre de recherche en gestion (CRG), désormais intégré à l'Institut interdisciplinaire de l'innovation (i3). Auparavant, j'ai passé l'essentiel de ma carrière au Royaume-Uni, notamment à l'université de Londres, où je suis toujours *research fellow*. Je suis également rédacteur en chef associé de la revue *International Journal of Manufacturing Technology and Management*.

Mes thèmes de recherche ont toujours traité des technologies numériques, dans la musique et le cinéma pour commencer, puis avec, entre autres, l'impression 3D, les médias sociaux et, plus récemment, l'intelligence artificielle et la *blockchain*. Ce qui m'intéresse, c'est de comprendre comment toutes ces technologies numériques changent le comportement des individus en leur donnant des moyens de création, de diffusion ou de reproduction qui leur permettent de cocréer et font d'eux des innovateurs et des *prosumers*[1]. Comme elles touchent également les groupes, on a vu apparaître des communautés d'innovation, de l'économie collaborative, de l'*open innovation* sociale, etc. Tout cela implique que les entreprises doivent elles aussi s'adapter, ce qui contraint à changer les modèles d'affaires et, dans certains cas, les politiques liées à la propriété intellectuelle. Une partie de ma recherche porte ainsi sur les écosystèmes d'innovation et l'évolution des stratégies des firmes.

Qu'est-ce que la *blockchain* ?

Il semble que ce soit désormais le bon moment pour parler de la *blockchain*. En effet, après une période d'attentes démesurées à l'endroit de cette technologie, semble s'amorcer une phase de déception. Pour comprendre cet excès d'enthousiasme et cette déception qui l'a suivi, et pour anticiper ce que va être, à long terme, l'impact de cette technologie, je vais me faire l'avocat du diable, au risque de paraître extrêmement sceptique.

En 2008, Takishi Nakamoto – un individu ou un groupe d'individus, son existence n'étant pas avérée –, diffuse un *white paper*[2] décrivant une nouvelle technologie. Dans le contexte très particulier de la crise qui éclate alors et de grande défiance à l'égard des institutions financières, la question sous-jacente à cette technologie est de savoir comment créer une monnaie qui soit un actif d'échange décentralisé sans aucun intermédiaire de confiance. Cela implique que, lors d'un échange, chacun puisse savoir ce qui a été échangé et qui possède quoi. Très classiquement, cela s'appelle un registre de compte partagé, un *ledger* – on ne parle pas encore, à ce stade, de *blockchain*.

Mais nous sommes ici dans une perspective très particulière, celle où aucune autorité centrale, telle une banque, n'atteste de la véracité des informations contenues dans ce *ledger*. L'idée est de remplacer la confiance que l'on accorde d'ordinaire à cette autorité par de la cryptographie. Dès lors, l'environnement est très différent de celui du système bancaire, qui garantit les cartes de paiement de ses clients. Dans le cas de cette *cryptocurrency*, le client utilise une application et, en lieu et place des banques, c'est un protocole informatique, le bitcoin, qui garantit les transactions. Le bitcoin est donc une cryptomonnaie, ou plutôt un cryptoactif, qui utilise la technologie dite de *blockchain*. Ce n'est qu'un exemple parmi d'autres de cryptoactif, même si c'est le premier et le plus connu.

Comme ce protocole ne doit être validé par aucune autorité centrale, il faut trouver un moyen de distribuer le registre de compte entre tous les utilisateurs et, à cette fin, on utilise deux types de technologies, qui existaient

1. *Prosumer* est un terme anglo-saxon signifiant consommateur et professionnel. Les termes employés en France sont *prosommateur* et *prosommation*.

2. Un *white paper* est une publication destinée à présenter des informations concises sur un sujet complexe tout en présentant la philosophie de l'auteur sur ce sujet.

elles aussi bien avant la création de la *blockchain*. La première est un chiffrement classique de la signature électronique et la seconde, des fonctions de "hachage" cryptographique[3].

Grâce à cette signature numérique, on sera en mesure de vérifier le contenu du *ledger,* car, pour que tout fonctionne correctement, il faut évidemment garder trace de qui a payé quoi et à qui, et vérifier périodiquement les transactions réalisées par chacun des acteurs pour, éventuellement, égaliser les comptes au moyen d'une "vraie" monnaie.

Pour apporter toutes les vertus prêtées à la *blockchain*, il faut impérativement combiner la totalité de ces dispositifs. Si l'un de ces dispositifs manque, on peut sûrement encore appeler cela *blockchain*, mais les vertus d'invulnérabilité et de désintermédiation avec les banques disparaissent.

Bob et Alice font du business…

Pour définir ce protocole, deux choses sont importantes.

La première est que tout utilisateur peut ajouter des lignes à ce carnet de compte, bien que toutes ne soient pas forcément légitimes. Imaginons Bob et Alice, puis Charlie. Si Bob inscrit indûment qu'Alice lui a payé 100 dollars, Alice contestera à juste titre la transaction. Il faut donc s'assurer de la véracité de cette opération et, pour cela, chaque personne ajoutant une ligne va devoir la signer, certifiant ainsi que l'opération est valide, de la même façon qu'une banque s'assure qu'un chèque est bien signé ou que le bon code PIN valide un paiement par carte. Or, tout comme une signature manuscrite peut-être imitée, une signature numérique peut facilement être usurpée.

