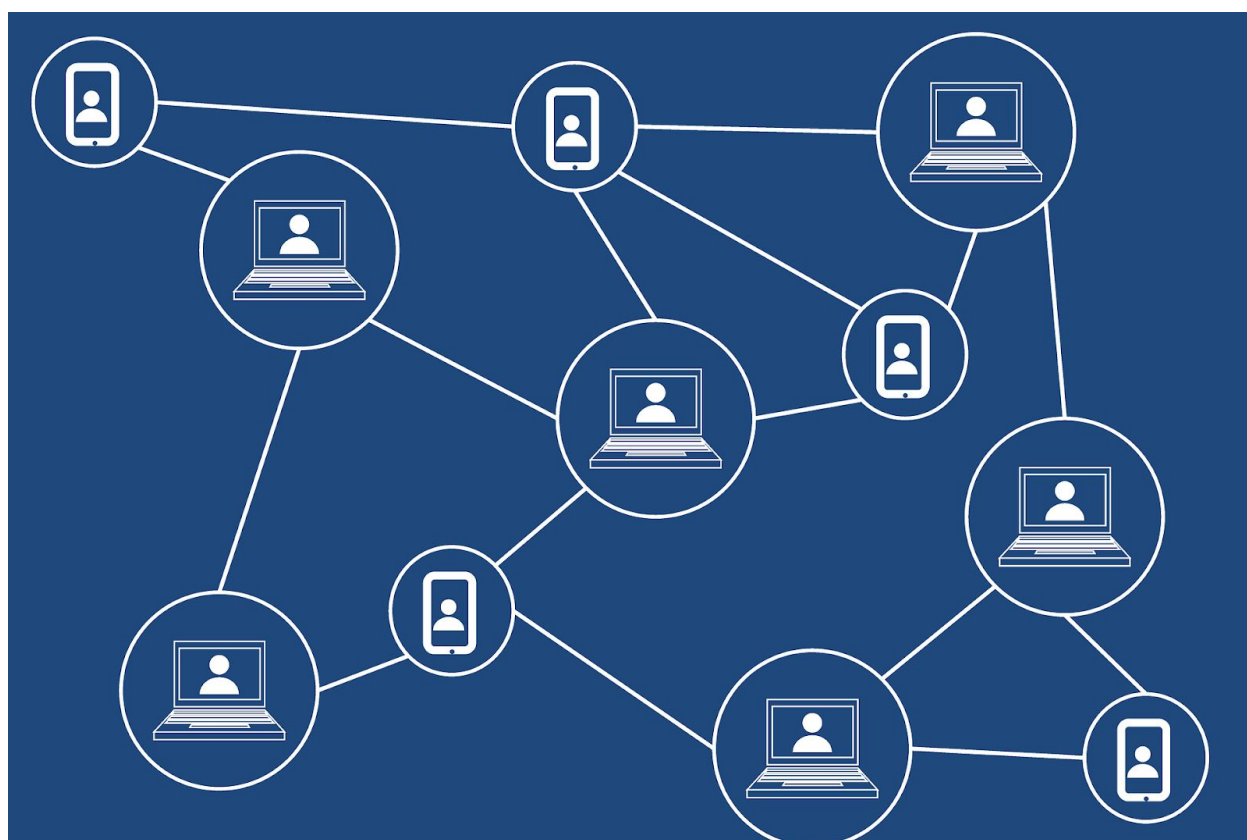


ANALYSE

LA TECHNOLOGIE BLOCKCHAIN

Présentation des principes de cette
base de données d'un nouveau type



Alors que nous avons déjà publié une première analyse introductive¹ sur ce sujet l'année dernière, il semble important d'y revenir car les potentielles applications de la technologie blockchain dans le secteur financier sont nombreuses et en voie d'apparition. En terme d'impacts, on peut s'attendre à l'arrivée de nouveaux services, à de meilleures performances en matière de transactions commerciales et de transferts de valeurs, tant en termes de coût qu'en termes de rapidité. Toutefois, pour donner à tout un chacun la capacité de percevoir les risques et opportunités que recèle cette nouvelle forme de base de données, cette deuxième analyse, sans doute un peu technique, en présente les principales caractéristiques et particularités, indispensables pour poser convenablement la base d'une compréhension critique. Elle nous servira de référence dans les analyses à venir, qui s'attelleront aux applications existantes ou à venir dans le secteur financier.

