La Blockchain et ses potentielles applications

Ribeiro, André

La Blockchain et ses potentielles applications

André Ribeiro

GENEVA SCHOOL OF ECONOMICS AND MANAGEMENT
Information Science Institute

UNIVERSITÉ DE GENÈVE

La Blockchain et ses potentielles applications

Projet de recherche en gestion d'entreprise

présenté à la Faculté d'Economie et de Management
de l'Université de Genève

par

André Ribeiro

sous la direction de

prof. Dimitri Konstantas

pour l'obtention du

Baccalauréat universitaire en économie et management

Genève, Août 2016

L'auteur de ce projet est le seul responsable de son contenu, qui n'engage en rien la responsabilité de l'Université ou celle du professeur chargé de sa supervision. Par ailleurs, l'auteur atteste que le contenu est de sa propre rédaction, en dehors des citations parfaitement identifiées, empruntées à d'autres sources.

Table of Contents

Résumé

Le Bitcoin et les crypto-monnaie sont des monnaies numériques et ont comme singularité d'être décentralisé et fonctionne sans autorité hiérarchique.

Ces monnaies digitales (ainsi que la Blockchain, qui est issue de ces dernières) possèdent leurs caractéristiques propres pouvant déboucher sur de nombreuses applications et utilisations dans toutes sortes de secteurs ou industriels.

Néanmoins, ces innovations présentent des risques qui nous amènent à nous interroger sur les cadres juridiques, politiques, sociaux et éthiques qui devraient les limiter.

Le Bitcoin et les crypto-monnaies présentent également des limites technologiques : par exemple, la volatilité de certaines valeurs boursières de ces monnaies digitales pose des problèmes qu'il importe de résoudre, si ces nouvelles technologies veulent gagner en notoriété et confiance auprès du grand public et si elles veulent devenir des alternatives crédibles au système centralisé que nous connaissons aujourd'hui.

Les attributs innovants des crypto-monnaies poussent les gouvernements à proposer des mesures de régulation qui sont, au niveau international, peu homogènes.

Introduction

La première monnaie numérique inventée a été le Cyber Buck, créé en 1990 par le mathématicien américain David Chaum. Cette première monnaie électronique reposait sur des protocoles cryptographiques et était anonyme. L'entreprise de David Chaum, « DigiCash BV », qui s'est associée à la Mark Twain Bank afin de développer son domaine d'activité, les micros paiements sur internet, a dû déposer le bilan 8 ans plus tard. Peu après, entre 1998 et 2005, Nick Szabo conçut le projet « Bit Gold », du cash numérique décentralisé, qui, comme les Cyber Bucks, n'a pas convaincu le grand public en raison de sa vulnérabilité aux attaques. Néanmoins, le « Bit Gold » est considéré comme le prédécesseur direct du protocole Bitcoin[1], de par leurs similarités dans leurs « architectures » respectives, telles que l'horodatage, les signatures numériques, ou encore les clés publiques[2] (Jean-Luc, 2016). Ces différentes tentatives de création d'une monnaie digitale reflètent l'origine d'une nouvelle révolution technologique qui arrivera conjointement au Bitcoin, c'est-à-dire la Blockchain –en français « chaîne de blocks »- qui est sa technologie sous-jacente. Le Bitcoin est la première Blockchain à avoir été conçue, mais il est important de savoir que le Bitcoin n'est qu'une application financière de cette technologie, et qu'elle peut être appliquée à d'autres secteurs, comme nous le verrons plus loin dans le développement. Le 31 octobre 2008, Satoshi Nakamoto[3] publie l'article: *« Bitcoin A Peer-to-Peer Electronic Cash System[4] »*. Bitcoin étant un logiciel libre ou autrement dit, « open source », n'importe qui peut en inspecter le code source et s'en inspirer pour créer sa crypto-monnaie. Actuellement, on dénombre 600 monnaies digitales. Des communautés d'utilisateurs existent pour chacune d'entre elles, et organisent des meetings dans le but de perfectionner les points techniques des différents systèmes, notamment la sécurité. De ce fait, la date du 31.08.2008 est représentative de la création de toutes les autres crypto-monnaies qui ont pu accéder librement au code source du protocole Bitcoin et le modifier en fonction de leurs objectifs et utilités.

Le Bitcoin est créé dans un contexte bien particulier: en pleine crise financière de 2008, le système monétaire étant fragilisé et les citoyens méfiants envers les Etats et les banques, le Bitcoin émerge comme une solution. Il est la concrétisation et la parfaite illustration d'une volonté de changement des institutions financières. La crypto-monnaie la plus connue et utilisée est le Bitcoin, suivie de l'Ether (de la plateforme DAO[5] Ethereum). La première a une

---

[1] Dans l'ensemble de ce travail, lorsque Bitcoin est écrit en majuscule, c'est qu'il fait référence au système de paiement décentralisé et lorsqu'il est rédigé en minuscule, on parle de l'unité monétaire. Il n'a aucune existence physique.

[2] Jean-Luc. « *Histoire du bitcoin* ». URL : https://bitcoin.fr/Histoire/, 2016

[3] Satoshi Nakamoto est un pseudonyme. Jean Luc. «*Satoshi Nakamoto».* URL: https://bitcoin.fr/satoshi-nakamoto/

[4] Document original publié par Satoshi Nakamoto le 31 ocotbre 2008. URL : http://www.bitcoin.org/bitcoin.pdf

[5] DAO signifie en anglais Decentralized Autonomous Organization : logiciel, programme, qui fournit des règles de fonctionnement transparentes et immuables à une communauté s'organisant autour d'un objet commun. Elle a pour but, à la manière d'un fond d'investissement classique, d'évaluer des projets qui lui sont soumis, de décider

capitalisation boursière de 10.43 milliards de dollars et correspond à 80% de la masse monétaire des 600 monnaies numériques existantes. La seconde a une valeur boursière de près de 1 milliard[6].

