ceis

JANVIER 2018

BLOCKCHAIN : ETAT DES LIEUX ET PERSPECTIVES

Michel Benedittini
Amélie Rives

D'après une étude réalisée pour la DGRIS du Ministère des Armées avec la participation de Henri d'Agrain, Pierre Gérard, Eric Larchevêque, Renaud Lifchitz.

Les notes stratégiques

L'INTELLIGENCE DE LA DÉCISION

LES NOTES STRATÉGIQUES

Notes d'étude et d'analyse

TABLE DES MATIÈRES

TABLE DES MATIÈRES

1. INTRODUCTION

Consacrée « Méga Tendance » par le World Economic Forum en septembre 2015[1] et présente au cœur des débats qui se sont tenus à Davos au début de l'année 2016[2], la blockchain n'en finit pas de faire parler d'elle[3]. Popularisée par son application la plus répandue, la crypto-monnaie Bitcoin, la blockchain est souvent présentée comme une technologie révolutionnaire qui promet de bouleverser nos modes de vie et nos modèles économiques. Pour certains experts, elle représente même un potentiel égal à celui de certains standards clés de l'Internet comme HTTP (Hypertext Transfert Protocol) ou TCP-IP (Transmission Control Protocol / Internet Protocol). Selon eux, le « phénomène blockchain » pourrait donc connaître un développement analogue à celui qu'ont connu l'Internet et l'émergence du web dans les années 1980 et 1990.

Signe de l'engouement qu'elle suscite, la blockchain fait l'objet d'expérimentations industrielles de plus en plus nombreuses et dans des secteurs très variés. Si celles-ci sont pour la plupart portées par des start-ups, les grands acteurs de la banque et de la finance étudient également les possibilités d'appliquer la blockchain à certaines procédures collaboratives. Le phénomène blockchain séduit même désormais les États, qui s'intéressent aux apports potentiels de la blockchain pour la puissance publique et pour les forces armées. Des recherches en ce sens sont menées par des organisations comme la DARPA aux États-Unis, ou l'agence de communication et d'information de l'OTAN (NCIA).

Mais à l'instar de beaucoup d'innovations technologiques, la blockchain court aujourd'hui le danger de devenir un simple « buzzword[4] » sans être toutefois toujours bien comprise par ceux qui en font la promotion. Le développement de cette technologie dont les usages ne sont pas encore matures suscite en effet confusion et emballement. D'où la nécessité de bien comprendre ce qui se cache derrière cet objet technologique complexe, au croisement de l'informatique, de la cryptographie et de la théorie des jeux.

---

1 *http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf*
2 *Financial Times - BLOCKCHAIN debate eclipses Basel III at Davos – 21/01/2016*
3 *R. Contri - Davos 2016: Will BLOCKCHAIN be the tipping point for financial services disruption? – Deloitte Blog*
4 *BLOCKCHAIN France (coll) - La BLOCKCHAIN décryptée – les clefs d'une révolution – NetExplo Observatory juin 2016*

2. DÉFINITION

2.1. GENÈSE

Clé de voûte de la monnaie virtuelle Bitcoin et plus généralement des crypto-monnaies, la blockchain a été théorisée dès 2008 par un inconnu (ou un groupe inconnu) identifié sous le pseudonyme de Satoshi Nakamoto, qui en a posé les principes fondateurs.

Le Bitcoin et le système blockchain qui le sous-tend sont nés d'une défiance croissante vis-à-vis des institutions et des banques[5], portée par la crise financière de 2008 qui a remis à l'ordre du jour la question du rôle et de la responsabilité des régulateurs. Le débat engendré par l'ampleur de la crise a bousculé les banques centrales. Il a remis en question leur monopole d'émission, manifestation par excellence du pouvoir régalien et clé de voûte de la politique monétaire. Ce contexte a contribué à encourager le mouvement de réappropriation de la monnaie par les citoyens[6] (monnaies locales, …).

C'est dans ce contexte qu'est née la blockchain, avec pour vocation première d'éliminer, dans la réalisation de transactions monétaires, l'intermédiaire que constituent les « tiers de confiance » auxquels on fait finalement de moins en moins confiance : sociétés, organismes, régulateurs, administrations... L'idée derrière la « désintermédiation » étant à la fois de faciliter les échanges, de les rendre plus rapides et d'en réduire le coût de façon significative, et ce en apportant les mêmes garanties de fiabilité, de sécurité, de confidentialité et d'auditabilité des transactions que les tiers de confiance.

En d'autres termes, la blockchain a été conçue pour résoudre le problème dit « des généraux byzantins[7] », en permettant à un nombre indéfini de participants de coordonner leurs efforts sans se faire confiance a priori et sans passer par une autorité centrale. Elle repose donc sur un algorithme qui permet aux parties d'obtenir un consensus de manière distribuée, et ce en créant une situation d'équilibre telle que la théorie de Nash, c'est à dire une situation dans laquelle l'ensemble des choix faits par plusieurs joueurs, qui connaissent leurs stratégies réciproques, devient stable du fait qu'aucun ne peut modifier seul sa stratégie sans affaiblir sa propre position.

---

[5] *P. Noizat – Imaginer une nouvelle devise – in Bitcoin Book édition 2012*
[6] *F. Bosqué – Les monnaies citoyennes – Editions Yves Michel 2014*
[7] *L. Lamport, R.Shostak et M. Pease, « The Byzantine Generals Problem », ACM Transactions on Programming Languages and Systems, vol. 4, no 3, *juillet 1982*

2.2. DÉFINITION

La blockchain, c'est donc d'abord un système de stockage et de partage de données, transparent, sécurisé, et fonctionnant sans organe central de contrôle. Ces échanges, auxquels il sera fait référence sous le terme générique de « transactions », ne sont pas limités au domaine monétaire et peuvent concerner des informations de toute nature.

Par extension, une blockchain constitue une base de données distribuée (partagée par ses différents utilisateurs, sans intermédiaire) qui contient l'historique infalsifiable et horodaté de toutes les transactions qui y ont été enregistrées par ses utilisateurs depuis sa création.

On considère donc que l'on peut parler de blockchain quand trois éléments sont réunis :

1. le principe d'une chaîne, cumulative et séquentielle, de blocs liés entre eux par un chaînage de signatures numériques,

2. un consensus entre la majorité des participants à la blockchain sur la validité des transactions qui leur sont soumises,

3. une architecture distribuée, c'est à dire un fonctionnement en réseau utilisant la technologie de pair à pair (P2P, « Peer-to-peer »).

Plus précisément, et c'est en cela que la blockchain est une réelle innovation, il s'agit d'une combinaison de technologies informatiques et cryptographiques qui permettent d'assurer une confiance inaltérable dans la validité et l'intégrité des informations échangées et stockées, et qui garantit la résilience du système : Peer-to-peer, cryptographie asymétrique et fonctions de hachage.

Cette définition permet donc d'écarter les approches présentant la blockchain comme un simple « protocole informatique ». Elle permet aussi de détacher la blockchain du Bitcoin, auquel elle est pourtant intimement liée puisqu'il en est toujours la seule application largement utilisée et que c'est son code, libre et gratuit, qui sert le plus souvent de référence et de base à la création de nouvelles blockchains.

On peut en effet parler de blockchain dès que ces trois briques technologiques sont réunies, quelles que soient les caractéristiques particulières de chacune dont on verra qu'elles sont toutes paramétrables. Nous verrons ainsi qu'il existe plusieurs types de blockchains aux caractéristiques et avantages spécifiques, qui permettent en théorie une grande diversité d'applications hors du domaine monétaire dès lors qu'il s'agit d'assurer tout ou partie des fonctions suivantes :

- enregistrer et certifier des transactions et l'ordre dans lequel elles ont été validées,

- garantir la parfaite intégrité de leur contenu,

- partager la vision des transactions validées et assurer la résilience du système.