En quelques mots :

- Une blockchain est une base de données, une blockchain n'est qu'une base de données
- Qu'est-ce qui différencie une blockchain d'une base de données classique ?
- Forces et faiblesses, un match qui se joue point par point.

Mots clés liés à cette analyse : blockchain, base de données, technologie financière

INTRODUCTION

Il existe de multiples manières de décrire la technologie blockchain afin de rendre cette nouveauté compréhensible à tout un chacun. La comparaison entre la technologie blockchain et la base de données traditionnelle fait partie, parmi la littérature compulsée, des plus intelligibles, en voici dès lors les points les plus saillants.

Une base de données dont la gestion est décentralisée²

¹ L. Beth, A. Cayrol, juillet 2017, « La blockchain, une révolution pour la finance ? », Réseau Financité, disponible sur : https://www.financite.be/sites/default/files/references/files/analyse_blockchain_170713_com_final.pdf

² Cette section repose sur la contribution majeure suivante : Gideon Greenspan, 17 mars 2016, « Blockchains vs centralize

Une base de données, qui, dans la sphère financière, peut par exemple prendre la forme d'un registre de transactions (monétaires / financières), est le plus souvent gérée de manière centralisée : les acteurs (usagers) ne se connaissant pas, ils n'ont pas de raisons ni d'éléments sur laquelle construire une confiance mutuelle. Dans ce cas précisément, la confiance des acteurs est accordée à un organe central, souvent appelé « tiers de confiance », dont le rôle est de garantir la conformité des transactions : ça peut être une banque, une société de transferts de fonds, une société de cartes de crédit ... Dans ce cas encore, c'est « le tiers de confiance qui détient le monopole de la mise à jour du registre des transactions afin d'écartier tout risque de fraude »¹³.

La technologie blockchain repose quant à elle sur une validation décentralisée, confiée à un nombre significatif d'acteurs-validateurs. En général, tous les acteurs ne sont pas en charge de cette validation. Seule une partie de ces acteurs se voient confiés cette tâche de validation : pour cela, ils doivent prouver leur capacité à le faire de manière sécurisée. À cette fin, dans l'exemple du Bitcoin, ils sont mis en concurrence dans leur capacité à résoudre des problèmes de cryptage qui leurs sont confiés. Les mineurs, c'est comme ça que les « acteurs-validateurs » s'appellent pour le Bitcoin, sont rémunérés pour ce travail de cryptage qui mobilise une importante capacité de calcul des ordinateurs qu'ils emploient. La validation décentralisée, sécurisée par des techniques de cryptage mises en œuvre par les mineurs, permet d'atteindre un degré de sécurité élevé et de construire un registre à l'historique qualifié par beaucoup d'infalsifiable⁴. Ce qui fait que la technologie blockchain rend une base de données infalsifiable, c'est d'avoir résolu, à travers ce système de « minage », le problème de la « double dépense », c'est-à-dire, la possibilité d'une personne mal intentionnée de multiplier son argent en manipulant la base de données. C'est un petit miracle à l'ère du numérique, où rien n'est plus facile que de copier/modifier l'information.

Dès lors, pour les potentiels développeurs d'un registre, d'une base de données, les questions essentielles qui détermineront la préférence pour la base de données centralisée ou pour la technologie blockchain porteront donc sur l'intérêt que la décentralisation peut avoir, sur le niveau de solidité et de résilience nécessaire, sur le niveau de sécurité et de confidentialité souhaité. Enfin, la question de la performance est elle aussi un élément déterminant du choix : la rapidité et le coût énergétique ont

databases », posté sur : <https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/>

³ Côte Berbain, août 2017, « la blockchain : concept, technologies, acteurs et usages », in F.F.E.- « Annales des Mines - Réalités Industrielles », p.6. Disponible sur : <https://cairn.info/revue-realites-industrielles-2017-3-page-6.htm>

⁴ Un bloc de la chaîne intègre systématiquement l'information relative au bloc dont il est issu. Ce lien au bloc précédent (la chaîne) est considérée comme ineffaçable et toujours visible par l'ensemble des acteurs.

d'ailleurs déjà été évoqués dans une précédente analyse⁵.