La monnaie électronique bitcoin a donc été créée pour répondre à trois problématiques et enjeux qu'a pu révéler, entre autres, cette crise: en premier lieu, le Bitcoin est un nouveau système qui permet aux utilisateurs d'effectuer des transactions entre eux sans passer par des intermédiaires financiers. Si le système actuel de paiement en ligne ne peut se passer des banques, le bitcoin veut permettre d'en supprimer leur dépendance. Ensuite, il veut remédier au problème de double dépense: en empêchant les utilisateurs d'utiliser deux fois le même bitcoin, on évite la création monétaire infinie, sans quoi la monnaie ne serait pas viable. Enfin, la dernière problématique à laquelle veut répondre Bitcoin est celle d'assurer une monnaie sans autorité centrale et donc de s'affranchir de tiers de confiance. Les solutions trouvées ont ainsi été les suivantes: pour se passer d'intermédiaire, la solution choisie a été l'échange « peer-to-peer » (P2P) : d'utilisateurs à utilisateurs. Ensuite, pour parer au problème de double dépense, toutes les transactions sont enregistrées dans un grand livre comptable public, anonyme et infalsifiable qui est la Blockchain. De même, pour ce qui est de se passer d'une autorité centrale, le rôle de régulateur a tout simplement été donné aux utilisateurs mêmes du Bitcoin. Ils ont donc la capacité de valider ou non une transaction et de remonter eux-mêmes l'historique des transactions. Tout ceci est rendu possible par le fait que tous les utilisateurs ont accès au registre public. La transaction est soumise au réseau, dans lequel les mineurs, les personnes qui contribuent à vérifient la validité ou non des transactions, mettent la puissance de calcul de leurs ordinateurs au service du réseau. Ainsi, l'utilité d'une création monétaire alternative comme le Bitcoin a comme finalité de permettre aux secteurs non financiers de s'affranchir du monopole des banques sur les moyens de paiement, ou du moins en réduire leur dépendance. C'est grâce à ces innovations qu'apporte la Blockchain que le bitcoin est une révolution technologique et monétaire.

Bien que les crypto-monnaies et la technologie révolutionnaire liée à celles-ci possèdent un potentiel de développement fort intéressant pour bon nombre d'industries, et de belles perspectives d'avenir, son utilisation peut néanmoins s'avérer risquée et possède également ses limites. Dans le cadre de ce travail, je vais tenter d'expliquer de quelle manière les crypto-monnaies vont pouvoir être utilisées dans différentes secteurs, quelles peuvent être leurs différentes applications, mais également leurs risques et leurs enjeux. Nous allons principalement traiter du Bitcoin, car il est la première monnaie numérique et le premier système de paiement décentralisé à avoir été adopté par le grand public, mais également le principal et le plus populaire. Bitcoin est également la Blockchain la plus aboutie actuellement et la plus sécurisée. Etant donné que les autres crypto-monnaies se sont inspirées de Bitcoin, en comprenant le

---

collectivement avec les détenteurs de jetons de la DAO de financer ou non ces projets, et de distribuer les risques et récompenses qui y sont relatifs. Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.129

[6] https://coinmarketcap.com/, visité le 10.07.2016

fonctionnement de celui-là, on comprendra le fonctionnement des autres crypto-monnaies.

Ce travail se décompose en quatre parties. Dans la première partie, je vais tenter de décrire les concepts généraux liés au Bitcoin, notamment les aspects techniques et ce qui le différencie d'une monnaie fiduciaire. Dans un second temps, je vais parler des fonctions principales de la Blockchain, qui sont vitales pour comprendre le potentiel des crypto-monnaies. Ensuite, je vais essayer d'expliquer quelles sont les possibles utilisations et cas d'applications du Bitcoin et de la Blockchain. Finalement, je vais tenter d'expliquer quels sont les risques et les enjeux liés à l'utilisation de ces monnaies digitales.

Chapitre 1. Description des concepts

1.1 Le fonctionnement d'une monnaie centrale

Les monnaies traditionnelles, comme le franc suisse ou l'euro dépendent d'institutions monétaires centralisées, au sein de leurs pays respectifs : les Banques centrales. En Suisse, par exemple, l'autorité monétaire est la Banque Nationale Suisse (BNS). Il est important de savoir que lorsque l'on parlera de monnaie, il s'agira de la monnaie fiduciaire, c'est-à-dire les pièces et les billets, directement utilisables. Néanmoins, l'essentiel de la monnaie en circulation, près de 90%, est la monnaie scripturale, qui n'est qu'un jeu d'écriture comptable centralisé sur la base de données de notre banque (cf. paiement par carte de crédit). Il y a deux principales manières de créer de la monnaie scripturale : le financement interbancaire et le financement auprès de la Banque centrale. Lorsqu'une banque commerciale, auprès de laquelle nous déposons notre épargne, a un déficit de financement, elle se dirige vers une autre banque commerciale à excédent de ressources qui va lui prêter de l'argent. La banque recevant les nouveaux fonds va en garder, conformément à la loi, un certain pourcentage en réserve et va utiliser le reste pour faire crédit à une autre banque commerciale en déficit de financement. Ainsi, le schéma initial est répété et c'est ainsi que la monnaie scripturale peut être créée à l'infini. Cependant, lorsqu'une banque commerciale en déficit de financement ne trouve pas une contrepartie pouvant lui prêter le montant nécessaire, elle peut s'adresser à la Banque centrale qui lui prête les liquidités suffisantes. La deuxième manière de créer de la monnaie, c'est lorsque la Banque centrale d'un pays émet de la dette souveraine ou achète des titres sur les marchés financiers.