En second lieu, il va falloir utiliser un système de chiffrage basé sur deux éléments, une clé publique et une clé privée, toutes deux attribuées à chaque utilisateur. La clé publique sera ouverte à tous et permettra à chacun de connaître l'identité de l'auteur d'un message. La clé privée sera secrète et permettra à son seul possesseur de générer sa signature pour chacune des opérations qu'il réalisera sur le carnet de compte. Contrairement à une signature habituelle, toujours la même quel que soit le message, celle-ci aura l'avantage d'être différente d'un message à l'autre. Pour cela, la signature numérique sera constituée d'une fonction qui associe le message et la clé secrète de l'émetteur. Une seconde fonction, dont chaque utilisateur dispose, va ensuite permettre à celui qui le reçoit de vérifier si le message est authentique en associant la clé publique à la signature de l'émetteur.

C'est cette combinaison de technologies de chiffrement qui est à la base de la sécurisation de ce système. Pour garantir l'authenticité de l'identification, on utilise dans cette fonction un chiffrage à 256 bits. Pour la signature unique d'un message et une clé publique d'émetteur donnée, le nombre de combinaisons possibles est de 2^{256}, ce qui rend tout "crackage" hautement improbable.

De plus, le processus est non réversible, ce qui signifie qu'à partir de la clé publique et de la signature du message reçu, il est impossible de retrouver, pour l'utiliser à des fins malveillantes, la clé privée de l'émetteur. Après avoir vérifié la signature du message reçu grâce à la clé publique en votre possession et dès lors que la fonction renvoie "VRAI", vous pouvez être absolument certain que le signataire de ce message est bien le titulaire de la clé privée qui a servi à l'émettre.

Concrètement, si Bob a indûment écrit dans le carnet de compte qu'Alice lui a payé 100 dollars, le message sera invalidé, car Bob ne sera pas en mesure de prouver que c'est bien Alice et non lui qui a écrit ce message. De plus, Bob ne pourra pas copier la signature d'un message valide antérieur pour s'en resservir, car, dès lors que le moindre changement lui est apporté, la signature du nouveau message sera complètement différente, et ce, de manière complètement imprédictible. Lorsque, en fin de mois, on règle les échanges, seules les transactions qui auront été signées seront considérées comme valables, les autres étant ignorées.

3. Une fonction de hachage, ou *hash function*, cryptographique est une fonction dont la propriété essentielle est qu'elle est impossible à inverser.

… et Charlie fait des dettes !

Pendant ce temps, Charlie, quoiqu'impécunieux, a contracté quantité de dettes en émettant des paiements parfaitement signés et donc valides, équivalents en cela à des chèques en bois. Mais, à la fin du mois, quand il s'agit de les régler, il a disparu ! Manifestement, le protocole manque donc d'une fonctionnalité pour éviter ce genre de désagrément. Un tel scénario ne peut cependant se produire que si le règlement se fait à terme et non au fil de l'eau. Dès lors que cette condition disparaît, le risque en fait autant.

Pour que le système fonctionne, on va donc l'alimenter par un apport de monnaie en amont. Chacun provisionnera son compte en début de mois et, le protocole n'autorisant aucune opération à découvert, Charlie ne pourra pas dépenser plus de bitcoins qu'il n'en a. Désormais, à chaque fois que Charlie entrera une transaction, tout le monde pourra vérifier les montants en jeu et sa solvabilité. S'il n'a pas de quoi honorer sa transaction, celle-ci ne sera pas prise en compte, tout comme si elle n'avait jamais été signée.

Dans un *ledger* classique, les transactions se font en dollars. Or, les bitcoins ne sont pas des dollars. Si tout le monde accepte des paiements en bitcoins, cela crée de fait une nouvelle unité de compte indépendante d'autres monnaies. Alice pourra alors donner des dollars à Bob qui, en retour, lui donnera des bitcoins. Cela génère une nouvelle difficulté en instaurant des taux de change fluctuant entre le bitcoin et les autres monnaies.

Au final, le bitcoin n'est donc qu'un carnet de compte, un historique de transactions, et c'est ce qui en fait la valeur.

La preuve de travail

Jusqu'ici, nous avons considéré que cette cryptomonnaie était centralisée, ce qui pose problème. Où est situé ce carnet de compte ? qui le contrôle ? et qu'est-ce qui empêche le contrôleur de modifier à sa guise telle ou telle opération ? Il faudrait que l'on ait confiance en cette autorité centralisatrice, ce qui, en l'occurrence ne peut être le cas, cette autorité n'existant pas par hypothèse. Comment faire ?

Il faudrait que chacun dispose d'une copie du carnet de compte. Dès lors, la difficulté disparaîtrait. Or, comment être sûr que les transactions sont envoyées à tout le monde ? et que les carnets envoyés sont bien tous identiques ? Face à des problèmes aussi triviaux que des interruptions de communication ou à de gros volumes de transactions n'arrivant pas dans le même ordre, la mise en œuvre serait proprement impossible. L'idée d'une décentralisation paraît donc absurde et irréaliste.