Ce qui ne change pas : le type de contenu

Sur ce point, Gideon Greenspan (2016, p.1) affirme sans détour que les contenus d'une base de données classique ou de la technologie blockchain ne diffèrent pas : ce que l'on stocke dans l'une peut être stocké dans l'autre. Cela comprend aussi ce que l'on appelle aujourd'hui les « smart contracts / contrats intelligents » qui sont des lignes de code informatiques qui permettent, notamment, de vérifier et d'exécuter un contrat⁶.

Décentralisation : le point est pour la technologie blockchain

Si l'initiateur d'un registre, d'une base de données, ne souhaite pas devoir opérer de manière centralisée, car cela le contraint à construire une sécurité basée sur un dispositif où il serait le seul à en être le garant, la technologie blockchain est une alternative intéressante.

Pourquoi décentraliser ? Ce choix peut reposer sur une philosophie du partage des rôles entre les usagers d'un registre. Il peut également reposer sur la pertinence de faire appel au grand nombre pour la vérification / la validation des données ou des documents stockés dans la base de données.

Ce choix semble également opportun si la logique de la base de données est d'en rendre le contenu et la gestion accessibles à un grand nombre d'acteurs.

L'aspect économique n'est pas non plus étranger à ce type d'option, car c'est aussi un moyen de réduire les coûts significatifs que génèrent le développement, la gestion, l'entretien et la protection d'une base de données centralisée. Ces dernières opérations représentent de la main-d'œuvre et du temps de travail qui sont largement remplacés, dans la technologie blockchain, par de la puissance de calcul, du codage et du cryptage dit intelligent, potentiellement bien moins coûteux⁷.

⁵ L. Beth & A. Cayrol, juillet 2017 « La blockchain, une révolution pour la finance ? », Réseau Financité, disponible sur : https://www.financite.be/sites/default/files/references/files/analyse_blockchain_170713_com_final.pdf

⁶ Un contrat intelligent permet de vérifier qu'une condition est respectée afin de déclencher une procédure définie : ex : le code postal est bien dans la liste qui déclenche l'envoi d'un message publicitaire, ex : les informations requises dans le formulaire sont complètes et génèrent automatiquement un profil utilisateur...

⁷ Quoique potentiellement gourmand en énergie.

Confidentialité : avantage à la base de données centralisée

Comme il a déjà été évoqué, la validation de nouveaux blocs d'information dans la base de données partagée (blockchain) est réalisée par des mineurs. Ce qui est particulier à la technologie blockchain et sur lequel il est important d'insister, c'est que chaque mineur participe, indépendamment les uns des autres, à la validation d'un nouveau bloc. En effet, dans le cas de certaines applications de la technologie blockchain, tous les mineurs ont une vue complète, quasiment en temps réel, sur : 1) l'état présent de la base de données ; 2) les modifications requises par l'introduction d'un nouveau bloc (chaque bloc contient une série de transactions⁸ qui seront ainsi validées et enregistrées dans la base de données) ; 3) la signature digitale qui prouve l'origine de la transaction (origine qui est donc enregistrée et non modifiable)⁹.

Cette manière de construire une base de données est particulièrement maline, certes, mais la question de la transparence maximale est en revanche véritablement rédhibitoire dans certains secteurs où la confidentialité est importante, ce qui est encore le cas dans de nombreux domaines financiers notamment.