2.3. PRINCIPES DE FONCTIONNEMENT

Le principe de la blockchain consiste à lier (chaîner) un ensemble de transactions dont la validité a été vérifiée, et qui sont enregistrées dans des blocs de façon telle que le bloc en faisant référence au bloc n-1, la modification d'un bloc modifierait l'ensemble de la chaîne, ce qui rendrait immédiatement visible une tentative de modification ou de fraude et permettrait d'empêcher rapidement la propagation d'erreurs sur le principe de l'autorégulation.

On peut distinguer plusieurs grandes étapes dans un échange de données via la blockchain :

2.3.1. LA TRANSACTION

L'utilisateur souhaitant partager des données via une blockchain crée, depuis l'interface de cette blockchain, un compte auquel est associé une adresse (éventuellement « pseudonyme ») qui lui est propre et qui peut être si nécessaire renouvelée à chaque transaction. L'utilisateur envoie alors les informations à l'adresse de son interlocuteur. Des procédés de cryptographie asymétrique protègent l'intégrité des échanges, garantissent l'authentification de l'expéditeur et du récepteur, et assurent si nécessaire la confidentialité des données.

2.3.2. VÉRIFICATION ET VALIDATION DES TRANSACTIONS

La transaction est ensuite soumise à l'ensemble des nœuds du réseau peer-to-peer. L'un d'eux vérifie alors la validité de la transaction, c'est à dire qu'il s'assure, le cas échéant, que l'expéditeur est bien propriétaire de ce qu'il envoie et que le récepteur en est bien le correspondant désigné. Il ajoute ensuite la transaction validée à un bloc de transactions.

Avant d'être ajouté à la blockchain, le bloc en question doit à son tour être validé par le nœud qui le propose. Il doit pour ce faire résoudre un problème cryptographique ou informatique particulièrement difficile prenant la forme d'une preuve de calcul ou d'enjeu (voir 2.4.2).

Il est alors généré pour chaque bloc ainsi validé une empreinte unique reposant sur une fonction de hachage. L'empreinte d'un bloc validé n intègre l'empreinte du bloc précédent n-1. C'est le principe du chaînage, qui rend impossible toute modification d'un bloc donné sans devoir modifier également l'ensemble des blocs ultérieurs. Le chaînage garantit donc à la fois l'intégrité et l'ordre des transactions.

Comme le système part du principe que les nœuds du réseau peuvent être défectueux ou frauduleux, la validité d'un bloc de transactions doit ensuite être confirmée par la majorité des nœuds avant qu'il ne soit ajouté à la chaîne.

Un bloc validé par un nœud est donc soumis à tous les autres. Ils vérifient d'abord de nouveau que chaque transaction qui le constitue est valide, puis que le nouveau bloc s'intègre bien à l'extrémité actuelle de sa blockchain en en comparant l'empreinte avec celle calculée par le nœud qui l'a diffusé. En d'autres termes, ils vérifient que le résultat du problème cryptographique ou informatique résolu par le nœud qui a soumis le bloc au réseau, est exact. En cas de réussite, le nouveau bloc est ajouté localement à la blockchain par chaque nœud.

C'est en cela que l'on peut parler de consensus : si plus de 50% des nœuds du réseau valident le bloc, cette version de la blockchain devient la référence. Le bloc est ainsi stocké dans un registre décentralisé, qui techniquement prend la forme d'un vaste réseau constellé de « nœuds » formés par des serveurs qui hébergent chacun une réplique identique de la chaîne de blocs. Les transactions, ainsi enregistrées sur tous les nœuds du réseau, ne peuvent plus être ni écrasées ni modifiées et deviennent alors infalsifiables tout en restant facilement vérifiables.

2.4. PARAMÈTRES DÉTERMINANTS

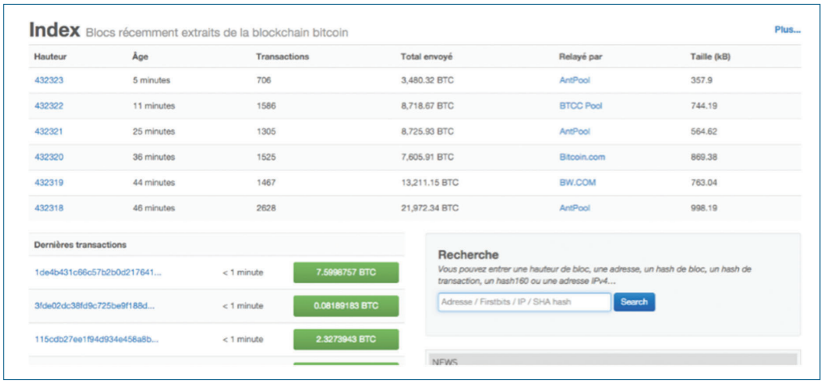
Au-delà des éléments constitutifs d'une blockchain, certains paramètres structurants définis lors sa création permettent de fait d'en orienter sinon d'en déterminer le champ d'application et les usages potentiels : les accès et autorisations, les modes de validation et de chaînage des transactions, et l'objet de la blockchain.

2.4.1. LA TRANSACTION

LES BLOCKCHAINS PUBLIQUES

Les blockchains publiques sont ouvertes, consultables et utilisables par tout individu depuis leurs interfaces Internet, sans barrière à l'entrée. Pour effectuer une transaction ou partager des données sur une blockchain, il suffit à l'utilisateur de choisir, parmi les solutions existantes, un « portefeuille » (appelé aussi parfois porte-clés, ou *wallet* en anglais) qui lui permettra à la fois de conserver ses clés privées de façon sécurisée et de générer une adresse unique pour envoyer et recevoir des données. L'historique des transactions est accessible à tous, non seulement aux utilisateurs mais également à tout visiteur de la plate-forme. De même, chacun peut se constituer en nœud et ainsi participer à la validation des transactions, à leur regroupement dans un bloc et au chaînage des blocs. En d'autres termes, une blockchain publique n'est soumise à aucune autorisation de lecture ou d'écriture.

Ces blockchains sont principalement destinées à des échanges entre individus, constituant actuellement le plus souvent des transactions monétaires, mais pouvant être d'autre nature. De fait, la blockchain publique la plus connue et la plus mature à ce jour est celle du Bitcoin, qui permet d'effectuer des transactions monétaires :



Interface Internet de la blockchain du Bitcoin

LES BLOCKCHAINS PRIVÉS

Contrairement aux blockchains publiques, les blockchains privées ne sont pas accessibles à tous car elle sont soumise à des droits de lecture et d'écriture différenciés, accordés de manière centralisée par l'entité créatrice de la blockchain. Elle peuvent être déployées dans un réseau fermé sur différents équipements informatiques appartenant à une seule et même entité, une entreprise ou toute autre organisation. La validation et le chaînage des transactions peuvent être centralisés et réservés à l'autorité créatrice ou à un nœud désigné par avance, ou être attribués à plusieurs nœuds préalablement autorisés.

Ces blockchains ne nécessitent pas de crypto-monnaie sous-jacente car elles ne supposent pas de rémunérer les nœuds qui valident les blocs. Elles sont particulièrement adaptées à des usages internes à une entité, organisation, entreprise, afin de faciliter le travail collaboratif ou le partage de fichiers.

LES BLOCKCHAINS DE CONSORTIUM

Une blockchain de consortium est une blockchain privée dans son fonctionnement, mais dont la gouvernance est partagée entre diverses entités ayant un intérêt à utiliser une blockchain commune. Cette gouvernance attribue notamment les droits d'effectuer des transactions, définit quels sont les nœuds chargés de valider les transactions et de constituer les blocs, ainsi que la nature et les modalités de la recherche du consensus.

