Les risques des *blockchains*

La technologie informatique de la *blockchain* a un énorme potentiel de développement par ses possibles applications à de nombreux domaines où la confiance joue un rôle essentiel. Sa marque de fabrique est en effet de fonctionner de façon totalement décentralisée, donc sans tiers certificateur de confiance. Pourtant, les risques et les inconnus restent importants.

Auteurs
Laurent Dehouck
Maître de conférences en sciences de gestion, ENS Rennes
Audrey Thomas
ENSAM[1]

Le Bitcoin, valorisé à plus de 1 000 $ en janvier 2017, a ensuite chuté à 750 $ en une dizaine de jours, pour se stabiliser autour de 850 $ avant de remonter autour de 1 200 $ début mars. L'instabilité de son cours atteste des risques que les utilisateurs du Bitcoin doivent supporter. Tel semble, apparemment, être le sort, de cette crypto-monnaie, qui est la première application de la technologie (sous-jacente) des *blockchains*. Pour autant, juger de la dangerosité des *blockchains* à travers cet exemple isolé donne une image inexacte des potentialités de cette technologie. En effet, le Bitcoin[2] est avant tout le nom de l'unité de compte d'un système expérimental de transfert de propriété sécurisé, qui repose sur un réseau de pair à pair sans autorité centrale. Autrement dit, il s'agit de la face émergée d'un logiciel et d'un protocole de communication crypté, qui se substitue à la monnaie, à la banque centrale supposée y être liée et à l'État qui l'encadre. Outre l'échange de monnaie entre ses utilisateurs, le réseau soutient la construction d'un consensus partagé sur la valeur détenue par chacun sans tiers de confiance.

On comprend mieux, dès lors, les interrogations qui s'attachent à l'application de cette *blockchain*. Elle pourrait remettre en question les débats économiques relatifs à la place de l'État et des entreprises en tant qu'entités coordinatrices. En effet, comme elle consiste en une nouvelle technologie décentralisée de coordination, elle pourrait rendre inutile l'existence de « tiers de confiance », socle fondamental de légitimité de nombreuses institutions (la banque centrale, l'État, l'assureur, etc.).

Certains acteurs des *blockchains*, créateurs de start-up comme Vitalik Buterin (Ethereum), ne craignent pas d'évoquer « la révolution » *blockchain*.

1 > Nous remercions M. Jean-Baptiste Lenhof pour ses commentaires et son aide.
2 > https://bitcoin.fr

D'aucuns défendent même l'idée qu'il s'agirait d'une nouvelle classe de réseau, dont le potentiel de transformation de la société serait comparable à celui d'internet (Swan, 2015).

De nombreuses incertitudes accompagnent toutefois l'émergence de cette nouvelle technologie, parce que ses usages et ses applications potentielles se multiplient (Caseau et Soudoplatoff, 2016). Des débouchés nouveaux s'ouvrent en matière de preuve et/ou d'échange de propriété de contenus numériques, par exemple dans le domaine de la programmation, du stockage de données, sans préjuger des futures applications. En effet, la technologie commence à intéresser les acteurs privés de la santé, de l'art, de la bancassurance, mais également les acteurs publics, à propos des papiers d'identité ou du cadastre (Caseau et Soudoplatoff, 2016). Les annonces d'investissements en la matière ne cessent d'alimenter la chronique, notons juste l'une des dernières en date : Scor rejoint un consortium mondial d'assureur B3I (Blockchain Insurance Industry Initiative) qui compte dans ses rangs, par exemple, Munich Re, Swiss Re, Allianz ou encore Generali.

Au-delà des effets de mode et d'enthousiasme, il convient cependant de s'interroger sur les principes de fonctionnement de la *blockchain* en vue d'en évaluer les risques. Cela implique, tout d'abord, de comprendre le concept général de *blockchain*. Nous établirons, ainsi, qu'il s'agit d'un réseau décentralisé, cryptographié et dépourvu de tiers de confiance, mais que ses applications sous forme de « *blockchain*s privées » ont fait évoluer ce concept initial. Il s'agira, ensuite, de recenser les risques associés aux utilisations de cette technologie en fonction de la diversité des objectifs recherchés par leurs concepteurs. Nous nous attacherons en conclusion à mesurer les enjeux des transformations sociales susceptibles d'en découler.