Le Bitcoin, par exemple, utilise ce système de transparence complète. En revanche, de nombreuses autres « cryptomonnaies » ont pour but l'anonymat et souhaitent au contraire rendre intraquables les transactions. À titre d'exemple, Monero, Dash et ZCash, sont les trois « cryptomonnaies » les plus utilisées à ces fins. Mais de nouveaux projets émergent en continu. Par exemple, Verge est une « cryptomonnaie » qui intègre l'utilisation du réseau Tor¹⁰ pour complètement masquer à la fois les adresses IP et les transactions dans la base de données elle-même. Enfin, même si la confidentialité n'est pas « intégrée » dans le Bitcoin, il existe de nombreux moyens de rendre les transactions difficilement traçables. Par exemple, on peut avoir recours à un « mixer », qui est un service en ligne permettant de « mélanger » ses Bitcoins avec d'autres et ressortir avec le même montant, mais visant à rendre impossible de « suivre » un paiement de façon continue. Aussi, il ne faut pas oublier qu'il est possible d'ouvrir des comptes Bitcoin à l'infini (en théorie en tout cas) et que donc, les utilisateurs qui cherchent à conserver leur anonymat peuvent créer des adresses à « utilisation unique » qui sont abandonnées une fois leur transaction effectuée.

⁸ L'enregistrement dans la base de données blockchain ne se fait pas par transaction mais bien par lots de transactions.

⁹ L'immutabilité de la blockchain, pour probable qu'elle soit, n'en est pas moins mythique. Nous invitons le lecteur intéressé à lire le passionnant article, en anglais, de Gideon Greenspan, « The Blockchain Immutability Myth », posté le 4 mai 2017, à l'adresse suivante : <https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/>

¹⁰ [https://fr.wikipedia.org/wiki/Tor_\(r%C3%A9seau\)](https://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau))

Ce que l'on doit retenir à ce stade, c'est qu'une base de données centralisée contrôle par essence qui aura le droit d'intervenir sur le contenu de la base et qui aura le droit de la compulser. A contrario, par essence, la technologie blockchain contrôle qui écrit dans la base (dans le cas du Bitcoin, il s'agit des mineurs), qui sont toutefois souvent nombreux¹¹, mais pas ce qui est visible, potentiellement accessible à tous si le système adopté par les créateurs de cette solution blockchain le permet.

Dans un cas comme dans l'autre, des correctifs peuvent être apportés afin d'ouvrir à plus dans un cas, restreindre à d'autres dans le second cas, mais ces aménagements vont toutefois à l'encontre des flux naturels que génèrent ces deux architectures différentes et peuvent en réduire la performance, la fluidité.

Robustesse et résistance aux « bugs / erreurs / attaques / ... » : avantage à la technologie blockchain

Indéniablement, la technologie blockchain est construite de façon telle qu'elle peut tolérer erreurs, bugs et attaques sans pour autant que cela bloque son fonctionnement ou pervertisse largement son contenu. Ceci est dû à la méthode de validation, faite de manière redondante par l'ensemble des mineurs.

En effet, puisque chaque mineur valide chaque transaction, aucun des mineurs ne tient un rôle prépondérant, crucial pour la base de données. En outre, puisque chaque mineur est connecté à d'autres dans un réseau dense (peer-to-peer), il y a tellement de connexions dans la chaîne qu'une paralysie est très peu probable. La base de données est répliquée en permanence dans la technologie blockchain par chaque mineur. Si des connexions entre mineurs devaient s'interrompre, elles n'auraient qu'un impact minime sur le fonctionnement global. La réplication (backup) d'une base de données centralisée est une opération qui est également routinière dans le cadre d'une gestion attentive du risque, mais on comprend qu'elle n'est pas inscrite dans son ADN.

Dès lors, le fait d'activer un backup lors d'un bug sur une base de données centralisée reste une opération risquée, toujours difficile à finaliser correctement, faisable mais coûteuse. En temps, en argent et en réputation : le scandale récent de l'attaque d'Equifax¹², un registre de crédits américain en est une belle illustration.

¹¹ La logique de la technologie blockchain construit en effet sa solidité sur le fait de faire valider par un nombre important de « mineurs » chaque nouveau bloc. Ce n'est qu'une fois validé par une majorité de mineurs qu'un nouveau bloc est finalement confirmé dans la base de données.