1.2 Le Bitcoin et ses fonctions monétaires

Le Bitcoin remplit les mêmes fonctions qu'une monnaie traditionnelle. Il représente une unité de compte, c'est-à-dire qu'il permet de mesurer l'utilité d'un bien ou d'un service. Il permet également de faciliter les échanges, c'est-à-dire qu'on peut l'utiliser, tout comme une monnaie fiduciaire, pour acheter des biens et des services. Il peut également servir de réserve de valeur, et donc être utilisé pour acheter des biens et des services dans le futur. En ce sens, le Bitcoin, qui est la première monnaie sans banque, peut être considéré comme une monnaie.

Néanmoins, il existe des différences entre le Bitcoin et une monnaie fiduciaire comme le franc suisse. Le franc suisse a un cours légal, c'est-à-dire qu'il est reconnu par le gouvernement suisse, et que toutes personnes ou institutions doivent être payées en franc suisse. Alors que personne n'est obligé d'accepter d'être payé en Bitcoin. Un autre inconvénient, c'est que rien ne garantit qu'il soit accepté dans le futur[7]. Ainsi, l'échange de bitcoin est uniquement possible entre personnes qui acceptent de l'utiliser ; c'est pour cela que c'est une monnaie appelée « du fait des usages », complémentaire ou encore alternative. De plus,

[7] Voir chapitre 4.3 sur la réglementation.

contrairement au franc suisse par exemple, dont les trop importantes fluctuations,vers le haut ou vers le bas, peuvent être régulées par la BNS, le Bitcoin repose sur un système décentralisé, c'est-à-dire qu'il n'est sous le contrôle d'aucune autorité, il n'appartient ni à une personne, ni à un gouvernement, ni à une entreprise, et donc sa valeur ne dépend que de l'offre et de la demande. Ce qui peut expliquer sa forte volatilité. En outre, dans un système centralisé, l'utilisation de la monnaie fiduciaire est encadrée par des règles, ce qui permet aux clients des banques de se faire rembourser lorsque quelqu'un utilise frauduleusement une carte bancaire. Dans un système décentralisé, il n'y a aucun recours légal possible, même si les utilisateurs peuvent souscrire des assurances dans le but de se faire dédommager auprès d'organismes spécialisés, en cas de problèmes[8].

1.3 Les aspects techniques du Bitcoin

Une des innovations fondamentales du Bitcoin est qu'il repose sur le réseau « peer-to-peer », un réseau informatique où les utilisateurs sont reliés entre eux via des nœuds[9] et sur lequel ils peuvent s'échanger directement et gratuitement de la monnaie électronique, sans passer par une entité tierce. Les utilisateurs peuvent contribuer à la puissance du réseau en mettant la puissance de calcul de leurs ordinateurs au profit du réseau bitcoin. Une autre invention majeure spécifique au Bitcoin est que les transactions sont chiffrées grâce à la cryptographie asymétrique, c'est-à-dire par un système de clé publique/clé privée. Les signatures des transactions bitcoin découlent toutes de la clé publique ECDSA, un des algorithmes les plus sûrs actuellement. L'adresse de la clé publique permet d'envoyer des bitcoins alors que la clé privée permet d'en recevoir ou d'en débourser. La troisième singularité révolutionnaire à elle seule, est la Blockchain. La « chaîne de blocks » est l'innovation sous-jacente au bitcoin, «une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente et fonctionnant sans organe central de contrôle» [10]. Plus intuitivement, une « chaîne de blocks » est une base de données distribuées et sécurisées permettant à tout utilisateur du protocole d'observer l'ensemble des transactions presque instantanément et de pouvoir en vérifier la validité. Par analogie, une Blockchain peut donc être comparée à un grand livre comptable public, anonyme et infalsifiable. Cette innovation permet de régler le problème de double dépense, c'est-à-dire qu'un bitcoin puisse être utilisé deux fois par une même personne. Dans le système bancaire traditionnel que l'on connaît, chaque banque conserve la base de données de tous ses clients de manière individuelle et privée et les autres acteurs économiques, comme les institutions de régulation telle que la FINMA, n'ont pas accès à ces informations. Alors qu'avec la monnaie fiduciaire il est possible de fabriquer de la fausse monnaie, avec le bitcoin, ce problème est résolu grâce à la

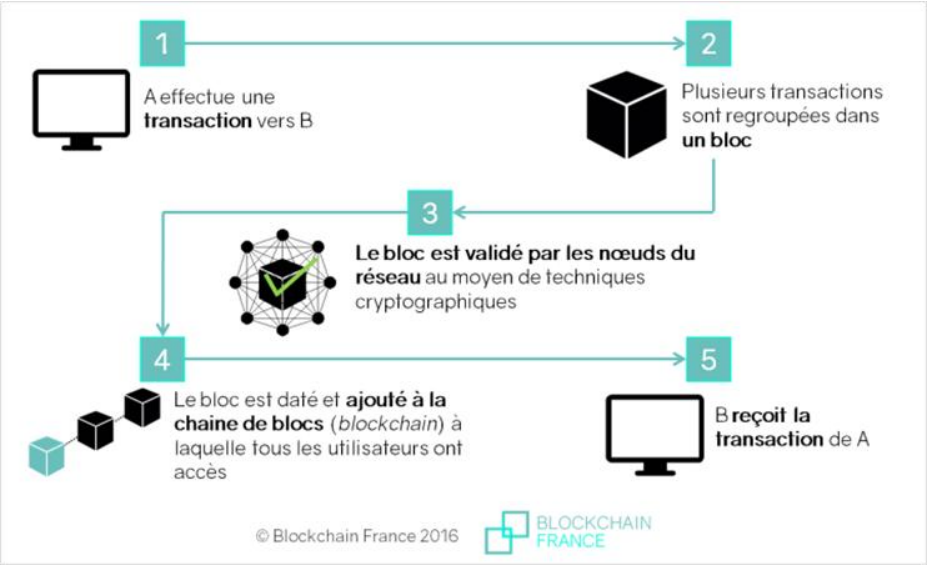
[8] *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. P. 1-48