Une solution existe toutefois. Lorsque l'on constate des conflits ou des dissonances entre différents carnets de compte reçus, on va faire confiance à celui qui comporte le plus de travail "computationnel". Pour cela, on va faire en sorte que la quantité de calculs informatiques nécessaires pour forger ce carnet de compte soit impossible à reproduire, afin d'écarter tout risque de fraude, le tout à l'aide des fonctions de hachage déjà évoquées. C'est ce que l'on appelle la preuve de travail (en anglais *proof of work*, ou PoW), qui ne peut être obtenue que par la réalisation d'une tâche fortement consommatrice en puissance de calcul, mais dont le résultat est facile à vérifier. Le travail doit donc être difficilement réalisable pour le demandeur tout en étant facilement vérifiable pour un tiers. C'est la base du bitcoin et, dans le monde de la *blockchain*, cette notion est incontournable.

Pour établir la preuve de travail, les fonctions de hachage vont d'abord produire, à partir d'un message particulier, un output chiffré par SHA-256[4] et d'apparence complétement aléatoire. Si le moindre élément du message originel est modifié, du fait de ces fonctions, l'output sera totalement différent. Ce processus est entièrement cryptographique et ne peut être réversible, rendant impossible de retrouver le message en partant de l'output ainsi généré.

4. Le hachage SHA-256 est le standard du gouvernement fédéral des États-Unis faisant correspondre une empreinte de 64 caractères hexadécimaux à une donnée initiale.

La preuve de travail va consister à imposer à l'émetteur, toujours en utilisant SHA-256, de coder sous forme de chaînes hexadécimales[5] un grand nombre de variations du message originel en ajoutant un nombre aléatoire au début de chacune des milliers de chaînes ainsi obtenues jusqu'à obtenir un numéro spécial comportant, par exemple, 30 zéros. Compte tenu de la quantité extrêmement élevée de chaînes ainsi produites, la probabilité de retrouver cette clé de chiffrement est mathématiquement impossible. Pour le récepteur, il n'y a donc pas d'autre solution que de générer aléatoirement des clés et de les essayer ensuite une par une. Cette vérification se fera en identifiant, parmi toutes les autres, la chaîne à laquelle ce numéro spécial est attaché. Une fois le bon hachage retrouvé, le message initial pourra être récupéré.

Ce processus dépend en fait de la puissance de traitement numérique disponible. Grosso modo, dans le cas du bitcoin, il faut avoir effectué environ un milliard d'opérations en moyenne avant d'obtenir cette preuve de travail. L'idée de base du bitcoin est que cette recherche doit nécessiter une telle capacité de calcul qu'un individu ne pourra jamais y parvenir seul.

La *blockchain*

Nous avons donc un cahier de compte, des signatures, des transactions qui y sont ajoutées. La version de ce cahier à laquelle nous ferons confiance sera celle qui aura nécessité le plus de travail. Pour éviter toute manipulation frauduleuse, les transactions sont ensuite regroupées en blocs de transactions, chaînés les uns aux autres, chaque bloc comportant une preuve de travail spécifique qui lui est attachée et dont la valeur dépend notamment du hachage du bloc précédent. Chacun peut alors vérifier en confiance si un bloc comporte le nombre spécial. Si oui, il sera validé, sinon, il sera ignoré. C'est pour cela que l'on ne parle plus de *ledger*, mais de *blockchain* ou de chaîne de blocs.

Ce chaînage a pour conséquence que tout changement sur un bloc invalide sa preuve de travail intégrée au bloc suivant, ce qui invalide donc l'ensemble de la chaîne en aval. Dès lors, cela contraint à recalculer une autre chaîne, c'est-à-dire à réitérer le milliard d'opérations à chaque fois qu'une chaîne comporte un bloc invalide jusqu'à en trouver une dont tous les blocs seront valides. Par conséquent, non seulement on ne peut rien changer dans un bloc, sauf à avoir une puissance de calcul énorme, mais on ne peut également pas intervertir des blocs, sauf à tout réécrire. L'historique étant à la disposition de tous, chacun pourrait théoriquement le modifier, mais cela s'avèrerait infiniment coûteux.

Il est donc important de bien distinguer le bitcoin, qui est un cryptoactif, du protocole sur lequel il est basé, qui s'appelle la *blockchain*. Par ailleurs, les cryptomonnaies ne sont pas les seules applications de la technologie *blockchain*, comme nous le verrons plus loin.

L'or des mineurs

Des individus vont effectuer des transactions tandis que d'autres, les *block creators*, vont écouter ces transactions, les grouper au sein d'un bloc et essayer de trouver ce nombre spécial commençant par 30 zéros ou plus[6]. Une fois ce nombre trouvé, le *block creator* gagnant va le diffuser à chaque participant qui en prendra ainsi connaissance. Cela lui aura demandé beaucoup de temps de calcul, mais, en faisant cela et par exception, il va pouvoir ajouter une ligne dans le carnet de compte qui créera une certaine quantité de monnaie dans le système. Celle-ci sera imputée sur son compte personnel. Dans le cas du bitcoin, afin de limiter la création de monnaie, le montant de cette récompense diminue avec le temps et disparaîtra totalement en 2025.