¹²<https://www.theguardian.com/technology/2017/sep/19/equifax-credit-firm-march-breach-massive-may-hack-customers>

Cependant, il ne faut pas surestimer la robustesse de la technologie blockchain. Il reste des manières d'attaquer une blockchain, notamment l'attaque des « 51% », c'est-à-dire, prendre le contrôle de plus de la moitié des « mineurs » ou ordinateurs qui sécurisent le réseau. A priori, on pourrait penser que c'est impossible, vu le nombre de machines impliquées dans le minage, par exemple pour le Bitcoin. Mais la « tendance » à la centralisation est toujours difficile à contrecarrer. Un des problèmes est la croissance des « mining pools » ou « bassins de minage ». Une fois que le nombre de mineurs sur un réseau atteint un certain nombre, la probabilité que l'ordinateur d'un mineur trouve la bonne solution au problème, confirme les transactions et se voit récompenser en « cryptomonnaie » diminue sensiblement ! Et donc, il se pourrait que sa machine tourne pendant des années, consommant de l'électricité, avant de recevoir pour ses efforts une « récompense » en « cryptomonnaie ». Afin de résoudre ce problème, les mineurs rejoignent des « bassins de minage » où les bénéfices sont redistribués de façon plus équitable entre eux. Cette évolution fragilise toutefois le principe même de la « décentralisation » et de la robustesse dont elle est porteuse. Il ne faudrait donc pas prendre le contrôle de milliers d'ordinateurs dispersés à travers le monde, mais de quelques « bassins de minage » pour corrompre une blockchain¹³.

Pour ce qui est de la correction de bugs, la technologie blockchain n'est pas non plus le système le plus pratique. Afin de modifier le mode de fonctionnement d'une blockchain, il faut obtenir le consensus, idéalement unanime, de la communauté qui la maintient (mineurs et ceux qui hébergent une copie de la base de données sur leur ordinateur). C'est un processus très lent et qui, lorsqu'il n'y a pas de consensus, peut soit donner lieu à une « séparation » de la base de données et la naissance d'une nouvelle « cryptomonnaie » (par exemple, la création de Ethereum Classic¹⁴) ou l'annulation d'une mise à jour et donc l'impossibilité de réparer un problème (par exemple, les coûts élevés des transactions en Bitcoin sont en partie dû à l'impossibilité pour la communauté Bitcoin à se mettre d'accord sur une solution).

Enfin, n'oublions pas qu'une blockchain ne vit que par la libre participation des mineurs. Le site « deadcoins » par exemple, recense toutes les initiatives de « cryptomonnaies » basées sur la technologie blockchain qui se sont éteintes¹⁵. Et contrairement à une base de données centralisée où on peut identifier une personne ou une entreprise « responsable » et donc que l'on peut poursuivre en justice, ou la forcer à maintenir/modifier la base de données, il n'y a personne qui est « responsable » de l'extinction d'une base de données de type blockchain.

¹³ <https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27>

¹⁴ Gideon Greenspan, 4 mai 2017, Op.cit, § « Mutability in public chains »

¹⁵ <http://deadcoins.com/>

Rapidité : le point pour les bases centralisées, pour l'instant...

Cette qualité est sans doute la plus intuitive : puisque pour l'enregistrement dans une base de données, la technologie blockchain doit, en plus des opérations faites dans les deux approches¹⁶, prendre en charge trois tâches supplémentaires :

- **la vérification de la signature** : on l'a déjà évoqué, chaque transaction est signée. La signature cryptée authentifie l'origine de la transaction. Puisque dans un système décentralisé, les nouvelles inscriptions¹⁷ dans la base de données se transmettent de mineurs à mineurs selon une logique peer-to-peer, la sécurité du système repose sur la traçabilité des transactions elle-même garantie par cette signature cryptée. On l'aura compris à ce stade, la signature cryptée est la base de la solidité du système, de sa fiabilité. Pour ce faire, une signature cryptée requiert d'importantes puissances de calcul à même de résoudre des problèmes complexes, ce qui demande du temps et de l'énergie aux mineurs.
A contrario, dans une base centralisée, une fois encodés, les codes d'accès permettant d'agir dans la base par son gestionnaire, il n'est pas nécessaire de vérifier l'origine des données qui s'y trouvent pour y ajouter des transactions, puisqu'à l'origine des données contenues dans la base, on trouve le gestionnaire.
- **la validation des transactions par consensus** : quand un bloc de transactions est ajouté par un mineur dans la technologie blockchain, il n'en est pas pour autant validé de manière définitive. Le processus de validation, dans la technologie blockchain, n'est pas un processus instantané. En effet, comme on l'a dit, tous les mineurs valident toutes les modifications de toute une blockchain. Chacun vérifie donc que l'information nouvellement introduite n'entre pas en contradiction / en conflit avec le contenu des blocs précédents. Si une majorité de mineurs considèrent que le bloc nouvellement introduit est correct, il sera finalement validé dans la blockchain¹⁸. Cela peut toutefois donner lieu à des allers et retours entre mineurs jusqu'à ce qu'une position quant à la validité de la transaction soit prise.