[9] « Un nœud est un ordinateur relié au réseau et utilisant un programme relayant les transactions. ». URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/

[10] Blockchainfrance. « C'est quoi la blockchain ? » URL : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

Blockchain. Depuis la première transaction, le 3 janvier 2009 à 18h15[11], il n'y a jamais eu de faux bitcoins en circulation[12].

Lorsqu'une transaction est envoyée sur le réseau Bitcoin, elle est dirigée vers un nœud aléatoirement, puis redirigée vers tous les autres nœuds du réseau. Les transactions sont regroupées dans ce qu'on appelle des blocks. Pour que le protocole puisse vérifier les transactions, « sécuriser le réseau mais également permettre à tous les utilisateurs du système de rester synchronisés »[13], il faut de la puissance de calcul, et c'est ce qu'on appelle le minage. Les mineurs sont certains membres du réseau qui ont fait la demande de mettre à contribution du réseau la puissance de calcul de leurs machines. En plus de valider des données relatives aux transactions qui formeront un bloc, les mineurs, doivent résoudre des problèmes mathématiques très complexes. La complexité de ces problèmes varie constamment en fonction du nombre de mineurs connectés. C'est pourquoi l'algorithme de hachage SHA-256 fait partie intégrante du protocole bitcoin, afin d'adapter constamment la difficulté du problème, ce qui permet de maintenir un temps de validation par block proche des 10 minutes. En plus de la complexité des problèmes, leur résolution dépend d'une variable aléatoire, ce qui permet de faire en sorte que ça ne soit pas toujours le même mineur qui valide tous les blocks. C'est un des points essentiels qui sécurise la Blockchain. Lorsque le problème est résolu par un des utilisateurs, il doit fournir une preuve que c'est bien lui qui a la solution. C'est ce qu'on appelle la preuve de travail (*proof of work*) ou preuve de calcul[14].



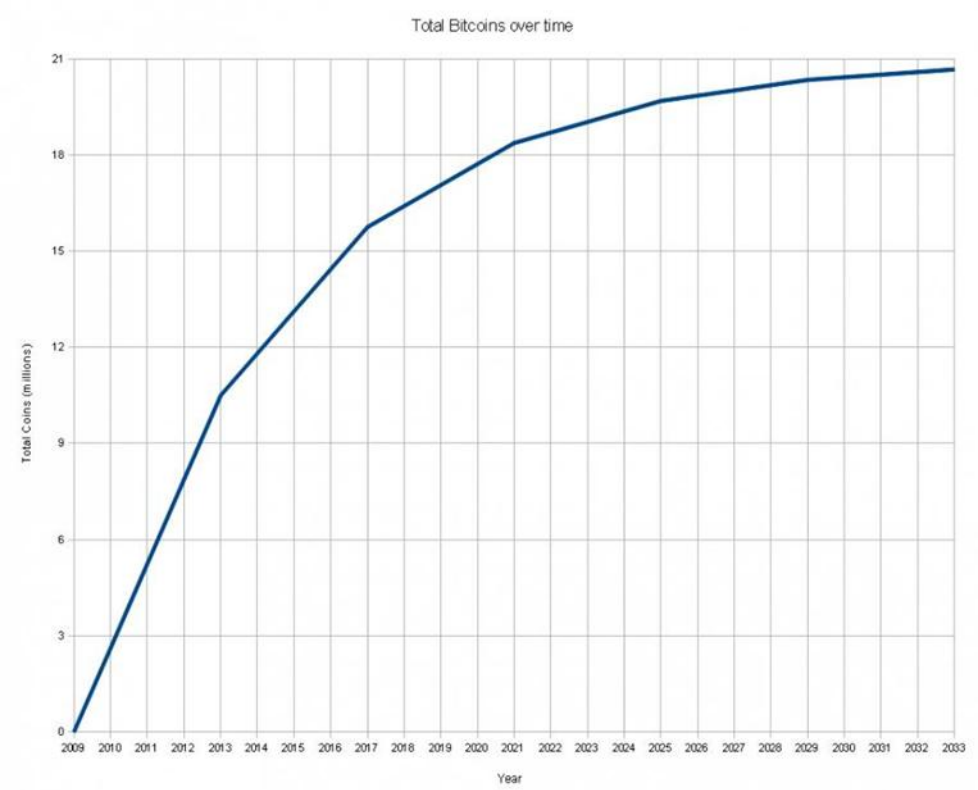
Source : URL : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[11] *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. 3 p.
[12] *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. P. 1-84
[13] https://blockchainfrance.net/le-lexique-de-la-blockchain/
[14] *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. P. 1-84

Le bloc validé par ce mineur est ensuite inséré temporairement dans la Blockchain, afin que les autres utilisateurs authentifient la preuve de travail. Si le consensus distribué diffère selon les utilisateurs, on peut se retrouver avec deux chaînes de blocks différentes, et parallèles. Dans un cas comme celui-ci, la règle est que tous les nœuds du réseau doivent conserver les deux chaînes et, cependant, qu'une des deux chaines travaille. Très rapidement, une des deux chaînes va prendre le pas sur l'autre. C'est pour cela qu'on dit qu'il faut attendre en moyenne une heure avant qu'un bloc soit irréversiblement confirmé, ce qui équivaut à attendre que cinq à six autres blocs soient intégrés dans la Blockchain.