Ces créateurs de blocs sont couramment appelés des *mineurs*, puisqu'ils vont chercher de l'or au tréfonds des blocs. Ces mineurs sont en concurrence entre eux, tous cherchant simultanément à trouver ce nombre spécial

5. La plupart des ordinateurs peuvent atteindre au moins quatre millions de hachages par seconde (H/s), mais il existe des systèmes beaucoup plus complexes, qui requièrent des preuves de travail pouvant dépasser 2 milliards de GH/s.

6. Ce nombre évolue afin de faire en sorte qu'un nouveau bloc soit "miné" en moyenne toutes les dix minutes.

dans ce qui ressemble à une loterie, afin de gagner la récompense[7]. Or, parmi les 2^{256} nombres potentiellement générés, il en existe de nombreux commençant par les 30 zéros de notre exemple. Seul gagnera alors le premier mineur à trouver l'un de ces nombres, grâce au milliard d'opérations qu'il aura effectuées, tous les autres ayant travaillé pour rien[8].

Le numéro en lui-même n'a aucune importance, il aurait été différent s'il avait été trouvé par un autre mineur. La preuve de travail est seulement là pour assurer que cet énorme travail a bien été fourni. Le nombre de zéros sera alors déterminé par la puissance de calcul en présence et ajusté en conséquence avec la volonté qu'un bloc soit créé toutes les dix minutes dans le cas du bitcoin. Néanmoins, 2 400 transactions traitées toutes les dix minutes, c'est très peu en comparaison des 1 700 par seconde traitées par VISA ! Cette lenteur est justifiée par des questions de sécurité, mais a été la cause de la séparation entre le bitcoin et d'autres cryptomonnaies.

En cas de conflit, on fera arbitrairement confiance à la chaîne de blocs la plus longue, c'est-à-dire au registre apportant la plus grande preuve de travail computationnel. De ce fait, cette chaîne sera celle qui aura le moins de risques d'avoir été falsifiée. Lorsque deux chaînes auront la même longueur, on attendra simplement qu'émerge une nouvelle chaîne plus longue. La confiance dans une quelconque autorité centrale est donc désormais bien remplacée par la confiance dans la puissance du travail computationnel.

Comment falsifier une transaction ? Imaginons qu'Alice veuille faire croire à Bob qu'elle lui a versé 100 bitcoins, sans que les autres aient connaissance de cette transaction et puissent donc vérifier sa réalité. Cela permettrait à Alice de dépenser ces mêmes 100 bitcoins à nouveau. À cette fin, elle lui enverrait une chaîne avec un nouveau bloc qui contiendrait cette transaction. Or, d'autres mineurs travaillent parallèlement et diffusent des blocs également valides, mais ne contenant pas la transaction en question ! Bob entend donc deux sons de cloche différents.

Ainsi, pour qu'Alice soit en mesure de gruger Bob, il faudrait non seulement qu'elle soit capable de fournir à Bob un bloc valide, mais également une chaîne successive de blocs valides comprenant un bloc dans lequel figure la transaction en question. Or, la concurrence entre mineurs et le fardeau de la preuve de travail rend ceci tout simplement impossible.

Malgré cette forte compétition et du fait qu'il s'agit d'une loterie, il se pourrait cependant qu'Alice soit, sur un coup de chance, la première capable de générer ce bloc. Un deuxième coup de chance, hautement improbable, pourrait à la rigueur intervenir en faveur d'Alice qui générerait alors un second bloc. Cependant, les probabilités font qu'il y aura toujours un moment où Bob recevra une chaîne plus longue que celle d'Alice, tous les mineurs réunis fournissant obligatoirement plus de travail computationnel qu'elle seule, sauf à ce qu'elle possède plus de 50 % de la capacité de calcul globale. La chaîne d'Alice, qui ne peut compter que sur sa chance pour générer des blocs falsifiés sur toute sa longueur, sera donc plus courte qu'une autre qui ne comportera, quant à elle, aucune trace de la transaction prétendument effectuée au profit de Bob, qui se rendra alors compte qu'Alice ne l'a, en réalité, jamais payé.

Les mythes de la *blockchain*

La *blockchain* n'est donc qu'un cahier de compte, certes spécial, car décentralisé. D'abord mise en œuvre pour les cryptomonnaies, on s'est rapidement rendu compte qu'elle pouvait s'avérer utile dans d'autres domaines : actifs financiers, contrats, documents d'identité, dossiers médicaux, votes, etc. Cet engouement a également donné lieu a beaucoup de mythes.

7. Au delà de la récompense, les mineurs peuvent par ailleurs toucher un "pourboire" offert par des utilisateurs pressés de voir leur transaction validée. Il s'agit de fait de frais de transactions.

8. En pratique, dû à la nature décentralisée du protocole, il se peut que plusieurs mineurs "gagnent" et diffusent concurremment un bloc valide. Cependant, la chaîne ne comprendra au final qu'un seul de ces blocs concurrents ; un seul mineur aura donc gagné, et être le premier à diffuser un bloc valide augmente la probabilité d'être inclus dans la chaîne la plus longue, qui sera celle considérée comme valide.