Les blockchain privées ou de consortium sont parfois qualifiées de « distributed ledger technology » (DLT) par les puristes qui considèrent qu'on ne peut parler de blockchains que pour les technologies de registres partagés distribués entre des utilisateurs qui n'ont a priori aucune raison de ce se faire confiance. Une autre approche consiste à considérer ces différents types de blockchains comme étant destinés à des usages particuliers et qu'elles peuvent être complémentaires. Les blockchains publiques sont particulièrement adaptées à des applications consumer-to-consumer, alors que les blockchains privées et de consortium sont plus appropriées dans le cas d'applications business-to-business, notamment parce qu'elles facilitent le travail collaboratif.

Les blockchains publiques, utilisées par des acteurs qui a priori ne se font pas confiance, présentent donc un modèle de consensus totalement distribué, réalisé par des « mineurs » qui valident les transactions de façon totalement indépendante les uns des autres. Le besoin de confiance étant un enjeu moindre dans les blockchains privées du fait que les différents rôles ne sont assurés que par des utilisateurs et des nœuds dûment autorisés et authentifiés, le type de consensus n'est pas distribué, mais centralisé, ou décentralisé si l'autorité centrale en délègue l'exécution à certains nœuds précis.

Il est possible de relier plusieurs blockchains, éventuellement de natures différentes, grâce à une « sidechain », ou « chaîne latérale », par exemple pour assurer et tracer des transactions entre ces blockchains, ou répartir la charge de validation entre elles.

2.4.2. LES MODES DE VALIDATION ET DE CHAÎNAGE DES TRANSACTIONS

On distingue le mode de validation distribué, caractéristique des blockchains publiques, et le mode de validation centralisé (ou décentralisé), qui caractérise les blockchains privées.

MODÈLE DISTRIBUÉ

Les blockchains publiques présentent un modèle distribué, dans lequel la vérification et la validation des transactions, la création des blocs et leur ajout à la blockchain, sont effectués par certains nœuds du réseau que l'on appelle les mineurs. Les mineurs sont d'abord chargés de vérifier la validité d'un échange, en s'assurant par exemple, dans le cas des blockchains monétaires, que chacun ne dépense que son propre argent et qu'une seule fois. Il s'agit aussi de vérifier l'authentification de l'expéditeur et l'intégrité du contenu de son message.

Les mineurs valident une transaction soit par une « preuve de travail » qui consiste à résoudre un problème cryptographique, soit par une « preuve de participation » ou « preuve de détention » (« proof of stake »), qui consiste par exemple à prouver la possession d'une certaine somme de cryptomonnaie ou d'actifs gérés par la blockchain en question.

Pour être efficace, la preuve de travail doit être asymétrique : difficile à résoudre, mais facile à vérifier. Dans la blockchain du Bitcoin par exemple, la preuve de travail est un calcul mathématique complexe consistant à trouver un nombre aléatoire appelé « nonce » et donnant par calcul un grand nombre de « zéros » préfixant le hash du bloc courant. La difficulté de travail est donc liée à la probabilité de trouver ce nombre dès la première tentative, obligeant potentiellement à répéter plusieurs centaines de milliards de fois l'opération pour espérer résoudre le problème. Chez DataCoin, il s'agit du calcul de nombres premiers. Dans la blockchain d'Ethereum, il s'agit d'une « preuve d'enjeu ». D'autres comme Primecoin utilisent un système hybride qui mêle plusieurs types de preuves de travail.

Les mineurs peuvent être rémunérés pour effectuer cette tâche, le plus souvent par émission d'un quantum d'une crypto-monnaie attachée à la blockchain en question. Ainsi, si certaines blockchains publiques sont fondées sur des crypto-monnaies car elles ont pour objet les transactions monétaires, d'autres ne sont qu'adossées à des crypto-monnaies sous-jacentes pour inciter et rémunérer les mineurs. Elles peuvent alors se doter de leur propre crypto-monnaie ou être liées à d'autres crypto-monnaies.

MODÈLE CENTRALISÉ / DÉCENTRALISÉ

Le principe de la « preuve de travail » n'est en général pas une nécessité, notamment dans le cas des blockchains privées où le processus d'approbation peut être limité à un acteur unique. D'autres types de consensus sont plus adaptés aux blockchains privées ou de consortium. La « preuve d'autorité », par exemple, consiste simplement en l'autorisation par l'organe central qui gère la blockchain, d'un ou plusieurs nœuds à ajouter des blocs dans la blockchain. L'ajout de blocs n'est donc plus distribué mais décentralisé.

Quant à la délégation de preuve de possession (DPOS), applicable aux blockchains tant publiques que privées, elle utilise généralement un système de réputation pour élire un groupe limité de personnes ayant le droit d'inscrire des blocs à tour de rôle de façon aléatoire. Tous les membres du réseau peuvent voter selon un mécanisme qui pondère les votes en fonction de leur rôle et/ou de leur influence dans le réseau. Un participant au comportement jugé suspect peut être exclu par les autres votants, et un participant qui ne produirait pas le bloc dans le temps imparti peut voir sa tache attribuée au prochain participant sur la liste.

2.4.3. L'OBJET

Si toutes les blockchains permettent par définition le transfert, le partage et le stockage d'informations, certaines servent aussi de base à l'exécution d'applications plus complexes qui élargissent son champ d'application et sa portée.

Certaines contiennent en effet des instructions beaucoup plus complexes, conditionnelles et programmables. On parle alors de « contrats intelligents » (« *smart contracts* »). Ces contrats sont des protocoles informatiques autonomes qui s'exécutent automatiquement à la réalisation de certaines conditions d'engagement, en prenant en compte l'ensemble des conditions et des limitations qui avaient été programmées dans le contrat à l'origine. Ces *smart contracts* sont nourris par des « oracles », services qui permettent d'entrer une donnée extérieure dans la blockchain pour permettre à un smart contract de s'exécuter en fonction de cette donnée. C'est par exemple l'objet de la blockchain d'Ethéreum, qui se distingue de la blockchain du Bitcoin par un langage de programmation Turing complet, et qui lui permet précisément d'exécuter des *smart contracts*.

L'attaque dont a été victime en juin 2016 l'une des applications qui s'exécutent dans Ethereum, la DAO, montre que des erreurs d'écritures ou des bugs dans les *smart contracts*, qui sont le fondement même de ces applications, peuvent remettre en question leur fonctionnement alors même que la chaîne de bloc elle-même n'est pas en cause et n'est pas affectée.

2.5. VARIABLES AJUSTABLES

Au-delà des éléments constitutifs et des paramètres déterminants, une série de variables ajustables permettent d'adapter la blockchain à une multitude d'usages.

2.5.1. TAILLE DES BLOCS ET NOMBRE DE TRANSACTIONS PAR MINUTE

La taille des blocs dépend du volume de transactions qu'ils intègrent, et a une incidence sur la durée du processus de validation des blocs. Elle est donc paramétrée et adaptée à l'usage auquel est destinée la blockchain en question.

2.5.2. CHIFFREMENT

Les mécanismes de cryptographie utilisés par toutes les blockchains assurent l'intégrité des données partagées et l'authentification de l'expéditeur. Si les exigences de confidentialité l'exigent, il est aussi possible de chiffrer le contenu des transactions.