¹⁶ Notamment : formatage, encodage, tri... des données

¹⁷ Les nouvelles inscriptions, théoriquement, dans la blockchain, n'en recouvre, n'en efface jamais des plus anciennes. En ce sens, elles sont toujours de nouvelles transactions. En cas d'erreur, on peut introduire des données nouvelles dans un bloc (le n° 15 par exemple) qui a pour but de corriger des données passées erronées disponibles dans un bloc situé en amont de la chaîne (le n°11). Ces dernières restent donc visibles, mais on sait alors que les données du bloc 11 sont erronées et remplacées par les données du bloc 15.

¹⁸ Le ou les blocs ainsi identifiés comme incorrects seront abandonnés, d'une certaine manière détricotés, car c'est toujours la chaîne la plus longue qui est la chaîne active. Lecteur intéressé trouvera plus d'informations en compulsant des articles traitant de la question des fourches (blockchain fork) et de l'abandon systématique des chaînes interrompues ou courtes. D'une certaine manière, la réalité des fourches remet partiellement en question le caractère prétendument inaltérable et ineffaçable de la chaîne... Matière à réflexion, donc.

Ce processus de dialogue et de consensus est absent du schéma de contrôle d'une base centralisée, dont la procédure est en général moins gourmande en temps. En outre, dans une base centralisée, la procédure ne risque pas de générer des goulets d'étranglement liés à un intense *dialogue* entre mineurs.

- **la répétition des opérations** : c'est toute la force et aussi la plus grande faiblesse de la technologie blockchain dont il est question ici. Dans une base centralisée, une fois la transaction encodée par le responsable, il n'y a plus rien à faire. Dans le cas de la technologie blockchain, la nouvelle transaction devra être traitée par tous les mineurs de la chaîne. Cela représente une débauche en force de calcul, en temps et en énergie, totalement disproportionnée par rapport au résultat, identique, atteint par la base centralisée.

Néanmoins, il y a de nombreuses initiatives qui visent à réduire la durée de confirmation des transactions. On peut citer, à titre d'exemple, Ethereum qui a une vitesse moyenne de confirmation de transactions de 14 secondes. Ripple, qui est basé sur une blockchain centralisée, a une vitesse de confirmation de 4 secondes. À l'avenir, de nouvelles solutions comme le « Proof of Stake », qui vise à remplacer le coûteux processus de minage, ou encore les transactions « off chain » et le « sharding » (décider stratégiquement quelles transactions doivent être conservées dans une blockchain et celles qui peuvent être réalisées en dehors et donc plus rapidement) pourront également accélérer la rapidité des transactions.

Droit à l'oubli : le point va sans hésiter à la base centralisée

Pour ce qui est du droit à l'oubli, de l'effacement d'un fichier ou même de la rectification d'une « erreur » nécessitant une intervention humaine, les bases de données centralisées resteront toujours la référence. Il est essentiel de rappeler qu'une blockchain ne peut pas être modifiée, mis à part des événements exceptionnels (une décision unanime de toute la communauté de modifier la base de données). Dans le cas d'une erreur de paiement sur une blockchain, il sera impossible de l'annuler, mis à part retrouver le destinataire et le « forcer » à rendre la « cryptomonnaie ». Dans le cas d'une perte des codes d'accès à un compte sur une blockchain, l'accès sera perdu à tout jamais. Les bases de données centralisées, quant à elles, disposent toujours d'un mécanisme, plus ou moins facile, pour modifier la base de données en cas de problème/nécessité. Par exemple, modifier une erreur dans un registre de crédit, ou récupérer une nouvelle carte de banque si on a

oublié son code PIN.