Les mineurs sont rémunérés en bitcoins spécialement créés pour la validation du bloc et en fonction de la puissance de calcul qu'ils apportent au réseau : c'est une forte incitation à contribuer à la puissance de calcul du protocole. Afin que le processus soit équitable, une variable aléatoire est introduite dans le protocole pour valider un bloc. C'est le seul moyen de créer de nouveaux bitcoins et donc l'unique manière d'augmenter la masse monétaire. Pour l'anecdote, la raison pour laquelle on les appelle « les mineurs », fait référence aux chercheurs d'or qui faisaient augmenter la masse monétaire au fur et à mesure de leurs découvertes. Initialement, en 2009, la rémunération était de 50 bitcoins par bloc inséré dans la Blockchain. La règle est que la rémunération est divisée par deux tous les 210'000 blocks créés. Un procédé qui prend approximativement 4 ans. Aujourd'hui, les mineurs touchent 25 bitcoins par block et ce chiffre sera prochainement divisé par deux à nouveau car on a bientôt atteint les 203'000 blocs[15]. Le mécanisme est ainsi fait que la récompense pour miner les bitcoins va décroître au cours du temps, et donc, au final, la masse monétaire en bitcoins est prévisible. On sait qu'elle va converger vers 21 millions de bitcoins. Chaque bitcoin est divisible jusqu'au 100 millionième. C'est particulièrement intéressant, car ce mécanisme est connu d'avance et complètement transparent[16].

[15] URL : https://blockchain.info/fr/stats
[16] *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. P. 1-84



Source : *Pierre Noizat. Le bitcoin book.* Editeur : Pierre Noizat. 2012. p.62

1.4 Les autres crypto-monnaies

Les crypto-monnaies différentes du Bitcoin se font appeler les *altcoins*[17]. Ces *altcoins* diffèrent du Bitcoin selon que le code-source ait été modifié par rapport à l'original, c'est-à-dire celui du Bitcoin, par des manières de chiffrer le code avec d'autres algorithmes ou selon l'utilité que les créateurs ont voulu conférer à l'*altcoin*. Malgré leurs différences, elles sont toutes descendantes directes du Bitcoin.

Sachant qu'il existe plus de 600 crypto-monnaies, je vais vous parler ci-dessous de celles qui dominent soit :

- par leurs capitalisations boursières,
- ou par leur singularité ou notoriété,
- ou par leurs usages.

[17] Altcoin est une abréviation de « alternative coin ». Fait référence aux crypto-monnaies autre que le bitcoin. URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/

Cette classification est tirée du site de Cyril Fiévet[18].

Les monnaies « infrastructures » sont les crypto-monnaies qui ont l'ambition d'être plus que de la simple monnaie. Comme disent certains spécialistes, ce sont des projets « Bitcoin 2.0 ». Ce sont des plateformes qui «visent à construire de véritables alternatives aux systèmes financiers existants, en généralisant les principes inhérents aux crypto-monnaies (décentralisation, sécurisation, consensus distribué…) à tous types d'applications : marchés décentralisés, *smart contracts* (contrats malins), actifs cotés et échangeables, etc. »[19]. Ce ne sont pas les plus intuitives, donc on pense qu'elles seront plutôt utilisées dans le monde professionnel plutôt que par le grand public. On n'en dénombre qu'une dizaine, mais ce sont celles-ci qui ont le plus gros potentiel de disruption, « c'est-à-dire susceptible de transformer en profondeur les systèmes d'organisation sociale, notamment en matière de production économique : la Blockchain. Sa caractéristique principale réside dans sa faculté à établir un consensus entre des acteurs n'ayant a priori pas de raison de se faire confiance, ni mis dans l'obligation d'agir de concert par la force d'une autorité surplombante »[20].

Une de ces monnaies « infrastructures » les plus en vue est l'Ether. Elle est la seconde capitalisation boursière après Bitcoin. *L'Ether* est la monnaie électronique d'Ethereum, « dont le jeune fondateur, Vitalik Buterin, veut faire la « colonne vertébrale » d'une multitude de « cyber entreprises autonomes décentralisées » [21] . Elle veut permettre aux entreprises de se passer complètement des intermédiaires. Effectivement, selon Primaverra de Filippi, « lorsque l'on observe la Blockchain, et notamment le projet d'ordinateur global Ethereum, c'est que la Blockchain ne constitue pas simplement une « nouvelle technologie », c'est-à-dire en économie classique une simple transformation des facteurs de production et une hausse transversale de la productivité. Elle possède une capacité de transformation à même de proposer de nouvelles formes d'organisation et de gouvernance économique»[22]. Ether est la première crypto-monnaie décentralisée permettant à ses utilisateurs de réaliser des contrats intelligents (*smart contracts*). « Les smart contracts sont des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés. »[23] L'algorithme de hachage utilisé dans le protocole d'Ethereum est Ethash. Le type de preuve de travail est la même que bitcoin, c'est-à-dire « *proof-of-work* » (PoW). La *« proof-of-work* » est caractérisée par le fait que l'unique moyen d'obtenir des unités de monnaies est via la puissance de calcul d'une machine (le Hash Rate). Cependant, ce système de validation est de plus