La blockchain *est une innovation*

Le premier de ces mythes, particulièrement durable, est que la *blockchain* serait quelque chose de nouveau. En fait, il n'y a rien en elle de véritablement nouveau puisqu'elle résulte de la combinaison de trois champs informatiques lui préexistant de longue date : les scripts de transactions, les questions de consensus et celles des réseaux. Ces trois types de protocoles ont été réunis afin d'atteindre un objectif particulier, celui de réaliser des échanges d'actifs de manière décentralisée. Lorsque j'étais en poste à Cambridge, le laboratoire d'informatique avec lequel je travaillais étudiait déjà la question de la sécurité de réseaux décentralisés. Cependant, à la place d'un carnet de compte, ils ne s'intéressaient alors qu'à la possibilité de censure de leurs contenus, par exemple du fait d'un État totalitaire, et à la façon de rendre inattaquables les informations. Il m'était alors apparu que sécuriser un réseau informatique décentralisé était extrêmement coûteux.

Les chercheurs s'étaient également aperçus que 97,7 % des ressources étaient utilisées pour simplement vérifier que les nœuds du réseau étaient bien les nœuds du réseau, ce qui rendait tout le processus absolument inefficace ! Pour l'économiste que je suis, il apparaissait donc parfaitement inutile de sécuriser le réseau de manière totale si personne n'avait d'incitation forte à corrompre ou à attaquer le réseau. Nous avions alors défini le concept de *réseau pair à pair suffisamment sécurisé*, dans lequel le niveau de sécurité (et donc la quantité de ressources informatiques utilisées) évolue avec la valeur du réseau (et donc la probabilité d'attaque), principe repris dans la preuve de travail.

La blockchain *est une chaîne*

Le deuxième mythe est que la *blockchain* est une chaîne, alors que c'est en réalité un arbre, ce qui n'a rien d'anecdotique. Dans les processus habituels de consensus en informatique, on sait qui représente les nœuds du réseau et l'on peut s'accorder sur une chaîne. Dans le cas de la *blockchain*, on ne peut que constater qu'une chaîne est la plus longue au sein d'une arborescence à l'instant T, sachant qu'à l'instant T+1, une configuration complètement différente peut émerger, bouleversant les antécédents.

Cela implique que de nombreuses attaques peuvent être subies par le réseau, un bloc peu exploité pouvant être repéré par un acteur malveillant qui le travaillera afin de créer une alternative à la chaîne la plus longue obtenue jusque-là. Cette incapacité à figer l'historique de façon définitive est l'une des faiblesses de ce système. Cette forme très spéciale de consensus, dit de Nakamoto, permet de vérifier que tous les blocs sont corrects, mais, au bout d'un moment, il faut rapidement qu'une convergence apparaisse. La relation entre vitesse du réseau et capacité de calcul est alors essentielle et la preuve de travail est donc nécessaire pour établir ce consensus et réduire la probabilité d'attaque

La blockchain *est peu coûteuse*

Le troisième mythe affirmait, lorsqu'elle est apparue, que la *blockchain* était très efficace et peu coûteuse. Les banques comme Western Union allaient disparaître, les transferts d'argent se réduisant à un jeu d'enfant quasiment gratuit.

Pour éclairer la question du coût réel de la *blockchain*, penchons-nous sur la question suivante : quel est le point commun entre un réfrigérateur, une maison et le Danemark ? Tous trois permettent de parler du coût du bitcoin, car une seule transaction en bitcoin consomme plus de 100 kilowattheures, c'est-à-dire de quoi faire fonctionner le premier pendant un an et la seconde pendant deux jours. Ce coût transactionnel est donc plus de mille fois plus élevé que celui d'une carte de crédit. Quant au Danemark, il a été estimé que la consommation énergétique du système bitcoin pour l'année 2018 avait été équivalente à celle de ce pays sur la même période. La cause en est la preuve de travail pour laquelle des milliers de personnes effectuent simultanément des calculs alors qu'un seul sera finalement utile.

Ce système est donc très coûteux en ressources. Par ailleurs, actuellement, il en coûte 5 dollars US, frais compris, pour passer une transaction en bitcoin et cela prend du temps puisqu'il faut attendre au minimum dix minutes pour qu'une opération soit validée. Lors de périodes de pic, ce délai a pu monter jusqu'à trois jours.

Peut-on alors remplacer la preuve de travail ? Certains le prétendent, mais les alternatives qu'ils proposent, *proof of stake, proof of authority*, requièrent davantage de confiance ou un réseau plus centralisé, voire les deux à la fois. La preuve de travail s'avère donc être incontournable pour sécuriser un réseau décentralisé d'où la confiance est exclue.

La blockchain *est sécurisée*

On prétend également que la *blockchain* est sécurisée. C'est vrai dès lors que personne ne contrôle plus de 50 % de la puissance de calcul. Cela veut dire que, pour les petits réseaux, elle ne l'est pas.