CONCLUSION

Au terme de cette analyse, il semble important de tirer les principaux enseignements des spécificités techniques de la technologie blockchain d'une part, et de la base centralisée d'autre part, afin de structurer notre réflexion sur la place de l'un et de l'autre demain, dans le monde de la banque et de la finance.

Lorsque la confidentialité et la performance sont essentielles dans l'application envisagée, alors la base de données centralisée ou les « cryptomonnaies » utilisant des solutions rendant les transactions confidentielles est le choix recommandé : lorsque les données traitées sont sensibles, touchent à la vie privée. Combien de personnes seraient prêtes à rendre visible par tous, leurs transactions bancaires ? Leurs investissements ? Leurs comptes déclarés à l'étranger ?

Dans la mesure où c'est au contraire la décentralisation et la robustesse qui sont les qualités les plus recherchées, la logique de validation entre pairs peut être utile dans la traçabilité quant à l'origine des fonds tout comme la recherche de systèmes financiers structurellement plus légers.

L'usage du blockchain dans le monde bancaire, s'il est très sérieusement envisagé voire déjà implémenté, l'est dans des niches et des applications très particulières. On pense notamment à la possibilité de rendre traçable l'origine des fonds (dans le cadre d'une politique de lutte anti-blanchiment), de pouvoir tenir à jour des registres d'actionnaires qui permettent de prendre en compte les participations croisées (je possède 10 % de l'entreprise X et 7 % de l'entreprise Y qui possède 35 % de l'entreprise X...).

Dans le futur, on pense aux économies d'échelle que pourrait représenter une base dédiée à l'identification des clients, partagée entre les banques, construite sur la technologie blockchain. A ce jour, en effet, l'identification des clients (preuve de l'identité) est une obligation bancaire qui est coûteuse à mettre en place. Chaque banque y travaille de son côté, ce qui est pour le moins inefficace.

La technologie blockchain est également pressentie, voire déjà utilisée pour faciliter le développement d'un marché secondaire de crowdfunding ou pour permettre le partage et l'authentification de documents (commerciaux, légaux,...).

Bien entendu, c'est dans le domaine des monnaies et des paiements que la technologie

blockchain connaît ses applications les plus populaires, puisque les monnaies cryptées Bitcoin, Ethereum, et les levées de fonds qui se basent sur certaines « crypto-monnaies » (en majorité Ethereum) et abrégées ICO (Initial Coin Offering) en sont les représentants les plus médiatisés.

Financité y reviendra plus en détail dans d'autres analyses à paraître en 2018, à suivre donc.

Olivier Jérusalmy

Mars 2018

Si vous le souhaitez, vous pouvez nous contacter pour organiser avec votre groupe ou organisation une animation autour d'une ou plusieurs de ces analyses.

Cette analyse s'intègre dans une des 3 thématiques traitées par le Réseau Financité, à savoir :

Finance et société : *Cette thématique s'intéresse à la finance comme moyen pour atteindre des objectifs d'intérêt général plutôt que la satisfaction d'intérêts particuliers et notamment rencontrer ainsi les défis sociaux et environnementaux de l'heure.*

Finance et individu : *Cette thématique analyse la manière dont la finance peut atteindre l'objectif d'assurer à chacun, par l'intermédiaire de prestataires « classiques », l'accès et l'utilisation de services et produits financiers adaptés à ses besoins pour mener une vie sociale normale dans la société à laquelle il appartient.*

Finance et proximité : *Cette thématique se penche sur la finance comme moyen de favoriser la création de réseaux d'échanges locaux, de resserrer les liens entre producteurs et consommateurs et de soutenir financièrement les initiatives au niveau local.*

Depuis 1987, des associations, des citoyens et des acteurs sociaux se rassemblent au sein du Réseau Financité pour développer et promouvoir la finance responsable et solidaire.

Le Réseau Financité est reconnu par la Communauté française pour son travail d'éducation permanente.