[18] comprendrebitcoin.com, « Une classification des crypto-monnaies alternatives », rédigé le 4 février 2015 URL : URL : http://comprendrebitcoin.com/2015/02/04/une-classification-des-crypto-monnaies-alternatives/
[19] Ibid.
[20] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 47
[21] Herlin Philippe. Apple, Bitcoin, Paypal, Google : La fin des banques ? . Paris : Eyrolles, 2015, 115 p.
[22] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 33
[23] URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/

en plus controversé car, au fur et à mesure que les problèmes mathématiques se complexifient, la résolution de ces problèmes demande de plus en plus de ressources en énergie et en temps. En effet, la principale critique de cette méthode de résolution est la consommation exagéré en électricité qu'elle exigera[24]. C'est pour cela que les développeurs d'Ethereum vont changer de système de validation et opter pour une solution hybride, qui s'appelle Casper, entre la « proof of work » et la « *proof-of-stake* », lorsque la nouvelle version, *Serenity*, sortira en 2017. Les caractéristiques de la « *proof-of-stake* » (PoS), à la différence de la « *proof of work* », c'est qu'elles distribuent, à l'origine, des unités de monnaie à ses utilisateurs. Pour pouvoir miner, il faut en posséder. La réussite de la validation d'un nouveau bloc dépend du patrimoine des utilisateurs. Plus on possède d'unité monétaire, plus on a de chance de valider un bloc et donc de s'enrichir encore plus. La difficulté de ce système provient de l'allocation des unités monétaires initiales, afin de prévenir qu'un unique agent disposant du patrimoine le plus important prenne le pouvoir sur le système. Ainsi, un compromis et une tendance se sont formés. De plus de plus de crypto-monnaies optent pour une combinaison hybride entre les deux systèmes de validation afin d'hériter des avantages des deux consensus en se passant des inconvénients de chacun pour finalement avoir un arrangement plus robuste.

Une seconde monnaie infrastructure très bien valorisée sur coinmarketcap.com est *Ripple*. « Ripple est un système de paiement construit sur un protocole distribué et open source, sur un registre de consensus, et sur une monnaie appelée ripples (XRP). »[25] On peut définir *Ripple* comme le HTTP mais pour l'argent[26]. *Ripple* permet des « transactions financières mondiales sécurisées, instantanées et presque gratuites, de toute taille, sans rejets de débit »[27]. Il accepte toutes les monnaies fiduciaires, les crypto-monnaies et les commodités ou n'importe quelle réserve de valeur. Il repose sur une blockchain privée, et non publique contrairement au protocole Bitcoin. L'algorithme de hachage utilisé dans Ripple est l'algorithme ECDSA. Ce qui différencie une « chaîne de blocks » privée d'une Blockchain publique, c'est que son protocole est modifiable à tout instant par son ou ses développeurs. Ce type de blockchain intéresse principalement les banques. En effet, UBS et une dizaine d'autres institutions financières les plus importantes au monde ont déjà opté pour le protocole *Ripple* comme technologie d'infrastructure de paiement. Malgré tout, « la logique des blockchains privées va bien sûr à rebours du modèle libertaire pensé par les précurseurs de cette technologie, et des principes mêmes de la blockchain « historique », dont le cœur du potentiel repose justement sur l'ouverture et l'absence de contrôle centralisé- par un ou plusieurs acteurs. Pour autant, les blockchains publiques ne sont pas forcément incompatibles avec les blockchains privées, au contraire. La cohabitation semble possible, tant les atouts des unes complètent les limites des autres : d'un côté, une révolution capable de toucher de façon importante les banques, mais dont l'horizon ne

[24] Voir chapitre 4.2
[25] URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/
[26] URL : http://www.coindesk.com/chris-larsen-ripple-is-http-for-money/
[27] URL : http://www.finyear.com/Comment-marche-Ripple_a35971.html

semble pas à court terme ; de l'autre, une logique d'optimisation interne au monde bancaire, sans être toutefois de nature à bouleverser le secteur»[28].

Les monnaies complémentaires ou « vraiment alternatives », comme le dit Cyril Fiévet dans son livre, ce sont les monnaies analogues à Bitcoin, apportant toutefois quelques modifications ou innovations au protocole, notamment la diminution du temps de validation des transactions par exemple. Elles sont relativement faciles d'usage pour le grand public.

La monnaie complémentaire la mieux capitalisée est le *Litecoin*. Ce qui différencie le *Litecoin* du Bitcoin, est qu'il a premièrement, adopté une autre preuve de travail : le Scrypt. Le Scrypt, en cryptographie, est une fonction de dérivation de la clé. Le but de dérivée la clé est de permettre aux utilisateurs qui doivent s'identifier, par exemple, de diminuer considérablement le temps de calcul, tout en rendant le temps d'une attaque impensable, augmentant ainsi la sécurité. Autre différence entre ces 2 monnaies digitales considérables, c'est que le temps de validation des transactions entre chaque bloc est divisé par 4. Il n'est plus de 10 minutes, mais de 2 minutes 30 pour *Litecoin*. Ainsi, la confirmation d'une transaction se fait plus rapidement et permet, élément non négligeable, d'améliorer la capacité de stockage[29].