2.5.3. TYPES DE DONNÉES ENREGISTRÉES

Si les applications les plus connues de la blockchain concernent des crypto-monnaies, les échanges contenant alors des empreintes de transactions monétaires, il est possible d'échanger sur la blockchain des données de toute nature selon l'objet de la blockchain : documents (sous forme d'empreinte ou dans leur intégralité), éléments de signature électronique et d'horodatage, algorithmes, données brutes, scripts constituant des *smart contracts* …

2.5.4. TEMPS DE VALIDATION

Le temps de validation est étroitement lié au choix du type de consensus et en particulier au type de preuve de travail/ de participation.

Dans les blockchains publiques où le consensus est distribué, tous les nœuds doivent vérifier et exécuter toutes les transactions de chaque bloc et ce quel que soit le type de consensus choisi, ce qui ralentit le processus de façon significative. Mais on note toutefois de fortes disparités entre les différents procédés. Par exemple, la blockchain Ethereum accepte un nouveau bloc toutes les 12 secondes alors que Bitcoin impose un temps de latence de 10 minutes.

2.5.5. RÉMUNÉRATION DES MINEURS

La rémunération des mineurs est optionnelle. Elle est souvent associée aux blockchains publiques car elle constitue pour ceux qui la touchent une incitation qui permet de faire fonctionner et perdurer le système. La rémunération est liée au mode de création et de livraison de crypto-monnaie. Les deux systèmes les plus aboutis et les plus matures, Bitcoin et Ethereum, diffèrent sur ce point : alors qu'Ethereum définit une quantité illimitée d'Ether et rémunère les mineurs à raison d'un montant stable de 5 Ether par bloc miné, les créateurs du Bitcoin ont limité le nombre final de Bitcoins en circulation à 21 millions, ce qui implique donc de diviser la rémunération des mineurs

par deux environ tous les 4 ans pour ne pas dépasser cette somme. Le gain décroissant des mineurs de la blockchain du Bitcoin représente d'ailleurs un véritable enjeu car il implique qu'ils ne seront un jour plus rémunérés par le système, et qu'il faut donc envisager d'autres mécanismes pour récompenser les mineurs. Les coûts pourraient alors être supportés par les utilisateurs, ce qui remettrait en cause l'un des principaux apports de la blockchain, à savoir le faible coût des transactions.

2.5.6. TAILLE DU RÉSEAU ET NOMBRE DE NŒUDS

Dans ces systèmes qui prennent la forme d'architectures décentralisées, il est très facile d'accroître ou de diminuer le nombre de participants. Il suffit pour cela de rajouter un nœud dans le réseau distribué. Dans les blockchain publiques, et selon la loi de Metcalfe, un grand nombre de nœuds garantit la force et la fiabilité du réseau car plus le nombre de participants est élevé, plus le consensus est difficile à atteindre, et plus les possibilités de fraude et de corruption sont faibles.

2.5.7. IDENTIFICATION DES UTILISATEURS

Contrairement à ce qui est souvent écrit, la plupart des blockchains existantes ne sont pas anonymes car elles reposent justement sur le principe de la transparence. L'identité des utilisateurs n'est cependant pas directement visible car ils peuvent choisir d'y apparaître sous pseudonyme. Mais il peut être relativement aisé de retracer les historiques de transactions d'un même pseudonyme ou d'une même adresse blockchain. Plusieurs sociétés comme Scorechain se spécialisent dans ce type d'activités. Il est aussi possible d'identifier les auteurs de ces transactions, ne serait-ce que parce que la plupart des achats de crypto-monnaies s'effectuent sur des plateformes d'échange officielles et régulées nécessitant de dévoiler des informations personnelles (pièce d'identité, preuves d'adresse, numéro de téléphone, mail, adresse IP…) et que les autorités sont habilitées, dans de nombreux pays, à solliciter les plateformes en question si besoin. On parle donc de pseudo-anonymat.

Il existe cependant certaines crypto-monnaie qui semblent garantir véritablement l'anonymat comme Monero (XMR), basée sur un protocole de seconde génération et dont, contrairement à la plupart des autres crypto-monnaies, le code n'est pas dérivé de celui du Bitcoin. Les transactions s'y effectuent grâce à des procédés cryptographiques dites « signatures de cercles » qui permettent à ses utilisateurs de signer électroniquement de façon anonyme un message ou un document.

2.5.8. LANGAGE DE PROGRAMMATION

On distingue deux grands types de langages de programmation. D'une part, les langages de programmation aux scripts binaires, caractéristiques des blockchains dont les crypto-monnaies sont l'objet principal, qui ne permettent d'effectuer qu'un nombre limité d'actions (l'argent est dépensé ou non dépensé). D'autre part, des langages de programmation plus complexes, comme le langage Turing complet (quasi-Turing dans le cas d'Ethereum), qui n'ont pas de limitations théoriques et permettent d'effectuer des actions plus sophistiquées, ainsi que la mise en place de clauses, de boucles et de programmes en boucles qui ouvrent la voie à des applications plus diverses.

2.6. APPORTS

Portée par une défiance croissante vis-à-vis des institutions et des banques, la blockchain devait apporter confiance et sécurité aux transactions financières grâce à des mécanismes de désintermédiation et de décentralisation.

Nous l'avons vu, les technologies qui la sous-tendent lui apportent d'indéniables garanties en termes de sécurité des transactions, de résilience du réseau et de réduction de coût, sur lesquelles il convient de revenir.

2.6.1. SÉCURITÉ DES TRANSACTIONS ET RÉSILIENCE

La sécurité peut être appréhendée à travers 4 caractéristiques : a) disponibilité, b) traçabilité, c) intégrité/non répudiation, d) confidentialité. La blockchain peut apporter des garanties sur ces 4 points.

La résilience du système blockchain à des tentatives d'attaques ou de fraude, étroitement liée à sa sécurité, est selon les experts comparable à celle d'Internet. Les blockchains publiques sont d'ailleurs attaquées en permanence, comme celle du Bitcoin qui héberge actuellement un fonds d'environ 7 milliards de dollars. Aucune à ce jour n'a abouti.

- **DISPONIBILITÉ** : dans la blockchain, la disponibilité des informations est garantie par leur caractère distribué et par la technologie P2P sur laquelle il s'appuie. Comme l'ensemble de la chaîne et l'intégralité de l'historique des transactions sont consultables sur tous les nœuds du réseau, l'information reste disponible même dans le cas où plusieurs nœuds de ce réseau sont défaillants ou disparaissent. Ce qui contribue à assurer la résilience du système.

- **LA TRAÇABILITÉ** est la conséquence de l'horodatage de toutes les transactions sur un registre distribué consultable par tous qui offre la possibilité de remonter l'ensemble de la chaîne pour retrouver l'historique des transactions.

- **L'INTÉGRITÉ ET L'INVIOLABILITÉ**, qui ont pour conséquence la non répudiation, découlent de l'inscription dans un bloc de transactions qui ne peuvent pas être écrasées ou modifiées et deviennent ainsi infalsifiables tout en restant vérifiables.

- **MÉCANISMES CRYPTOGRAPHIQUES :** les technologies de blockchain intègrent des mécanismes de signature des transactions et leur vérification. L'algorithme utilisé est le plus souvent ECDSA (« Elliptic Curve Digital Signature Algorithm »), qui joue un rôle crucial dans la technologie bitcoin par exemple. ECDSA assure aussi la génération des paires de clés (clé privée et clé publique) nécessaires aux signatures. Toute adresse bitcoin est dérivée d'une clé publique ECDSA. L'algorithme a été démontré comme sûr cryptographiquement et adopté comme norme internationale. Il repose sur des courbes recommandées par des organisations comme le NIST ou Certicom. La fonction de hachage SHA-256 est utilisée pour assurer la signature des blocs par exemple.

- **LA RÉSILIENCE :** elle repose d'abord sur le fait que la répudiation des déviants se fait naturellement dans un réseau blockchain car les blocs frauduleux se retrouvent rapidement sur une chaîne qui n'est acceptée par personne, et qui finit donc par disparaître.