Les principaux risques du concept de *blockchain*

Le concept originel

On doit le concept de *blockchain* à Satoshi Nakamoto[3] qui l'a mis en œuvre pour la première fois en 2008. Il s'agissait, en l'espèce, de donner une infrastructure logicielle à la création du Bitcoin, constituée d'une chaîne de blocs liés dans un ordre chronologique (les blocs validés sont non modifiables). Chacun de ces blocs contient un ensemble de transactions finies entre les utilisateurs. L'objectif de Nakamoto était de permettre « des paiements en ligne, envoyés directement d'une partie vers une autre sans passer par l'intermédiaire d'une institution financière[4] ».

Afin que deux personnes puissent échanger ces paiements en toute sécurité, la *blockchain* est munie d'un système de cryptographie. Chaque utilisateur dispose de deux clés de cryptage, l'une publique et l'autre privée, pour encoder avec sûreté les messages de transaction. Supposons, par exemple, la transaction suivante : « A échange 1 Bitcoin avec B contre une baguette » (Nakamoto, 2008). Admettons que A soit l'émetteur du Bitcoin et B le receveur, A va crypter le message de transaction à l'aide de sa clé privée et envoyer sa clé publique à B, afin qu'il puisse décoder le message. B fera de même réciproquement pour finaliser l'échange de Bitcoin. Ce processus d'encodage est dit antisymétrique[5] pour éviter qu'un utilisateur ne découvre la clé privée d'un autre utilisateur et lui dérobe son identité. Cette étape de cryptage évite ainsi les fausses transactions.

Une fois le paiement accepté entre A et B, il convient d'en informer tous les autres utilisateurs, en ajoutant un bloc validé contenant cette transaction à la *blockchain* grâce à une procédure appelée « minage ». C'est l'étape de formation d'un consensus entre tous les participants. Si le cryptage d'une transaction est une condition nécessaire d'ajout de celle-ci à un bloc de la *blockchain*, il ne constitue pas une condition suffisante du consensus.

À cet effet, le message crypté d'une transaction entre A et B vient s'insérer dans un bloc temporaire, en attente d'une validation par les « mineurs[6] ». Le minage ajoutera la transaction au livre de compte (au registre), afin d'être propagée et reconnue par tous les détenteurs de Bitcoins (A aura un Bitcoin de moins et B un Bitcoin de plus). Cette étape forme le consensus distribué de la *blockchain*. Il permet aux utilisateurs de s'accorder sur la liste des transactions valides et sur leur ordre qui est immuable. Le nouveau bloc est alors inscrit dans un grand livre de compte partagé par chaque utilisateur et mis à jour automatiquement. Il contient toutes les transactions inscrites dans les blocs validés et réalisées sur la *blockchain*. Il autorise la traçabilité des échanges. Grâce à lui, les utilisateurs peuvent contrôler eux-mêmes que l'utilisateur avec lequel ils s'apprêtent à effectuer une transaction est bien solvable (la quantité de crypto-monnaie dont il dispose est

3 > Il s'agit d'un pseudonyme. L'identité réelle de cet innovateur demeure un mystère.
4 > Par exemple, utiliser le Bitcoin pour un transfert de fonds à l'étranger coûterait, en principe, quelques centimes et prendrait 10 min, contre des coûts de l'ordre de 10 % de la transaction et un délai de paiement de deux ou trois jours, lorsqu'on utilise, en comparaison, les services de Western Union.
5 > La méthode utilisée pour crypter le message n'est pas la même que celle utilisée pour le décrypter.
6 > Il s'agit de donner le pouvoir de la validation à un participant de la *blockchain* et s'assurer que tous ensuite entérinent la validité du nouveau bloc (de toutes les transactions qu'il contient). Le pouvoir de validation est donné au mineur qui résout le premier un problème mathématique de cryptage qui dépend notamment de la puissance de calcul consacré. Les utilisateurs rejoignent, ainsi, des *pools* de mineurs (groupes de mineurs associés) pour avoir une puissance de calcul plus importante et valider plus rapidement les blocs temporaires.

inscrite sur ce livre de compte). Ainsi, B verra qu'il a bien reçu un Bitcoin de la part de A et qu'il peut, en retour, lui délivrer une « baguette », comme dans l'exemple de Nakamoto.