Il existe également des monnaies décrites comme« sociales ». Elles ont été développées afin que les internautes puissent échanger des montants peu significatifs de manière extrêmement simple, principalement à travers les réseaux sociaux. Selon Cyril Fiévet, ce sont « les crypto-monnaies les plus intéressantes et celles avec le plus de potentiel à court terme »[30]. En effet, ces crypto-monnaies simples d'utilisation et accessibles à tous pourraient permettre aux internautes moins férus de technologies mais désireux de s'initier au monde des monnaies digitales, de se familiariser avec ce nouvel environnement, saisir l'intérêt et le potentiel de ces nouvelles technologies. Elles pourraient être un moyen de généraliser les monnaies numériques. Une forte compétition fait rage entre les différentes crypto-monnaies digitales pour s'imposer en tant que la crypto-monnaie des micro-paiements en ligne. Son utilisation principale est le « *tipping* », don d'un cybernaute à un collègue cybernaute destiné à le gratifier d'avoir publié du contenu pertinent[31]. La première à avoir vu le jour, la plus notable et la plus importante au niveau de l'ensemble de la valeur des titres sur son cours de bourse est le *Dogecoin*, décliné du *Litecoin*. Il utilise, comme le Litcoin, la même preuve de travail, c'est-à-dire le Scrypt, comme expliqué précédemment. Sa caractéristique principale est qu'elle est basée sur un même Internet[32] : le Doge.

Il existe toutes sortes de monnaies numériques et différentes classifications, comme les monnaies dites « shopping », « locales », « anonymes » ou

---

[28] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 20
[29] URL : https://litecoin.org/fr/
[30] URL : http://comprendrebitcoin.com/2015/02/04/une-classification-des-crypto-monnaies-alternatives/
[31] URL : http://dogecoin.com/
[32] Un « même internet » exprime un concept ou phénomène répliqué en masse sur internet.

expérimentales. Cette liste n'est évidemment pas complète. Elles sont plus anecdotiques que celles cités dans les catégories ci-dessus, qui ont un réel pouvoir de changement.

1.5 Les avantages d'utiliser une monnaie digitale

Les crypto-monnaies sont novatrices, tout d'abord pour les particuliers, par le fait qu'elles proposent une nouvelle forme d'argent et de paiement. Prenons le cas du bitcoin : bitcoin permet des paiements simplifiés via un téléphone portable. Une carte de crédit n'est alors plus nécessaire, il suffit de scanner le QR code du destinataire ou de mettre les 2 téléphones l'un contre l'autre pour effectuer un échange de valeur, grâce à une technologie sans contact (NFC). Ensuite, la sécurité et le contrôle de l'argent sont largement renforcés. La cryptographie utilisée dans le protocole bitcoin est composée des algorithmes les plus sûrs actuellement : l'ECDSA et l'SHA-256. De ce fait, aucun tiers de confiance ne peut ponctionner le compte d'un utilisateur ou usurper son identité, ni effectuer de paiements en son nom: certaines fraudes possibles avec le système de paiement actuel sont donc évitées grâce au bitcoin. Autre innovation : c'est une monnaie universelle, utilisable dans le monde entier et en tout temps. Il n'y a plus besoins d'avoir le même prestataire de services, puisqu'il est interopérable. De plus, étant donné qu'il n'a aucune existence physique, Bitcoin permet des transferts internationaux, peu importe le montant, de manière immédiate : des bitcoins peuvent être transférés d'un bout à l'autre du monde en moins d'une dizaine de minutes et à des frais quasi nuls. Si, actuellement, des prestataires de services comme Western Union prennent une commission de 10% sur les transferts d'argent, bitcoin permet tout simplement d'y remédier. En définitive, le bitcoin permet aux particuliers de payer de manière anonyme, en cash numérique[33].

Du côté des entrepreneurs, en plus de bénéficier de tous les avantages cités pour les particuliers, ceux-ci n'ont plus besoin de se soumettre à la réglementation PCI, contrôlant et sécurisant les paiements en ligne, qui est aujourd'hui à leurs frais dans le système actuel[34]. Bitcoin est également un nouveau marché, avec des clients cherchant à utiliser leur nouvelle monnaie. Utiliser des bitcoins est aussi une manière pour les entrepreneurs de se démarquer de la concurrence et de gagner en visibilité. De plus, Bitcoin permet plus de transparence au sein d'une entreprise, étant donné que, dans son protocole, les transactions ne sont effectuées qu'une fois que toutes les personnes autorisées à signer l'aient effectivement fait, grâce à la fonction multi-signatures. Et, finalement, comme dit précédemment, grâce à la Blockchain, la comptabilité de l'entreprise est totalement transparente et infalsifiable, ce qui permet de gagner la confiance des investisseurs[35].

[33] URL : https://bitcoin.org/fr/bitcoin-pour-particuliers
[34] URL : https://www.six-payment-services.com/fr/shared/know-how/pci/pci-dss.html
[35] URL : https://bitcoin.org/fr/bitcoin-pour-entreprises

Chapitre 2. Les 3 principaux usages de la Blockchain

Selon Blockchain France (2016), il est possible de classifier les utilisations de la Blockchain selon 3 catégories : les transferts d'actifs, la Blockchain en tant que registre et les *smart contracts* ou les contrats intelligents.

2.1 Les transferts d'actifs

La Blockchain a été utilisée initialement au domaine unique de la finance et aux transferts d'actifs via son usage dans les crypto-monnaies, et aux transactions monétaires. Mais son application pourrait dépasser son actuelle utilité première ; les paiements en ligne, et se propager aux transferts d'argent internationaux. Imaginons : nous voulons transférer 10 CHF à une personne au Canada. Il nous suffirait de convertir nos 10 CHF en bitcoins, de les transférer à notre partenaire au Canada, qui les convertira, une fois la somme reçue en bitcoins, en dollars canadien. Actuellement, les commissions prélevées par des intermédiaires financiers, comme les banques, *Western Union* ou *Paypal* sont prohibitives, de l'ordre de 10% sur les 440 milliards que représente ce marché[36]. Cette application de la Blockchain pourrait drastiquement baisser les coûts, notamment pour les pays en voie de développement. Mais la Blockchain ne se limiterait pas uniquement aux transferts monétaires proprement dits, mais pourrait aller au-delà et permettre de développer de nouveaux services et s'appliquer à n'importe quelle classe d'actifs réelle : matières premières, actions, obligations, titres de propriétés, voitures ou maisons etc. Cette application s'appele, dans le milieu, des *colored coins.* « En plus de sa valeur propre, chaque jeton peut en effet recevoir des métadonnées contenant des informations de tout type. Ainsi, la start-up *Colu* (mais également *Coinprism* ou *CoinSpark*) vise à faciliter des transactions extrêmement diverses, concernant des œuvres artistiques (notamment les droits d'auteur dans le milieu de la musique), des voitures, appartements, billets de spectacle etc. En pratique, pour un bien donné, *Colu* attache des métadonnées à un jeton du réseau, qui devient ainsi une preuve de la propriété du bien en question ; ce jeton peut ensuite être affiché pour preuve sur son téléphone, sous forme de QR code unique certifié et transféré si besoin à un autre utilisateur dans le cadre d'une transaction»[37].