Alors, quand une banque veut déployer une *blockchain*, il faut commencer par déterminer le nombre de nœuds que comporte son réseau, puis estimer si, quelque part dans le monde, quelqu'un de mal intentionné ne dispose pas d'un supercalculateur ou d'une armée de *bots* capables de le pirater. Il faut également que cette puissance de calcul soit distribuée harmonieusement en évitant qu'un acteur ne dispose d'une très grosse puissance de calcul qui l'avantagerait par rapport au reste des mineurs moins bien équipés.

On peut avoir confiance dans la blockchain

Ce cinquième mythe n'est vérifié qu'à la condition que la *blockchain* soit sûre, ce qui renvoie aux conditions précédemment vues concernant la taille, la décentralisation, la preuve de travail, etc. Dans ce cas, on peut effectivement avoir confiance dans la *blockchain*, mais uniquement pour les opérations liées à celle-ci. Ce qui se passe sur la *blockchain* reste sur la *blockchain* : les transactions sont sûres et validées, certes, mais tout ce qui se passe en dehors ne l'est pas. Ainsi, si au lieu de vrai dollars Alice a donné à Bob de faux billets en échange de ses bitcoins, la transaction ayant été validée au sein de la *blockchain*, Bob ne pourra jamais la remettre en question quand il s'apercevra de la supercherie.

La blockchain *est décentralisée*

Ce mythe est la raison d'être de la *blockchain*. En réalité, si l'on regarde qui "mine", on se rend compte que le travail est extrêmement mal distribué et, dans le cas du bitcoin, qu'une forte concentration se fait au profit de quelques acteurs majeurs, dont la plupart sont chinois, ce qui laisse planer le doute sur leur indépendance politique. Par ailleurs, une étude du Crédit Suisse nous indique que 4 % des adresses bitcoin possèdent 97 % des bitcoins.

De fait, le système bitcoin n'est pas décentralisé, car il repose entièrement sur des fermes de calcul basées en Chine. Ce pays disposerait ainsi d'un moyen de pression géopolitique dissuasif si le bitcoin venait à se généraliser dans le système économique mondial. Cette concentration est intrinsèque à la preuve de travail et ne peut être évitée. Puisqu'elle requiert de plus en plus de travail, il faut donc concentrer la puissance de calcul.

Au départ, le bitcoin a été concurrencé par nombre d'autres cryptomonnaies. Néanmoins, face à son succès, quantité de *blockchains* se sont adossées à lui, lui conférant de ce fait une situation largement dominante et accentuant ainsi le phénomène de concentration. Si vous êtes mal intentionné et que vous en avez les moyens, vous pouvez donc provoquer non seulement le crash du bitcoin, mais également celui de tous les marchés qui lui sont liés.

À quoi sert la *blockchain* ?

La *blockchain* va-t-elle tuer les banques ? L'enthousiasme initial sur ce point s'est très vite heurté à la limite liée aux coûts évoquée précédemment.

La seconde limite, fondamentale en informatique, tient à ce qu'il y a entre l'écran et la chaise. C'est une clé privée en 64 bits qui donne accès au système bitcoin, mais, sauf à avoir une mémoire exceptionnelle, personne ne peut retenir un mot de passe d'une cinquantaine d'éléments. Les usagers ne vont donc pas utiliser ces clés peu pratiques et vont préférer les déposer dans un *exchange*, c'est-à-dire un portefeuille électronique de bitcoins en ligne géré par un intermédiaire. Dès lors, pour payer, au lieu de taper leur clé, ils ne donneront que leur mot de passe

habituel permettant d'accéder à ce site web. Or, peut-on avoir davantage confiance en cet intermédiaire qu'en une banque ? Car, pour voler du bitcoin, il suffit désormais d'attaquer l'intermédiaire et l'espoir de récupérer les sommes volées sera nul, contrairement à ce que garantissent les banques. Le bitcoin n'est en effet pas une monnaie, mais, comme l'or, un actif qui, une fois perdu, est perdu pour de bon. Sauf à avoir des sommes à dissimuler au fisc, préférer le bitcoin aux banques ne semble pas être une très bonne idée. Si les cryptomonnaies se généralisent, cela servira donc sans doute plus à conforter les banques qu'à les fragiliser.

Dans le cadre d'un projet de recherche, nous avons épluché tous les rapports de chercheurs et de consultants sur les autres usages possibles de la *blockchain*. Outre les cryptomonnaies, on trouve tout ce qui concerne les échanges d'actifs, la traçabilité des chaînes logistiques, les *smart contracts*, l'identité numérique, le e-gouvernement, la vérification des médicaments, le micro-prêt, les micro-réseaux d'énergie, etc. Pour chacun de ces cas d'usage, nous nous sommes demandé si le besoin d'une *blockchain* était avéré. La réponse, sans surprise, a été négative dans tous les cas. Le besoin existant est celui d'une numérisation, qui sera réalisée d'une manière bien plus efficace au moyen d'une solide plateforme centralisée, qu'avec une *blockchain* distribuée.

Il existe cependant deux vrais cas où l'emploi de la *blockchain* est légitime. Le premier survient lorsque vous ne voulez pas d'intermédiaire, par exemple si vous échangez des kalachnikovs contre de la cocaïne. Effectivement, en ne passant pas par une banque, personne ne voit vos affaires de blanchiment d'argent. À ceci près que, toutes les transactions étant enregistrées aux yeux de tous sur le système bitcoin, le FBI peut faire le lien entre un compte bitcoin et un individu précis, et ainsi disposer de tout l'historique de ses transactions !