Ce registre est public, sécurisé et partagé par tous les membres du réseau (Pilkington, 2015). Il contient l'ensemble des transactions validées sur la *blockchain* depuis sa création jusqu'à aujourd'hui. À chaque nouveau bloc miné, le nouveau livre des transactions est modifié et diffusé à l'ensemble du réseau, si bien qu'il n'est pas falsifiable, car il faudrait modifier de la même manière toutes ses copies disponibles. Grâce à ce dispositif parfaitement décentralisé, la *blockchain* est un système sans tiers de confiance parce que chaque transaction inscrite dans un bloc ratifié devient vérifiable par tous les utilisateurs du réseau (Pilkington, 2015). La *blockchain* constitue donc une réserve de données hautement fiable, partagée, confidentielle et non réfutable (Hull, 2016).

La *blockchain* constitue donc une réserve de données hautement fiable, partagée, confidentielle et non réfutable

Les zones de risques : l'exemple du Bitcoin

En principe, les éléments ci-dessus qui décrivent la technologie *blockchain* assurent la sécurité du réseau et des échanges entre les utilisateurs de Bitcoin. Pour autant, ces objectifs initiaux ne sont pas toujours atteints.

Une des premières sources de risque concerne la procédure de minage. Lorsque la *blockchain* fonctionne sous « preuve de travail », un bloc validé offre au mineur ayant résolu le problème une récompense sous forme de Bitcoin (12,5 Bitcoins par bloc confirmé) pour le travail fourni. Des dérives peuvent alors apparaître. Si un mineur découvre la solution le premier, il dispose alors d'un bloc Be, qu'il devrait communiquer aux autres participants. Mais il peut garder ce bloc secret et travailler de suite à la validation du bloc suivant sans divulguer Be au reste du réseau[7]. C'est ce qu'on appelle du « minage égoïste » (Göbel, 2016).

Dès l'instant où un autre mineur, « honnête », trouve un bloc Bh allant à la suite de la *blockchain*, alors presque instantanément le mineur « égoïste » va divulguer son bloc Be. Le réseau se retrouve ainsi en présence de deux blocs validés presque en même temps et temporairement conservés sur la *blockchain*. Certains nœuds du réseau auront connaissance du bloc Be et d'autres auront connaissances du bloc Bh. Des nouveaux blocs vont alors s'ajouter à la suite de Be et Bh. Deux chaînes différentes se constituent et sont maintenues jusqu'à ce qu'une chaîne plus longue soit identifiée. C'est alors cette chaîne qui sera conservée dans la *blockchain*, tandis que l'autre sera supprimée. La création simultanée de deux blocs provoque ce qu'on appelle une « bifurcation » (figure 1). Si A, par exemple, échange un Bitcoin avec B et que cette transaction est inscrite dans Be, et que, dans le même temps, A échange un Bitcoin avec C dans Bh, alors on est dans un cas de double dépense (Decker, 2013) et, *in fine*, un des utilisateurs (B ou C) sera volé[8].

