La *blockchain* déchaîne les questions !

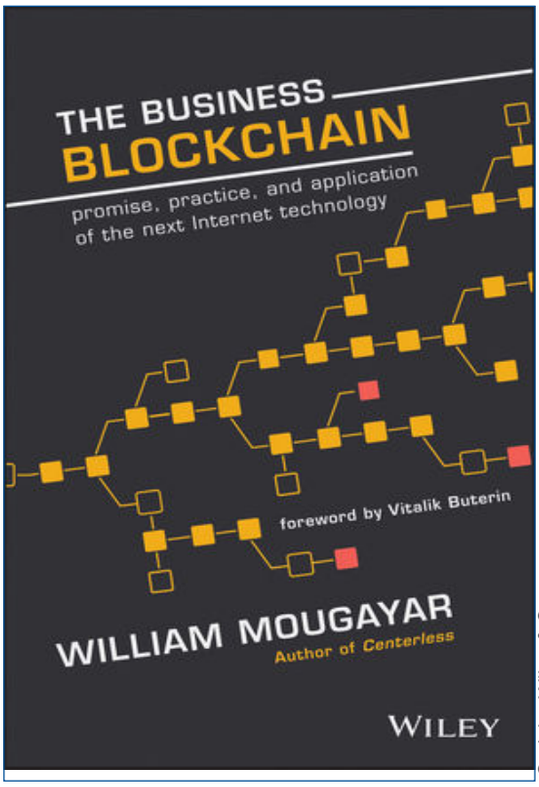
À propos des ouvrages de William Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley & Sons, 2016 ; de Don Tapscott et Alex Tapscott, *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world*, Penguin, 2016, et de Blockchain France, *La* Blockchain *décryptée – Les clefs d'une révolution*, NETEXPLO, 2016

Par Thierry BOUDÈS
ESCP Europe

Le tiers de confiance, un acteur clé de l'économie

Quel est le point commun entre votre banque, Airbnb et ENEDIS ? *A priori,* aucun. Trois secteurs distincts et trois entreprises aux histoires différentes. Pourtant, ces trois entreprises remplissent, à des degrés divers, le même rôle, celui de tiers de confiance : votre banque vous permet de régler vos achats par carte bancaire auprès de commerçants que vous ne connaissez pas et qui ne vous ont jamais rencontré auparavant ; Airbnb rend possible la location de la maison d'une famille que vous ne verrez qu'en photo avant d'y entrer et ENEDIS vous permet d'obtenir de l'électricité d'un fournisseur à qui vous ne serrerez jamais la main. En résumé, un tiers de confiance est un acteur qui facilite la transaction entre deux parties en les rassurant. Par exemple, Airbnb demande de nombreuses informations aux bailleurs et aux locataires et, de surcroît, permet à chacun de noter l'autre de façon publique. Ainsi, Airbnb crée de la confiance, et comme rien n'est gratuit, il se rémunère : Airbnb prélève des commissions.

Et si les technologies de l'information permettaient de se passer des tiers de confiance ? C'est la promesse de la *blockchain*. L'invention de cette technologie est attribuée à Satoshi Nakamoto, le pseudonyme de la personne ou du groupe (toujours inconnu(e) à ce jour et objet de nombreuses rumeurs) qui publie sur Internet, en octobre 2008, un manifeste qui pose les bases du bitcoin, une monnaie totalement électronique qui défraie la chronique en raison de sa volatilité, de ses variations spectaculaires de cours. Pour obtenir une monnaie électronique sans banque centrale, il faut une technologie qui évite qu'une même somme soit dépensée plusieurs fois, ce que les tiers de confiance empêchent dans la vie réelle. La *blockchain* le permet en résolvant informatiquement le dilemme connu comme « le problème des généraux byzantins » : comment organiser la communication entre des acteurs qui peuvent se trahir les uns les autres et qui ne peuvent communiquer que par des messages, sans avoir la possibilité de savoir si ceux-ci sont vrais ou faux ? Sur ce constat, Mougayar (p. 11) suggère de comprendre la *blockchain* comme la rencontre de trois champs : la théorie des jeux (le problème des généraux byzantins), la cryptographie (pour garantir l'authenticité et l'intégrité des informations) et l'ingénierie logicielle (pour faire circuler les informations, puisqu'il s'agit d'une couche technologique qui vient s'appuyer sur l'Internet).