Le second cas est celui où vous ne trouvez pas d'intermédiaire. L'exemple est celui des *microgrids* énergétiques de Brooklyn, qui permettent de s'échanger de l'électricité entre voisins. Personne ne faisant confiance à personne dans un tel cas et aucun tiers de confiance ne souhaitant – pour l'instant – organiser ces échanges, la *blockchain* peut alors s'avérer utile si son coût ne s'avère pas prohibitif.

Quel avenir pour la *blockchain* ?

Le futur de la *blockchain* est sans doute analogue à celui de toutes les technologies innovantes dont on tend, lors de leur émergence, à surestimer les effets à court terme. Le marché bancaire actuel, dont l'offre est pléthorique, risque-t-il alors de se faire concurrencer par des acteurs "low cost", utilisant la *blockchain* pour des usages existants (du transfert d'argent à l'étranger, du compte habituel, etc.), comme cela a été le cas dans d'autres secteurs ? Il semble évident que l'on ne pourra guère renverser, pour des raisons de coûts, une banque et son savoir-faire avec la *blockchain* telle que nous la pratiquons aujourd'hui.

Le problème est que l'on n'a considéré qu'une forme de rupture, celle par les coûts. Il existe cependant une autre forme de rupture, moins évidente, qui consiste à ne pas s'intéresser aux clients qui sont déjà servis, mais plutôt aux non-consommateurs ou aux consommateurs dans des situations de consommation non habituelles. Ainsi, à l'époque où l'industrie du disque produit des Super-Audio CD et DVD-Audio d'une qualité très supérieure à celle de leurs prédécesseurs, certains consommateurs commencent à écouter du MP3, de très médiocre qualité. Ce n'est certes pas pour une utilisation à domicile, mais dans le métro, avec des mesures et des exigences de qualité différentes. Il en va de même pour la *blockchain* : trop peu efficace et trop coûteuse pour les usages actuels, son application pour des usages que personne n'envisage à cette heure pourrait créer ce type de rupture.

Pour que la rupture numérique survienne, il faut essentiellement des plateformes. Cela s'étudie dans le cadre d'un phénomène connu, la *prosommation*, désignant le fait que des individus ont des activités productrices sur leur temps privé. Dans les années 2000, cela concernait les contenus – tweets, photos, vidéos, etc. –, puis, dans les années 2010, on a vu émerger des échanges de services entre particuliers, et demain, on fabriquera des objets en impression 3D. Or, pour que ces ruptures se produisent, il faut attendre qu'une plateforme de "confiance" – Facebook, Airbnb, etc. – émerge. La *blockchain* pourrait permettre à tout un chacun de créer rapidement une plateforme sans qu'aucune confiance a priori ne soit requise. En facilitant et en accélérant

l'émergence d'usages de rupture (non pris en compte par le marché) peut-être deviendra-t-elle alors elle-même une technologie de rupture.

Comme souvent, dans les transitions numériques, tout le monde se focalise sur les mauvaises choses, sur le piratage de la musique, par exemple, avant de se rendre compte qu'il s'agit en fait d'une nouvelle forme de concurrence. En outre, je ne suis pas certain que la *blockchain* sera effectivement utilisée, mais le simple fait de son existence et de sa disponibilité peut suffire à créer la rupture en créant une menace.

Aujourd'hui, n'importe quel marché peut devenir contestable, c'est-à-dire un marché dans lequel chacun peut entrer pour offrir un produit ou un service, et si les acteurs installés ne veulent pas prendre en compte les usages déviants des consommateurs, ils savent désormais que ceux-ci pourront se passer d'eux pour trouver satisfaction. Cela ne signifie pas que la concurrence est effectivement là, mais cela crée une pression concurrentielle telle que les acteurs établis se rendent compte que s'ils ne donnent pas aux consommateurs ce qu'ils souhaitent, au prix qu'ils veulent, cette concurrence finira par émerger.

Si les acteurs existants ne changent pas de modèle d'affaire, la menace deviendra effective, les usages déviants restant rarement déviants et devenant souvent la nouvelle norme.

Débat

Un intervenant : *Quel type de plateforme pourrait utiliser la* blockchain *?*

Thierry Rayna : Les grandes plateformes conventionnelles, comme Airbnb, rendent les transactions possibles parce que leurs usagers ont confiance en elles. Néanmoins, pour certains besoins qui ne sont pas encore pris en compte par ces plateformes, des initiatives locales vont pouvoir émerger sans les attendre, tels les micro-réseaux d'énergie, dans lesquelles l'absence de confiance pourra alors justifier l'usage de la *blockchain*.

Int. : *La* blockchain *est énergivore. Envisage-t-on des améliorations sur ce point ?*

T. R. : Selon les chercheurs du laboratoire informatique de Polytechnique, unanimes à ce sujet, il n'y a pas de moyens moins coûteux d'assurer le même niveau de sécurité que celui apporté par la preuve de travail. Toute autre alternative est beaucoup plus perméable aux attaques et requière davantage de centralisation et de confiance dans les acteurs du système.