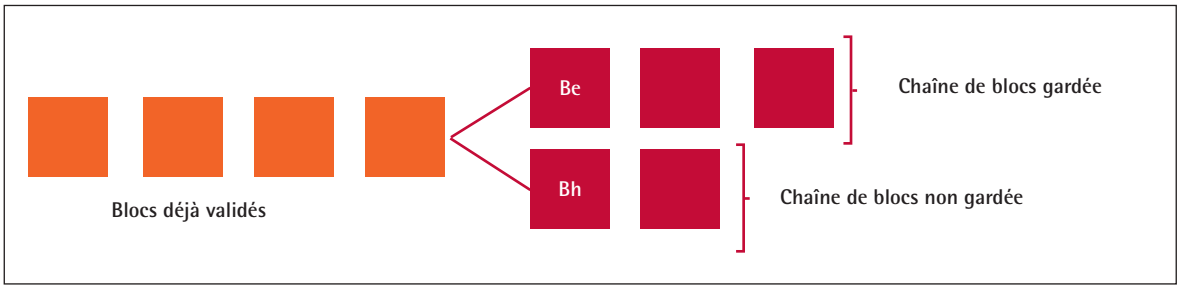
Pour le Bitcoin, les délais de propagation des blocs sont relativement conséquents (10 min) et sont la première cause de bifurcation.

Un autre objectif fondamental des échanges d'actifs est l'anonymat des utilisateurs. Or, il est possible, avec des outils appropriés, de connaître en détail l'activité d'un utilisateur (Reid, 2012). Pour contrer ce problème, la solution est de regrouper un certain nombre de signatures sous un lien unique et ainsi augmenter l'anonymat des utilisateurs ayant réalisé une transaction. Cette méthode consiste à utiliser une composition de signatures (Saxena *et al.*, 2014). Il sera alors inscrit sur la *blockchain*

7 > Le fait de ne pas divulguer le bloc Be lui fait prendre de l'avance vis-à-vis du reste des utilisateurs du réseau pour la recherche de la solution suivante, car chaque bloc validé est relié aux blocs précédents (Eyal et Sirer, 2014).

8 > Ce genre de pratique malhonnête remet en cause la confiance et conduit certains à proposer de transformer le concept initial. Faut-il une autorisation d'entrée sur la *blockchain* ? Donc une autorité centrale, un tiers de confiance ? Le développement de *blockchains* dites « privées » prend ce parti, en modifiant certains paramètres techniques (taille des blocs, acteur et durée de validation, récompense obtenue, etc.).

Figure 1. Illustration d'une bifurcation



Source : d'après J. Göbel *et al.*, « Bitcoin Blockchain Dynamics: The Selfish-Mine Strategy in the Presence of Propagation Delay », *Performance Evaluation*, n° 104, 2016, p. 23-41.

Quelques exemples d'attaques possibles qui diminuent la sécurité d'une *blockchain*

Les attaques « Man-in-the-middle-attack » : un « pirate » intercepte et transmet des informations en les modifiant sur la *blockchain*. Comme les transactions de validité ne sont pas auditées, il est possible d'insérer des transactions invalides qui ont l'air valides dans le registre (le livre de compte).

Les attaques « SYN-Flood » : elles consistent à envoyer des requêtes rapidement et de manière répétée jusqu'à ce que la cible soit saturée et qu'elle n'ait plus assez de puissance pour légitimer et contrôler le trafic.

Les attaques « Sybil » : un agresseur rentre dans le réseau *blockchain* grâce à des nœuds qu'il contrôle. Les mineurs associés à ces nœuds sont les siens. Il constitue ainsi un réseau de trafiquants, ce qui facilite ses futures attaques.

Les attaques « Éclipse » : elles provoquent des séparations du réseau en plusieurs groupes. Les utilisateurs d'un groupe ne peuvent joindre ceux d'un autre groupe et les chaînes continuent de s'étendre dans chacun des groupes. Il faut recevoir un bloc d'une chaîne inconnue pour que les utilisateurs prennent conscience de l'existence d'un autre groupe et puissent résoudre ce problème.

que les transactions regroupées sous la même signature ont bien eu lieu, mais il ne sera pas possible de les identifier une à une.

Un autre défi majeur, que la technologie *blockchain* n'a pas encore résolu pour devenir réellement une crypto-monnaie, est l'échelle des transactions (scalabilité). Pour les Bitcoins, elle est de sept transactions par seconde en raison de la taille des blocs retenus, alors qu'elle devrait permettre un nombre de l'ordre de 20 000 transactions par seconde, à l'instar des opérateurs de carte bancaire (par exemple Visa).