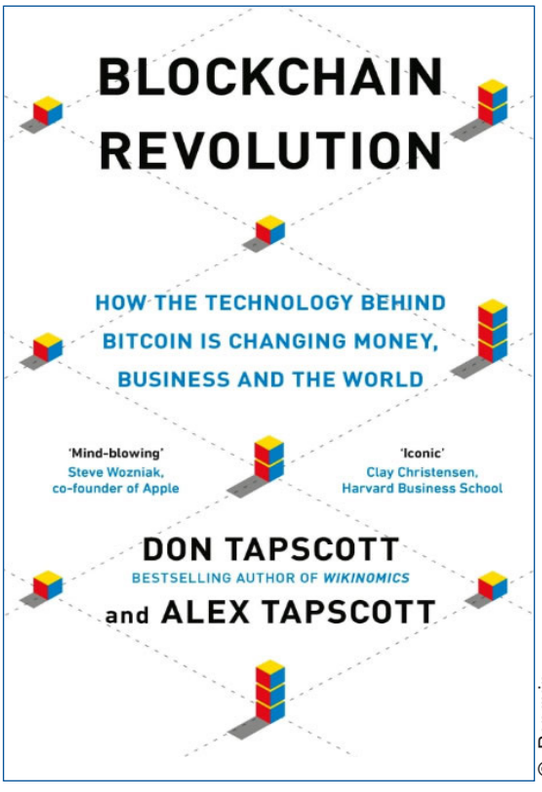


© John Wiley & Sons

Une révolution en germe

Les possibilités ouvertes par la *blockchain* sont donc nombreuses et très impactantes. Trois ouvrages

se sont intéressés dès 2016 à cette technologie : *The Business Blockchain,* écrit par un entrepreneur de l'Internet, cherche à montrer que la *blockchain* est une technologie à part entière ; *Blockchain Revolution*, rédigé notamment par l'auteur du célèbre *Wikinomics*, souligne les transformations profondes qu'elle va engendrer, et *La* Blockchain *décryptée,* un ouvrage proposé par de jeunes entrepreneurs organisateurs de la première conférence en France en 2015 sur le sujet, vise à le rendre accessible en donnant des exemples de champs d'application. Tous s'accordent sur les innovations de rupture qui sont en germe. Blockchain France décrit ainsi le cas des *smart contracts,* qui s'apparentent à « des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la *blockchain*. Ils fonctionnement comme toute instruction conditionnelle de type *if-then* (si telle condition est vérifiée, alors telle conséquence s'exécute) » (p. 11). Ainsi, dans le cas des assurances voyages, un tel service conduirait à ce que les passagers assurés qui subissent un retard soient automatiquement dédommagés, sans avoir à faire de démarche particulière. Selon les auteurs, 60 % d'entre eux ne font pas valoir leurs droits, alors qu'ils disposent d'une assurance (pour Tapscott et Tapscott – p. 258 –, c'est le cas de 80 % des ruptures de contrat, à un niveau général). De nombreux autres exemples de *smart contracts* peuvent être trouvés dans le numéro des *Annales des Mines*, série *Réalités industrielles*, d'août 2017, qui leur est entièrement consacré. Tapscott et Tapscott (pp. 156-161) dressent ainsi la liste de douze secteurs d'activité qui sont les plus concernés par une transformation radicale. Ils vont de la santé aux transports, en passant par la finance et la distribution. Le mélange de *smart contracts*, de transactions sans tiers de confiance et d'Internet permet d'imaginer des *business models* complètement nouveaux.



© Penguin

Le principe

Selon Blockchain France (p. 129), « la *blockchain* est une technologie de stockage et de transmission d'informations transparente, sécurisée et fonctionnant sans organe central de contrôle. […] Par extension, une *blockchain* constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs, et ce, depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne ». Pour se représenter cette technologie, l'image du grand livre est utilisée : « Imaginez qu'au centre de la place de la Concorde, à Paris, à côté de l'Obélisque, on installe un très grand cahier que, librement et gratuitement, tout le monde puisse lire, sur lequel tout le monde puisse écrire, mais qu'il soit impossible à effacer et indestructible » (Jean-Paul Delahaye, 2015[1]). Le principe général est le suivant : des membres rejoignent un réseau *blockchain* (celui-ci peut aller du totalement public au totalement privé, avec toutes les nuances possibles) ; ils réalisent des transactions. Celles-ci sont regroupées en blocs, qui sont validés par un « nœud du réseau », rôle que peut tenir n'importe quel membre. Le premier nœud qui parvient à résoudre un problème mathématique complexe crée la validation. Ce processus permet « la fabrication du consensus » : nul ne sait *a priori* quel est le nœud qui va valider, puisqu'ils sont en concurrence entre eux pour résoudre le problème mathématique. Le problème est difficile à résoudre (car il demande un temps long de computation), mais il est facile de vérifier qu'il a été résolu : c'est ce mécanisme qui fabrique la preuve de la validation, et donc la confiance. Ces nœuds sont appelés « mineurs » (par analogie avec les mineurs qui cherchent de l'or) et sont rémunérés (en monnaie électronique) pour leur travail de validation. Le bloc ainsi validé et daté est enregistré et est dès lors visible pour l'ensemble du réseau. L'intégralité de l'historique des transactions reste accessible.