En cas de crise

Int. : *En cas de crise majeure du système bancaire, peut-on imaginer que le système bitcoin se substitue à lui ?*

T. R. : Une analogie existe avec le milieu de la musique. Le premier réseau pair à pair était totalement centralisé autour de Napster, ce qui a permis au FBI de le fermer facilement. À sa place, un autre réseau, Gnutella, s'est développé en étant réellement décentralisé, ce qui rendait rigoureusement impossible toute tentative de fermeture. Néanmoins, son inefficacité a été telle que personne ne l'a utilisé ! Il faut donc un minimum de centralisation et c'est exactement ce qui est en train de se passer avec l'Éthereum, autre cryptomonnaie, et sa *proof of stake*, pour laquelle on est parti d'une complète décentralisation pour progressivement réintroduire une dose de centralisation. Personnellement, je ne voudrai pas vivre dans un monde où le seul moyen de transaction

serait le bitcoin, tellement il est inefficace ! Il ne faut pas oublier que, du point de vue économique, l'existence des institutions – entreprises, banques, etc. – s'explique par le fait que la confiance qu'on leur accorde permet de réduire les coûts de transaction[9]. Or, à l'opposé, le principe du bitcoin est de remplacer la confiance par des coûts de transaction. Est-ce vraiment souhaitable ?

Int. : *En ce qui concerne les montants, le bitcoin est à des années-lumière des masses monétaires circulant dans le monde. Son effondrement n'aurait donc qu'un impact limité sur l'économie.*

T. R. : Ce serait effectivement le cas aujourd'hui. Mais si, dans une ou deux décennies, l'engouement pour ces cryptoactifs perdurait, et dans un monde où les banques seraient stressées comme lors de la crise des *subprimes*, il en irait sûrement autrement !

Régulation !

Int. : *Les États n'auraient-ils pas intérêt à offrir des services adossés à la* blockchain *plutôt que de laisser des plateformes comme Uber structurer les marchés pour leur plus grand profit ?*

T. R. : Il est vrai que les États auraient pu prendre les devants et proposer des technologies pour des plateformes d'intérêt général. Mais pourquoi utiliseraient-ils la *blockchain* ? À de rares exceptions près, tout le monde fait confiance à l'État. On a sans doute besoin de plateformes ouvertes, pour lesquelles la confiance n'est pas remise entre les mains d'intérêts privés ou étrangers, mais la *blockchain* n'a de raison d'être que lorsqu'il n'y a pas d'intermédiaire de confiance. Dans tous les autres cas, elle est coûteuse et largement inefficace.

Int. : *La* blockchain *peut-elle être utile dans des pays en manque d'infrastructures ?*

T. R. : Dans de tels cas, la situation serait tout à fait différente et son usage pourrait se justifier en l'absence d'un réseau bancaire, par exemple. Encore faut-il qu'il y ait un réseau électrique suffisamment fiable pour pouvoir miner, ce qui n'est, par exemple, pas le cas aujourd'hui au Venezuela. Cela peut aussi permettre d'échapper à l'omniprésence de certains États qui nous pistent jusque dans notre vie privée.

Int. : *Vous avez beaucoup parlé de confiance, mais pas de la garantie en dernier recours, en l'occurrence l'État, donc chacun de nous. La carte bancaire n'est pas parfaitement sécurisée, nous courrons donc un risque en l'utilisant, mais, en dernier recours, nous serons remboursés.*

T. R. : J'ai rencontré quantité de start-up travaillant dans l'espace de la *blockchain*. Toutes n'ont qu'un seul mot à la bouche : régulation ! Pauvre Nakamoto ! Elles se rendent compte qu'à un moment, elles ne peuvent aller plus loin, car leurs clients leur demandent comment, si elles disparaissent, ils pourront récupérer leur mise, ce qu'elles ne peuvent évidemment pas garantir seules.

Int. : *La* blockchain *peut-elle changer les rapports sociaux ?*

T. R. : Aujourd'hui, on n'a pas besoin d'utiliser la *blockchain* pour cela, pas plus qu'il n'était nécessaire en son temps d'utiliser Gnutella pour se rendre compte qu'il existait un besoin latent de Spotify ou de Netflix. Mais la crainte de son utilisation peut pousser certains à s'ouvrir au fait que, demain, les gens voudront échanger quantité de choses qui ne sont pas numérisées à l'heure actuelle. Ces entreprises auront-elles alors peut-être la volonté d'innover, avec ou sans la *blockchain*.

9. Les coûts de transactions correspondent aux coûts induits par l'usage du marché : coûts de recherche, de négociation, de contractualisation, coûts de vérification, d'application des contrats, etc.

Présentation de l'orateur

Thierry Rayna : professeur de management de l'innovation à l'École polytechnique et chercheur au CNRS au sein du laboratoire i3-CRG (Institut interdisciplinaire de l'innovation, Centre de recherche en gestion, UMR CNRS 9217). Sa recherche porte sur l'impact des technologies numériques sur les modèles d'affaires, les modes de management de l'innovation et les politiques publiques.

Diffusion août 2019