Enfin, la généralisation du Bitcoin suppose une expérience utilisateur simple, sans risques, et dont l'évidence s'impose à chaque usage. Ce n'est pas encore le cas pour le Bitcoin qui semble s'apparenter davantage à un dispositif de construction de la confiance entre un groupe d'utilisateurs très motivés qu'à une monnaie.

On le comprend, la généralisation d'une crypto-monnaie en substitution d'une monnaie classique n'est pas encore pour demain ! Mais le Bitcoin et son développement montrent au moins en partie la validité du concept, même si de nombreux risques sont encore attachés à l'usage de la *blockchain* à des fins de transferts d'actifs (encadré).

C'est pour répondre à ces risques que des évolutions du concept se développent dans de très nombreux domaines sous la forme de *blockchains* privées et/ou de *smart contracts*.

Les développements du concept

Blockchain publique et *blockchain* privée

Pour répondre aux difficultés expérimentées avec le Bitcoin, de nouveaux protocoles de minage sont apparus[9]. L'utilisation d'un système de contrôle qui vérifie les transactions réalisées sur la *blockchain* et s'assure du bon fonctionnement de la plateforme est plus facile à mettre en œuvre. Ce sont des *blockchains* privées. Elles font cependant disparaître plusieurs des dimensions clés du concept : la décentralisation et l'absence de tiers de confiance (Pilkington, 2015).

Les utilisateurs d'une *blockchain* privée obtiennent l'autorisation d'entrer dans la chaîne d'une autorité centrale. Ces *blockchains* sont développées par de grandes institutions qui testent la technologie pour diminuer les coûts de traitement d'information et favoriser le partage de base de données communes (cf. supra, les B3I). Elles sont administrées par une ou plusieurs organisations, afin d'assurer le niveau requis de coordination, de confiance et de sécurité. Sur les *blockchains* privées, le réseau est souvent restreint à quelques membres identifiés par un contrôle de permission d'accès. Les coûts de transaction sont également moins élevés, car il y a un nombre réduit de mineurs. La connectivité entre les nœuds est améliorée, diminuant, de fait, les temps de validation des transactions par comparaison avec une *blockchain* publique. Il existe aussi, parfois, des restrictions d'accès sur une *blockchain* privée, qui ne sont pas autorisées sur une *blockchain* publique.

Le principe d'une rupture conceptuelle entre les concepts de *blockchain* privée et publique n'est pas si clair, car il existe entre ces deux conceptions tout un continuum de *blockchain* « partiellement décentralisée » (Brown, 2015).

Ces variations montrent à la fois le caractère expérimental de la technologie et les multiples applications possibles pour les acteurs qui les inventent et les testent. Ainsi, des applications récentes pour le suivi des approvisionnements dans une organisation industrielle « en flux tendus » mettent tout particulièrement une autre propriété distinctive de cette technologie : la traçabilité des trans-actions.

La variété des acteurs et des usages qu'ils inventent pour cette nouvelle technologie ne permet pas d'identifier de manière générique des risques. En effet, la définition de la norme ISO 3 100 du risque (2009)

9 > L'un des plus connus est celui associé à Ethereum, avec un principe de minage « *proof of stake* » différent de la preuve de travail du Bitcoin. Un troisième concept, « *proof of authority* », est utilisé par les *blockchains* privées et est fondé sur l'identité des mineurs autorisés à valider les données.

comme « l'effet de l'incertitude sur l'atteinte des objectifs » implique des registres très différents de risques selon les objectifs des acteurs. Cette variété des risques augmente encore lorsqu'on s'intéresse à un autre développement de la *blockchain*, les *smart contracts*.