La *blockchain* ouvre ainsi de nouveaux champs des possibles dans trois directions : un dispositif de cryptomonnaie (qui permet de transférer de la valeur), un système de transactions décentralisé (qui rend possible une collaboration entre de multiples acteurs,

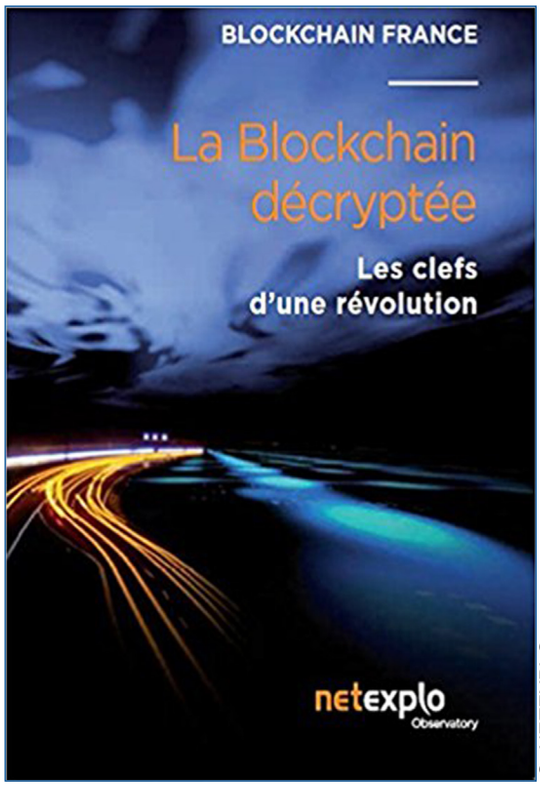
(1) DELAHAYE J.-P. (2015), « Les *blockchains*, clés d'un nouveau monde », *Pour la Science*, n°449.

tout en garantissant l'authenticité des échanges numériques) et une plateforme de développement logiciel (qui ouvre à des écosystèmes d'applications).

Des limites à la diffusion de la *blockhain*

Toutefois, la diffusion massive et rapide de la *blockchain* se heurte pour l'instant à plusieurs limites dont quatre majeures. Premièrement, en l'état actuel, la technologie ne peut supporter une hausse brutale et massive du nombre de ses utilisateurs (c'est un problème dit de « scalabilité ») : par exemple, les temps de traitement des transactions restent trop longs pour permettre un usage très large. Deuxièmement, le principe de validation des transactions par la résolution informatique d'un problème mathématique consomme énormément d'énergie. Un développement des *blockchains* à grande échelle va se heurter à cette limite. Or, pour Tapscott et Tapscott (p. 260), c'est là le prix à payer pour ne pas avoir à se soumettre à une autorité centrale. Troisièmement, la technologie *blockchain* reste difficile à comprendre pour un non-initié. C'est un frein majeur à sa diffusion. Enfin, la technologie présente de nombreux défis en termes de régulation, qui risquent de pousser les États et les gouvernements à contrôler sa progression.

D'un point de vue prospectif, le champ des possibles ouvert par la *blockchain* est immense. Les trois ouvrages montrent qu'il est actuellement exploré par deux types d'acteurs : des *start-ups,* qui défrichent le terrain en proposant de nouveaux *business models*, mais à des échelles très réduites et principalement à partir de *proofs of concept* (c'est-à-dire des prototypes), et des entreprises et organisations installées qui mènent des expérimentations sur le sujet afin de pouvoir intégrer cette technologie le moment venu, mais qui en protègent jalousement la confidentialité.



© NETEXPLO

La promesse de la *blockchain* est d'offrir une technologie qui permette de s'affranchir de tiers de confiance. Elle ne se limite donc nullement au bitcoin. Toutefois, il est utile de se souvenir, avec Mougayar (pp. 148 à 150), que c'était aussi la promesse de l'Internet au début des années 1990. Or, presque trente ans plus tard, force est de constater que la Toile se déploie au travers de très gros acteurs et que son évolution questionne désormais le principe fondateur de la neutralité du Net. Par analogie, il est possible de supposer qu'une diffusion massive des technologies *blockchain* puisse conduire, paradoxalement, non pas à la disparition des tiers de confiance, mais à leur mutation, voire à leur simple déplacement. Selon Mougayar (pages 110 et suivantes), de nouveaux géants pourraient émerger, devenant les spécialistes de l'établissement de la preuve pour l'identification des utilisateurs, les achats, les titres de propriété, etc. De telles organisations pourraient même se structurer *via* la *blockchain* et devenir des *Distributed Autonomous Organizations* (DAO).

Difficile de prédire jusqu'où nous mènera le train de la *blockchain.* Mais impossible de le savoir…, si l'on ne monte pas dedans !