En outre, dans ce système doté d'un mécanisme de consensus distribué, la majorité n'est pas déterminée sur le mode « un participant – une voix » comme pour un vote, car il serait alors trop aisé de créer des participants fantômes pour valider des transactions frauduleuses. La majorité de participants s'établit en fait par la plus grande puissance de calcul collective. Les tentatives de sabotage sont donc un exercice particulièrement difficile à réaliser dans un système distribué, ne serait-ce qu'en raison du coût d'une éventuelle attaque qui impliquerait de prendre le contrôle ou de faire tomber plus de 50% des nœuds du réseau. La puissance de calcul et la capacité de minage nécessaires seraient telles qu'une attaque réussie est inenvisageable à ce stade. Pour prendre l'exemple de la blockchain du Bitcoin, on estime que même si 90% de la capacité de minage du réseau était supprimée, la puissance de calcul installée serait des dizaines de fois plus importantes que les plus puissants supercalculateurs réunis. Une théorie, définie par la loi de Metcalfe, selon laquelle la sécurité d'un réseau augmente avec le nombre de ses nœuds.

Le véritable défi en termes de sécurité provient des points d'entrée sur le réseau, notamment l'ordinateur ou le périphérique non sécurisé de l'utilisateur. Certaines sociétés se sont donc spécialisées dans la sécurisation de ces points d'entrée aux différents réseaux blockchain.

2.6.2. RÉDUCTION DES COÛTS DE TRANSACTION

L'un des principaux apports de la blockchain est de réduire de manière drastique le coût des transactions dans un système qui permet de s'affranchir de nombreuses fonctions de back-office dont l'activité consiste à vérifier, valider et contrôler les transactions, quelle qu'en soit la nature.

2.6.3. AMÉLIORATION DE LA PRODUCTIVITÉ DES ÉCHANGES COLLABORATIFS

Conséquence de la réduction du coût des transactions, la blockchain permet d'une part d'améliorer la capacité des agents économiques de petite taille à travailler en réseau, et d'autre part de fluidifier les échanges entre les différents agents économiques. Ces deux aspects se traduisent par une réelle amélioration de la productivité des échanges collaboratifs, qui sont désormais l'une des composantes majeures de l'économie numérique.

2.7. LIMITES

2.7.1. TECHNOLOGIQUES

CAPACITÉ DES BLOCKCHAINS

Si le développement exponentiel des réseaux blockchains se poursuit et couvre des usages qui nécessiteront d'y enregistrer, non pas des transactions, mais des documents plus lourds, il pourrait rapidement se heurter à des problèmes de capacité. La taille de la base de données stockée sur de telles blockchains pourrait croître à un rythme exponentiel au cours des années, et nul ne sait ce qu'il adviendra si les serveurs constituant les nœuds n'ont plus la capacité nécessaire.

De même, de nombreuses blockchains restent limitées dans le nombre de transactions qu'elles peuvent effectuer par seconde, un problème notamment lié à la limitation de la taille des blocs. Certaines solutions sont déjà à l'étude pour faire évoluer la taille des blocs, ce qui permettrait de résoudre temporairement le problème. Une autre solution, encore au stade de l'expérimentation, notamment par la société Blockstream, consiste à rattacher des side-chains aux blockchains limitées, qui seraient horodatées et synchronisées avec la principale et permettraient donc d'accepter des charges de transactions plus importantes.

La fonction de hachage SHA-256 est utilisée pour assurer la signature des blocs par exemple.

COÛTS

En raison de la rémunération décroissante des mineurs dans certaines blockchains comme celle du Bitcoin, il est encore trop tôt pour savoir si la promesse de baisse des coûts pour l'utilisateur ainsi que celle de l'efficience pourront être tenues.

SÉCURITÉ

Autre incertitude liée aux développements technologiques, l'apparition à terme des ordinateurs quantiques qui pourraient rendre réel le risque de collision entre plusieurs adresses blockchain, et donc le risque de fraude. Mais ce risque est encore très mal évalué et il n'est pas possible à ce stade de le confirmer.

GOUVERNANCE TECHNIQUE

Une autre limite importante est liée à la problématique de la gouvernance technique qui est assurée par les forums et les groupes de développeurs, et qui a pour objectif le maintien en condition opérationnelle et de sécurité du protocole des différentes blockchains (protocole BIP en particulier pour le Bitcoin). Si ces groupes disparaissent, les développements dérivés du code source initial pourraient faire apparaître de nouvelles vulnérabilités non corrigées. À cet égard, rappelons la disparition de la solution TrueCrypt faute de son maintien à jour par la communauté qui l'avait développée.

Des doutes subsistent également sur la résilience des blockchains hébergées dans le *Cloud*, comme IBM par exemple le propose dans sa solution, du fait du risque que des nœuds en nombre important se retrouvent sur des serveurs physiques colocalisés et entretenus par un même opérateur, et puissent de ce fait tous tomber en cas d'attaque réussie sur ce *Cloud*. De manière générale, il n'est pas certain que la blockchain apporte un véritable avantage en matière de coût de possession, de performances ou de sécurité sur un système de distribution basé sur un serveur de fichiers centralisé classique et une preuve d'intégrité assurée à l'aide de certificats provenant d'une PKI.

2.7.2. HUMAINES

Obstacles de nature humaine ensuite, avec notamment la question de la gouvernance, comme évoqué plus haut. Se pose par exemple la question de l'évolution, en fonction des besoins, du modèle des blockchain publiques, puisqu'il n'existe pas d'autorité centrale en mesure de prendre des décisions. D'où le débat actuel et non résolu qui oppose spécialistes et experts sur la question de la modification de la taille des blocs et/ou des transactions pour permettre de dépasser les limitations techniques de la blockchain. Le codage des règles qui régissent des organisations humaines gérées par des algorithmes soulève enfin des difficultés qui sont encore plus prégnantes dans les blockchains où le code est force de loi.

2.7.3. JURIDIQUES

Obstacles juridiques enfin, puisque l'usage des blockchains dans le cadre de trafics ou d'activités illégales ont amené certains décideurs à proposer l'interdiction des crypto-monnaies. Cette mesure remettrait en cause l'existence même des blockchains publiques qui, indépendamment de leur fonction principale, sont encore intimement liées à l'existence d'une crypto-monnaie sous-jacente. Sans aller jusque-là, la puissance publique s'intéresse déjà à la blockchain pour en surveiller les échanges et certains de ses utilisateurs. On peut donc s'attendre à ce que certains États tentent aussi d'en contrôler ses usages.

La blockchain, ou plutôt, nous l'avons vu, les blockchains, permettent donc le partage et le stockage sécurisé, auditable et transparent de données ou d'informations de toute nature, sur un réseau dont la résilience n'a plus à être prouvée. Parce qu'elles peuvent prendre plusieurs formes (publiques, privées ou de consortium), elles permettent de répondre à des besoins différents pour des usages nécessitant de réunir les 4 critères de sécurité simultanément mais pas forcément dans la même mesure. De fait, les blockchains font l'objet de nombreuses expérimentations industrielles, et les start-ups plaçant ces technologies au cœur du développement de nouveaux produits ou services ne cessent de se multiplier, inventant ainsi de nouveaux modèles économiques. La blockchain semble même avoir investi le secteur de la défense, puisque des organisations comme la DARPA aux États-Unis ou l'OTAN étudient les possibilités de développement de la blockchain en milieu militaire.