La *blockchain* des *smart contracts*

Le concept de *smart contract* a été introduit en 1994 par Nick Szabo de la manière suivante : « ce sont des protocoles d'instructions automatiques, qui exécutent les termes d'un contrat », bref un programme inséré à l'intérieur de la *blockchain*. Ils permettent d'automatiser une suite de transactions sur la *blockchain* grâce à un élément déclencheur extérieur[10]. Par exemple, un assuré pourrait s'affranchir de remplir un formulaire de déclaration de sinistre. Le processus d'indemnisation serait lancé automatiquement grâce à un capteur extérieur qui transmettrait l'information de la survenue d'un sinistre. Cette étape d'automatisation permet de gagner en coût et en rapidité. Les actions effectuées sont ensuite inscrites dans la base de données partagée (la *blockchain*). L'objectif n'est plus de transmettre des Bitcoins mais d'exécuter un programme automatique convenu d'avance entre deux cocontractants. Les « *smart contracts* présentent plusieurs avantages. Ils permettent un échange juste entre deux parties avec des règles données dans une logique programmable » (Juels, 2016).

Le secteur des services financiers et des assurances semble retenir tout particulièrement ces deux idées dans l'expérimentation de « *blockchain* privée de *smart contract* », afin de diminuer les coûts de traitement des informations en back-office notamment (Trautman, 2016).

Des risques nouveaux apparaissent dans ce cas singulier. En effet, la minimisation et l'automatisation des interactions, liée à ce type particulier de *blockchain*, rend la découverte d'actions délictuelles plus difficile. De plus, la prise en compte d'événements externes pour le déclenchement d'un *smart contract* élargit les opportunités délictuelles à toute la vie courante. Par exemple, un utilisateur mal intentionné pourrait créer un dispositif qui offrirait une récompense automatique au complice qui lui aura fourni de manière confidentielle la clé privée d'un autre utilisateur (Juels, 2016). Face à ces risques, de nouvelles opportunités (risques positifs) sont évoquées pour ce type particulier de *blockchain* dans les services financiers (figure 2).

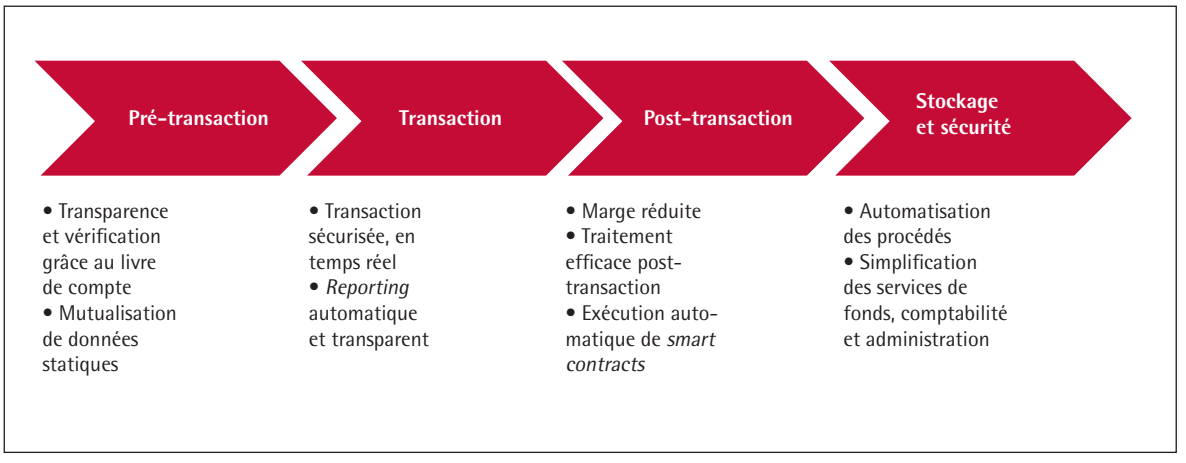
Le problème du *reporting* et du traitement des données en nombre entraîne un coût global d'environ 20 millions de dollars par an (Fanning, 2016). La technologie *blockchain*, parce qu'elle permet d'automatiser ces opérations, pourrait largement diminuer ces coûts.

