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

L'Association des Amis de l'École de Paris du management organise des débats et en diffuse les comptes rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

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

© École de Paris du management – 187, boulevard Saint-Germain – 75007 Paris
Tél. : 01 42 79 40 80 – e-mail : contact@ecole.org – http://www.ecole.org

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.