3. APPLICATIONS GÉNÉRIQUES DE LA BLOCKCHAIN

Si les initiatives visant à identifier de nouvelles applications pour la blockchain se multiplient, elles restent pour une grande majorité au stade de l'expérimentation et du prototype. Seules peut-être la blockchain de Bitcoin et celle d'Ethereum ont atteint un nombre suffisant d'utilisateurs pour que l'on puisse parler de solutions abouties.

D'autre part, la multiplication d'initiatives et expérimentations dans ce domaine suggère que les technologies de la blockchain sont dans la pente ascendante du « hype cycle » du Gartner : après l'émergence de ces technologies reconnues comme prometteuses, on assiste désormais à un emballement médiatique autour de la blockchain et à une prolifération rapide et tous azimuts de start-ups créées pour développer des produits et solutions qui y sont consacrées. Elles génèrent ainsi de réelles attentes quant à son potentiel, qui peuvent être suivies d'une période de relative désillusion si les produits disponibles ne répondent pas à ces espoirs. À terme, seuls les usages les plus pertinents se pérenniseront au fur et à mesure que seront reconnus les véritables avantages de la blockchain, ouvrant la voie à un développement solide et progressif du marché. Il convient donc à ce stade de rester prudent, et de considérer que la prolifération des initiatives autour de la blockchain reflète surtout les tâtonnements technologiques et la recherche d'usages pertinents plutôt que les applications fiables et durables de technologies matures.

Les projets à l'étude témoignent toutefois de l'indéniable potentiel de la blockchain. Pour certains types d'usages, c'est la propriété de désintermédiation de la blockchain qui représente le principal avantage, avec les conséquences qui ont déjà été mentionnées : rapidité des échanges et réduction de leur coût, élimination des tiers de confiance. C'est le cas pour les applications visant à utiliser la blockchain comme un moyen de paiement décentralisé. Dans d'autres cas, c'est une approche de la blockchain comme un grand registre distribué et inviolable, capable de conserver la trace inaltérable, permanente et décentralisée de tous types d'informations, qui est au cœur des usages.

3.1. MOYENS DE PAIEMENT DECENTRALISÉS

C'est le cas d'usage le plus classique et le plus connu de la blockchain puisque c'est celui qui a été à l'origine du phénomène blockchain. Désormais, les crypto-monnaies se comptent par centaines dont la plus sérieuse et établie, le fameux Bitcoin. Elles ont chacune des particularités qui les distinguent de leurs consœurs, mais leur fonctionnement reste le même : elles permettent à leurs utilisateurs d'effectuer des transferts monétaires dont les références sont stockées sur un grand registre distribué et auditable.

Les services de paiement sont en effet le domaine dans lequel la blockchain a commencé à se développer et celui dans lequel les expérimentations sont les plus concluantes. Tout d'abord, la désintermédiation financière qu'elle induit permet de réduire fortement les coûts et les délais des transactions. Dans le cas du Bitcoin, un particulier peut en effet envoyer de l'argent partout dans le monde, très rapidement et presque gratuitement, alors que les transferts d'argent par virement bancaire peuvent être longs et coûteux.

Les crypto-monnaies et les possibilités offertes par la blockchain sont également étudiées par les banques et instituts financiers. Ceux-ci voient dans la désintermédiation un moyen de réduire drastiquement les coûts et délais de transaction. Ce scenario est notamment au cœur d'une initiative poursuivie par un consortium international initialement composé d'une soixantaine de banques et d'établissements financiers de premier plan, parmi lesquels Goldman Sachs, JP Morgan, la Société Générale, BNP Paribas et UBS qui ont décidé de s'associer en septembre 2015 pour étudier les usages de la blockchain autour de l'entreprise de Fintech américaine R3CEV, spécialisée dans les transferts d'actifs et la sécurité cryptographique. Ce consortium s'appuie sur R3CEV pour réaliser des expérimentations, des illustrateurs de besoin et des preuves de concept. Toutefois, l'absence de résultats probants a conduit plusieurs membres, dont Goldman Sachs, à sortir du consortium début décembre 2016.

3.2. SERVICES DE MESSAGERIE

Très proches du fonctionnement des blockchains liées aux crypto-monnaies et destinées aux transactions monétaires, certaines applications comme Bitmessage, un protocole de communication en pair à pair décentralisé et chiffré, permettent d'échanger des messages chiffrés avec un ou plusieurs correspondants au travers du réseau Tor.

3.3. ECHANGES DE SERVICE : L'UBERISATION D'UBER ?

Les technologies de la blockchain peuvent également être utilisées entre particuliers pour des échanges de services complètement décentralisés et détenus par la communauté de leurs utilisateurs. Plusieurs expérimentations ont actuellement lieu dans ce domaine. La start-up israélienne La Zooz, par exemple, propose un service de co-voiturage entièrement repensé sur la base de la blockchain, un service *open source* qui permet aux conducteurs et aux passagers de se connecter en temps réel pour remplir les sièges vides des conducteurs, sans avoir à s'appuyer sur un acteur intermédiaire pour la mise en relation puisque tout passe par une plate-forme autogérée. Zooz rémunère ses conducteurs en jetons appelés « Zooz » (une monnaie basée sur le bitcoin) stockés sur une blockchain.

3.4. LUTTE CONTRE LA CRIMINALITÉ PAR L'ENREGISTREMENT ET LA TRACABILITÉ LES BIENS DE VALEUR

Il s'agit d'enregistrer, dans une blockchain publique, les caractéristiques d'un bien précieux. L'usage de la blockchain dans la traçabilité des biens est notamment pertinent pour lutter contre la fraude, la contrefaçon, les trafics internationaux ou les vols. Plusieurs domaines ont déjà fait l'objet de réalisations concrètes : généalogies de chevaux de sang, origines de pierres précieuses, certifications d'objets de luxe,

enregistrements d'œuvres d'art ... D'autres sont à l'étude, visant par exemple à lutter contre les copies portant atteinte à la propriété intellectuelle d'œuvres numériques (musiques, films…).

À titre d'exemple, Everledger est une société qui utilise la blockchain pour combattre la fraude dans le domaine du luxe. Le premier marché sur lequel s'est positionné Everledger est celui du diamant, où la fraude coûterait près de 50Md$ par an aux assureurs[8]. Il n'existerait pas, en effet, de base de données centralisée fiable qui permette de tracer l'origine des diamants et la suite des transactions. Everledger propose d'utiliser la blockchain pour bâtir un livre ouvert de transactions qui relève l'ensemble des données qui identifient correctement chaque diamant (les 4 C's – color, clarity, cut, carat – mais aussi les 40 méta-points qui le caractérisent spécifiquement).

3.5. CERTIFICATION DE TITRES

La blockchain est particulièrement adaptée à l'enregistrement de titres dont la propriété doit être attribuée de manière exclusive et infalsifiable à son titulaire. Les cas d'usage se sont multipliés et comptent par exemple les titres immobiliers ou des titres et diplômes universitaires.

Ainsi, la société Bitproof enregistre des titres immobiliers et universitaires dans la blockchain du Bitcoin afin de les rendre publics et infalsifiables. L'université de Nicosie expérimente d'ailleurs actuellement les premiers certificats universitaires dont l'authenticité peut être vérifiée sur le registre du Bitcoin, tandis qu'en France, le pôle Léonard de Vinci expérimente la certification des diplômes dans une blockchain avec la société Paymium.

De même, le gouvernement du Honduras a annoncé en mai 2015 un accord avec une entreprise texane spécialisée dans les usages innovants de la Blockchain, Factom Inc., afin de mettre en place à l'échelon national un outil de cadastre numérique basé sur la Blockchain permettant d'identifier les possessions de chacun à l'intérieur des frontières nationales et de lutter contre la fraude.