Dans le secteur de l'audit, on s'attend également à un bouleversement des pratiques en cas de diffusion de cette technologie. En effet, serait-il encore nécessaire de vérifier les transactions et les comptes lorsqu'on utilise un registre global et partagé (une base de données distribuée) ? Une simple lecture du registre permettrait de s'en assurer. De nombreux emplois d'audit ou d'application de procédures tels que audit financier, demande de formulaire, déclaration de sinistre… pourraient ainsi être mis en cause par une adoption généralisée de ce type de *blockchain*.

Certains envisagent également l'application de cette technologie dans le domaine des Big Data (Swan, 2015) pour faciliter l'automatisation de tâches prédictives. On peut également prévoir des expérimentations dans le secteur médical, où les dossiers des patients

10 > Dans le cas d'une assurance pour retard en matière de transport aérien, l'accès automatique à plusieurs bases de données de compagnies aériennes validant l'effectivité d'un retard pour un vol donné déclencherait automatiquement sans déclaration, ni suivi, le remboursement prévu au contrat de l'assuré.

Figure 2 : Bénéfices de l'adoption de la *blockchain*



Source : Euroclear et O. Wyman, « Blockchain in Capital Markets: The Prize and the Journey », février 2016.

© Yoann Constantin

seraient conservés en toute confidentialité sur la *blockchain* (Caseau et Soudoplatoff, 2016).

Conclusion

Pour Goertzel, à plus long terme, la technologie *blockchain* pourrait provoquer sur l'ensemble de la société des bouleversements majeurs : « Le concept de *blockchain* est un nouveau paradigme pour la découverte, la valorisation et le transfert de données et ainsi pour la coordination de toute activité humaine à une échelle bien plus large que ce qui a pu être réalisé jusqu'à aujourd'hui » (Goertzel, 2016). Il va même jusqu'à soutenir que ce concept pourrait permettre l'émergence d'un véritable « socialisme décentralisé » en raison de ses principales propriétés : la décentralisation des décisions, l'inutilité du « tiers de confiance » et la traçabilité transparente.

Si sa généralisation en économie se confirme et qu'elle constitue bien une rupture analogue à celle du réseau internet il y a vingt ans, elle pourrait même réfuter la thèse principale de « la route de la servitude » (Hayek, 1944) selon laquelle l'indisponibilité d'une information complète empêche l'intervention efficace de l'État (même bienveillant).

Pour Atzori, elle pourrait également contribuer à redéfinir les modes de gouvernance organisationnels parce qu'elle met en cause le rôle traditionnel de l'État et plus généralement des institutions centralisées comme tiers de confiance. Il soutient qu'elle « encourage les citoyens à créer leurs propres systèmes de gouvernance, dans lesquels la centralisation, la coercition et les hiérarchies cèdent la place aux mécanismes de consensus distribué » (Atzori, 2015).

On le voit bien, la *blockchain* représente une source de transformations économiques et sociales très importantes, et donc inévitablement de risques. Il importe cependant, comme on l'a montré, de distinguer plusieurs situations en la matière.

Dans le cas de la *blockchain* publique, le principe d'une base de données partagée automatisée, sans tiers de confiance, dont la finalité serait de remplacer une monnaie, interroge principalement des risques de sécurité et de scalabilité. Si l'on étend le concept à d'autres fonctions dévolues traditionnellement à des institutions centralisées jouant le rôle de tiers de confiance, ce sont des incertitudes plus larges qui s'attachent à la pérennité de secteurs économiques ou publics entiers.

Par ailleurs, dans les cas de *blockchains* privées associés à des *smart contracts*, on a vu que le concept initial est profondément transformé. Un dispositif de contrôle d'accès et de validation de la base de données partagée répond au moins en

partie aux questions de sécurité et d'échelle. En revanche, la réalisation des objectifs spécifiques attachés à ces projets n'est pas garantie. Elle comporte donc de nombreux risques distinctifs.