3.6. GESTION DE FICHIERS SÉCURISÉS

Certaines applications, proches des applications de type « messagerie », proposent des solutions hautement sécurisées de gestion et de partage collaboratif de documents, qui en garantissent la confidentialité et l'intégrité.

C'est le cas de « Keeex ChatOps », de la start-up KeeeX, une solution utilisable sur serveur, poste de travail ou terminal mobile, qui sécurise en confidentialité et en intégrité documents, conversations instantanées, emails et plus largement tout contenu numérique, et qui permet un travail itératif (versions successives par exemple) et collaboratif (comme entre clients et fournisseurs) ainsi que des liens directs vers d'autres documents pouvant être situés dans un *Cloud* (documents de référence entre autres). Chaque contenu « keeexé » se voit ainsi associé un identifiant unique, produit d'un hash cryptographique SHA 256, qui prouve son authenticité de façon permanente

---

[8] *Source : http://www.finyear.com/La-blockchain-une-technologie-avec-un-potentiel-immense-Partie-1_a34432.html*

et qui peut servir de pointeur vers d'autres fichiers tout en fournissant un index pour les moteurs de recherche. Au lieu d'être transférés vers les serveurs de Keeex, les données des utilisateurs et leurs documents sont auto-sécurisés et organisés en une chaîne infalsifiable selon le modèle des blockchains monétaires. Cette solution fonctionne donc sans serveur de fichier centralisé. Les usages et avantages d'un tel système sont multiples : il permet d'abord aux utilisateurs de créer des chaînes de documents et des versions d'un même document qui sont tout à la fois infalsifiables, signés par leurs rédacteurs et authentifiables. Ils sont compatibles avec le web, permettant d'accéder à un original éditable comme à sa plus récente version. Les professions réglementées, notamment les avocats, comptables, notaires et les entreprises du secteur tertiaire, ont montré un intérêt certain pour cette solution.

De même, la police néerlandaise s'intéresse depuis juillet 2015 à deux services *Cloud* basés sur la blockchain : storj.io et filecoin.io, grâce auxquels un document sauvegardé sur le *Cloud* sera fractionné en de multiples morceaux stockés à différents endroits. L'accès au document est garanti de manière cryptographique, dans une blockchain, au seul propriétaire des données et à ceux à qui il donne un droit d'accès. Il s'agit ici d'un modèle hybride qui stocke les données sur une blockchain publique visible par tous sans restriction, mais n'en autorise la reconstitution qu'aux seules personne autorisées.

3.7. SOUSCRIPTION ET DÉCLENCHEMENT D'ASSURANCES

Les services financiers et le monde de l'assurance font l'objet de nombreuses expérimentations. Par exemple, LenderBot[9] est le premier prototype d'assurance qui repose sur les technologies de la blockchain. Service de micro-assurance, elle assure le prêt d'appareils de haute valeur entre particuliers. La blockchain et son registre distribué jouent le rôle de tiers de confiance dans la contractualisation. Les particuliers s'accordent sur la nature du prêt via un bot disponible sur Facebook Messenger et donnent leur accord grâce à une signature électronique directement depuis l'interface de dialogue de Facebook.

L'idée de smart contrats s'exécutant automatiquement à la validation d'une certaine clause extérieure présente un intérêt significatif pour des applications dans le domaine des assurances. Des projets à l'étude envisagent par exemple l'utilisation de *smart contracts* dans la gestion et la compensation des retards des secteurs aériens ou ferroviaires. On pourrait en effet imaginer que la somme correspondant à la compensation à verser à un voyageur en cas de retard soit mise en séquestre sur le compte blockchain de l'utilisateur, et débloquée dès le retard confirmé par la compagnie de transport via une application dédiée et liée à cette blockchain.

---

[9] *http://www.itespresso.fr/blockchain-microassurance-lenderbot-138735.html*

3.8. INTÉGRATION DE L'INTERNET DES OBJETS

L'approche de consensus distribué proposée par la blockchain se prête bien aux enjeux posés par le développement de l'Internet des objets, notamment pour répondre aux besoins de sécurisation des échanges entre les objets et les plateformes de collecte des données qu'ils génèrent. Les technologies de la blockchain pourraient alors y trouver l'une de leurs plus larges applications car les questions de la confiance, de l'identité, du respect de la vie privée et de la confidentialité des données personnelles seront au cœur du développement du marché des objets connectés.

C'est l'objet par exemple d'un projet mené par SlockIt avec le géant allemand RWE pour la recharge autonome de véhicules électriques. La transaction entre les deux objets connectés, véhicule et borne de charge, est effectuée automatiquement et de manière sécurisée via un smart contract qui s'exécute sur la blockchain d'Ethereum, un système qui permettra au consommateur de ne payer que ce qu'il consomme au lieu de payer un forfait horaire.

De même la plate-forme de *crowdfunding* Usizo, mise en place par la société Bankymoon, active sur la blockchain du bitcoin, prévoit l'alimentation en électricité d'écoles équipées d'un compteur intelligent. Des donateurs sont invités à participer à l'approvisionnement en électricité de l'école en envoyant leurs contributions à son adresse Bitcoin.

3.9. GESTION D'ORGANISATIONS AUTONOMES DÉCENTRALISÉES

Smart contracts de grande envergure, les organisations autonomes distribuées (DAO) sont des applications collaboratives qui permettent de décentraliser et d'automatiser les prises de décisions d'une communauté autour d'un objectif commun. L'exemple le plus connu, la DAO d'Ethéreum, a ainsi pour objet le financement de projets. Zooz et Slock.it, déjà mentionnées, se présentent également de cette manière, préfigurant des entités économiques et relationnelles non centrées et permettant des relations symétriques entre pairs qui pourraient structurer l'économie collaborative de demain.

Les règles de fonctionnement d'une DAO sont en théorie connues de tous ses participants puisqu'elle est basée sur un code open source.

Mais ce modèle pose encore d'importantes questions, notamment en termes de gouvernance. C'est ce qu'a montré l'attaque dont a été victime mi-2016 la DAO d'Ethereum, qui souffrait d'une faille. En exploitant de façon récursive cette faille qui permettait de collecter plusieurs fois la même somme au cours d'une seule transaction, un attaquant a pu transvaser dans une DAO « fille » la somme de 3 millions d'Ethers (équivalent alors à plus de 50 millions de dollars US). Outre la vulnérabilité des blockchains exécutant des *smart contracts* comportant des erreurs ou bugs d'écriture, l'affaire a montré les limites d'un système autogéré. La crise n'a en effet été résolue que grâce à l'intervention du co-fondateur d'Ethereum, Vitalik Buterin, alors que les *smart contracts* sont conçus pour se gérer eux-même. Pour empêcher l'attaquant de retirer l'argent dérobé et invalider les transactions effectuées, Buterin a proposé de créer une « soft fork », un mécanisme qui consiste à créer une nouvelle branche de la blockchain en changeant les règles de consensus pour les rendre plus restrictives. Si la majorité des nœuds l'acceptent, la branche initiale est abandonnée car seules les transactions et échanges effectués sur la nouvelle branche selon les nouvelles règles sont validés. Un exemple qui montre les limites de ces modèles censés pouvoir se gérer de façon autonome sans autorité centrale.

3.10. VOTE EN LIGNE

La blockchain pourrait offrir un outil de vote sécurisé, auditable par tous et dont le résultat, transparent, ne pourrait être modifié par personne, y compris par l'administrateur du système, et pourrait être vérifié tout en respectant le secret du vote. Plusieurs initiatives, toujours au stade de l'expérimentation, étudient la possibilité d'appliquer le système blockchain au vote en ligne : Flux, PublicVotes, V-initiative ou encore FollowMyVote, la start-up la plus prometteuse en la matière, qui propose une plate-forme de vote en ligne open-source et transparente, fondée sur une blockchain.

Voter sur une blockchain serait un processus très similaire à une transaction monétaire. Comme pour une transaction, le système créerait un « portefeuille » pour chaque candidat et un jeton numérique pour chaque électeur, ce dernier pouvant alors attribuer son jeton au portefeuille - et donc au candidat - de son choix. Le processus serait enregistré sur une blockchain publique qui permettrait à chaque participant de vérifier que son vote a bien été pris en compte sans modification, tout en étant assuré de son anonymat puisqu'il voterait sous pseudonyme. Son identité serait garantie par une clé cryptographique, sorte de carte électorale digitale. Ce système permettrait d'alléger grandement au moins trois contraintes du système de vote traditionnel : le

coût d'organisation des élections, qui selon FollowMyVote pourrait être divisé par 2 ou par 3 ; le lourd dispositif du vote par procuration ; et les contraintes du dépouillement (besoin d'équipes de dépouillement et d'observateurs de chaque candidat, lenteur du processus).

Mais il reste encore de nombreux obstacles à régler pour que cette solution soit véritablement efficace et sécurisée. Le coût d'abord, car si voter sur une blockchain permet certes de s'affranchir de l'organisation d'élections traditionnelles, effectuer une transaction sur une blockchain a un prix (autour de 10 centimes selon le type de blockchain), ce qui porterait le coût d'un vote à 1 million de personnes à 100 000 euros, soit autour de 4,5 millions d'euros pour un pays comme la France qui compte près de 45 millions de votants, et le double dans le cas d'une élection à deux tours. Seconde limitation, la vitesse des transactions, estimée à 7 transactions par seconde sur une blockchain comme le bitcoin sur laquelle le vote en ligne pourrait être expérimenté, alors que 23 transactions par seconde seraient nécessaires pour faire voter 1 million de votants en 12h, et encore plus pour les 45 millions de votants français. Certaines solutions comme celle proposée par Stratumn permettent toutefois de contourner ce problème grâce à une architecture « offchain » qui agrège de façon extrêmement sécurisée d'importantes grappes de transactions. On peut aussi craindre une attaque contre la carte électorale digitale, nécessaire à un vote en ligne sécurisé, qui pourrait corrompre l'intégralité du processus. Un problème qui pourrait être résolu par l'utilisation de solutions matérielles plutôt que logicielles pour stocker de façon physique la clé cryptographique associée. Des parades et solutions existent donc mais elles complexifient le processus et l'alourdissent. D'autant que la question de la confidentialité du vote n'est pas tout à fait résolue. D'abord parce que, comme il a été démontré plus haut, l'anonymat de l'utilisateur, donc du votant, n'est jamais entièrement garanti, même avec l'utilisation de pseudonymes. Enfin, inscrire un vote sur une blockchain, qui se caractérise notamment par la transparence, suppose de mettre en place un mécanisme qui empêche de visualiser les tendances avant l'heure du dépouillement.

4. CONCLUSION ET RECOMMANDATIONS

Comme le montrent les cas d'usages présentés ci-dessus, le système blockchain promet des garanties en termes de sécurité, de tracabilité et de résilience qui présentent des avantages indéniables. Il est toutefois encore difficile de mesurer avec précision et certitude l'efficacité et la valeur ajoutée du système blockchain, car celui est encore à un stade de développement finalement peu avancé, et son potentiel comme ses limitations n'ont pas encore été entièrement appréhendés. La multiplication des recherches touchant à des aspects variés du système blockchain, et la prolifération des projets d'applications dans de très nombreux secteurs, mettent régulièrement en lumière de nouvelles potentialités mais également des doutes qui subsistent quant à ses avantages et ses limitations. Et ce d'autant que le système continue dans le même temps de se développer et d'évoluer.

Cette étude a également montré qu'il n'existe ni règle de fonctionnement, ni typologie figée de la blockchain, et que l'on peut imaginer potentiellement autant de blockchains que d'usages que l'on souhaite en faire en conservant le tryptique fondateur « chaînage/consensus/P2P ». En conséquence, il semble possible de préconiser une forme de blockchain en fonction des usages pour lesquels elle est prévue et des besoins auxquels elle doit répondre, mais il est difficile, à l'heure actuelle, de déterminer avec précision les paramètres et variables à adopter pour chaque usage. De même, si la mise en place ex-nihilo d'une blockchain semble assez simple puisqu'il suffit de reprendre le code de la blockchain du Bitcoin, libre et gratuit, en ne lui apportant que des adaptations mineures en fonction des attentes des utilisateurs, il est encore difficile à ce stade de déterminer avec précision les besoins nécessaires en termes de ressources humaines, financières et techniques.

Il est donc indispensable, pour identifier clairement les caractéristiques que devraient présenter les blockchains répondant aux besoins actuels et futurs des organisations, et pour éprouver leur efficacité et leur valeur ajoutée, de procéder à des expérimentations sur les cas d'usages cités plus hauts qui semblent les plus pertinents. Ces expérimentations devront être limitées dans leur objet et dans leur envergure, et permettront de mettre en avant les points forts et les points faibles.

5. LES RÉDACTEURS

Le Vice-Amiral (2S) ***Michel Benedittini*** a achevé une longue carrière dans la marine française avec le grade de vice-amiral. Détaché en 2006 auprès du Secrétaire général de la défense et de la sécurité nationale, il a notamment contribué à la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont il était le directeur général adjoint, et à la définition de la stratégie française de cybersécurité. Il a ensuite assuré, en 2012 et 2013, la fonction de Secrétaire général de la Commission du Livre blanc sur la défense et la sécurité nationale. Il poursuit depuis des travaux de recherche sur la cybersécurité et la cyberdéfense, notamment avec CEIS.

Consultante Senior chez CEIS depuis avril 2016, ***Amélie Rives*** intervient sur des études stratégiques relatives au numérique ainsi que sur la préparation des programmes et contenus du Forum International sur la cybersécurité. Elle est diplômée d'un Master en Sécurité Internationale de Sciences-Po Paris et d'un Master en Middle East Politics de la SOAS (Londres). Avant de rejoindre CEIS, Amélie Rives a d'abord effectué des missions de veille et d'analyse de risque chez GEOS et au Risk Advisory Group (Londres), puis au Centre de prévention des conflits de l'OSCE (Vienne). Elle a ensuite travaillé 4 ans à l'Ambassade de Grande-Bretagne à Paris, où elle était Attachée commerciale chargée des secteurs Sécurité et Défense.

PUBLICATIONS RÉCENTES

Le Plan d'action de la Commission européenne pour la Défense – une initiative encourageante mais à l'avenir encore incertain (Septembre 2017)

La survivabilité des hélicoptères : une préoccupation au coeur des engagements modernes, un enjeu majeur pour demain (Septembre 2017)

Le Système d'information des Armées (SIA) – Le programme SIA : changement de paradigme pour l'armée du futur (Août 2017)

Internet des Objets (IoT)- Une nouvelle donne pour la Défense ? (Août 2017)

Impression 3D – Des technologies de rupture au service des Armées (Août 2017)

Emploi du Cloud dans les armées – Première approche des concepts et contraintes (Août 2017)

Enjeux stratégiques du Big Data pour la Défense (Août 2017)

Cybersécurité dans le milieu maritime (Février 2017)

Android Malware in 2016: the emergence of a professional ecosystem (Janvier 2017)

A télécharger sur **www.sia-lab.fr** et **www.ceis.eu**

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G

Tour Montparnasse – 33, avenue du Maine

BP 36 – 75 755 - Paris Cedex 15

Tél. : 01 45 55 00 20 - Fax : 01 45 55 00 60