Ainsi, la variété des domaines d'application de la technologie *blockchain*, des concepts qui s'y réfèrent, tout comme la diversité de ses promoteurs et des utilisateurs potentiels déterminent bien davantage qu'un registre de risques génériques. Il apparaît nécessaire d'approfondir chaque cas particulier d'application, qui donne naissance à des risques singuliers, propres aux finalités des acteurs parties prenantes de chacun de ces projets. ●

> bibliographie

Pour commencer (en français)

Bourguignon S., « *Blockchain*, pas si simple pour les grands groupes ! », 20 mars 2017. En ligne : https://siecledigital.fr, entrer le titre de l'article dans le moteur de recherche.

Caseau, Y. et **Soudoplatoff S.**, « La *blockchain* ou la confiance distribuée », 8 juin 2016. En ligne : www.fondapol.org, entrer le titre de l'article dans le moteur de recherche.

Pour approfondir (en anglais)

Atzori M., « Blockchain Technology and Decentralized Governance: Is the State Still Necessary? », 2015. En ligne : https://papers.ssrn.com, entrer le titre de l'article dans le moteur de recherche.

Brown R. G., « The Unbundling of Trust, How to Identify Good Cryptocurrency Opportunities? », 14 novembre 2014. En ligne : https://gendal.me, entrer le titre de l'article dans le moteur de recherche.

Decker C. et **Wattenhofer R.**, « Information Propagation in the Bitcoin Network », Conference IEEE P2P 2013 Proceedings.

Eyal I. et **Sirer E. G.**, « Majority is not Enough: Bitcoin Mining is Vulnerable », International Conference on Financial Cryptography and Data Security, 2014.

Fanning K. et **Centers D. P.**, « Blockchain and Its Coming Impact on Financial Services », *Journal of Corporate Accounting & Finance*, n° 27, 2016, p. 53-57.

Göbel J., **Keeler H. P.**, **Krzesinski A. E.** et **Taylor P. G.**, « Bitcoin Blockchain Dynamics: The Selfish-Mine Strategy in the Presence of Propagation Delay », *Performance Evaluation*, n° 104, 2016, p. 23-41.

Goertzel B., **Goertzel T.** et **Goertzel Z.**, « The Global Brain and The Emerging Economy of Abundance: Mutualism, Open Collaboration, Exchange Networks and The Automated Commons », *Technological Forecasting and Social Change*, n° 114, 2017, p. 65-73.

Hull B. et **Chen D.**, « Towards a Shared Ledger Business Collaboration, Language Based on Data Aware Processes », *Lecture Notes in Computer Science*, n° 9936, 2016.

Juels A., **Kosba A.** et **Shi E.**, « The Ring of Gyges: Investigating the Future of Criminal Smart Contracts » Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

Kiviat T. I., « Beyond Bitcoin: Issues in Regulating Blockchain Transactions », *Duke LJ*, n° 65, 2015, p. 569-608.

Nakamoto S., « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008, En ligne : https://bitcoin.org/bitcoin.pdf

Pilkington M., « Blockchain Technology: Principles and Applications » ; in **F. X. Olleros** et **M. Zhegu** (eds), *Research Handbook on Digital Transformations*, Edward Elgar Publishing, 2016.

Reid F. et **Harrigan M.**, « An Analysis of Anonymity in The Bitcoin System », in **Y. Altshuler**, **Y. Elovici**, **A. B. Cremers** *et al.* (eds), *Security and Privacy in Social Networks*, Springer, 2013, p. 197-223.

Saxena A., **Misra J.** et **Dhar A.**, « Increasing Anonymity in Bitcoin », in **R. Böhme**, **M. Brenner**, **T. Moore** et **M. Smith** (eds), *Financial Cryptography and Data Security*, Springer, 2014, p. 122-139.

Swan M., *Blockchain: Blueprint for a New Economy*, Tim McGovern, 2015.

Trautman L. J., « Is Disruptive Blockchain Technology the Future of Financial Services? », 2016. En ligne : https://papers.ssrn.com, entrer le titre de l'article dans le moteur de recherche.

Yli Huumo J., **Ko D.**, **Park S.** et **Smolander K.**, « Where is Current Research on Blockchain Technology? – A systematic Review », *PloS One*, octobre 2016.