2.2 La Blockchain comme registre

La Blockchain peut être également être utilisée comme registre. En effet, ses caractéristiques intrinsèques (données infalsifiables, complétement transparente) font de la Blockchain une ressource inéluctablement intéressante « pour des enjeux de traçabilité et de certification. Les documents légaux de tout type sont concernés (par exemple, certificats de naissance, mariage, cadastre)»[38]. Néanmoins, il faut être prudent, car la « chaîne de blocks » ne

[36] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 10
[37] Ibid
[38] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 11

garantit pas l'authenticité d'un document. Il est disposé sur la Blockchain de la sorte, mais il faut en vérifier tout de même sa validité.

2.3 Les smart contracts

« Les smart contracts sont des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable. Ils fonctionnent comme toute instruction conditionnelle de type « if-then » (« Si » condition vérifiée « Alors » conséquence s'exécute), et présentent trois principaux apports : une vitesse accrue, une meilleure efficacité, et une certitude que le contrat sera exécuté comme convenu. Ces programmes sont capables de surmonter les problèmes d'aléa moral, et de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude »[39]. La différence essentielle entre un contrat intelligent se trouvant sur la blockchain et un autre n'y résidant pas, c'est que les termes du contrat de celui se trouvant sur ce support technologique ne pourront pas être altérés. Cette dernière utilisation de la Blockchain est la plus intéressante, car elle possède le plus de potentiels de cas d'usage.

Slock.it est la première application concrète de la technologie Blockchain utilisant les contrats intelligents. Elle est la première DAO au monde à voir le jour. Son objectif est de mettre en relation la Blockchain Ethereum avec de réels objets physiques afin que les contrats intelligents puissent interférer entre eux. Elle est considérée comme une des start-up les plus prometteuses. « Elle se définit, comme la « future infrastructure de l'économie collaborative », ayant pour slogan : « louez, vendez, ou partagez n'importe quel objet - sans intermédiaire » [40]. Nombre d'experts pensent qu'elle va révolutionner les échanges économiques émergents. *Slock.it* rend utiles les *smart contracts* en les rendant exécutables. L'application est basée, sur un verrou intelligent, appelé un *slock*. Un *slock* peut être utilisé avec un contrat Ethereum afin d'ouvrir n'importe quoi. Par exemple, une porte équipée d'un *slock* donne accès à un bureau ou un appartement à louer. Ces appareils sont coordonnés par la plateforme initialement développée par les mêmes développeurs que *Slock.it*, Ethereum, plus exactement l'ordinateur Ethereum. « Slock.it vise à rendre certains objets entièrement autonomes ; nous pourrions ainsi directement signer des contrats avec eux, sans intermédiaire »[41]. *Slock.it* développe une large gamme de technologies qui peuvent être intégrées dans n'importe quel objet intelligent. Ainsi, les individus comme les institutions pourront louer des vélos, édicter des assurances et recevoir des paiements en une seule opération. Sans être à la merci des hackers ou des centrales de paiement. Des utilisations ont déjà été démontrées. Par exemple, les propriétaires d'*Airbnb* équipés du verrou électronique Slock.it seront en mesure d'accepter les réservations à travers la Blockchain. « Un Airbnb-killer : L'exemple le plus souvent repris par les fondateurs de la société lors de leurs présentations est celui de la location d'appartement : si vous connectez la serrure de votre porte à la Blockchain, vous pouvez lier cette serrure à un *smart-contract* de location. Lorsque

[39] Ibid
[40] Ibid
[41] Ibid

quelqu'un veut utiliser votre appartement, il paye le prix de la location au contrat qui est lié à votre serrure sur la Blockchain. Une fois le paiement effectué, la porte s'ouvre automatiquement pour la personne qui a réglé la location, pendant la durée correspondant au paiement. En pratique, tout est géré par des *smart contracts* de façon transparente, la location se fait par l'intermédiaire d'une App et le paiement se fait en ethers. Slock.it travaille cependant à l'intégration de moyens de paiement classiques comme la carte bleue avec des partenaires commerciaux. Dans ce cas, les euros seront automatiquement convertis en crypto-monnaie, et vice versa. Le tout est contrôlé par une application sur le smartphone ou un site internet, de façon transparente pour l'utilisateur qui aura à gérer uniquement une interface web classique. Un fonctionnement similaire peut aussi être imaginé pour louer un vélo, une machine à laver, une voiture, etc. Le tiers de confiance disparaît donc de l'équation : les objets « se louent eux-mêmes », selon l'expression de Stephan Tual… »[42]. Ou encore un « uber-killer » : un prototype de voiture autonome qui se loue elle-même, fondé sur le projet de la start-up *Mobtiq*, permettant aux passagers de ne payer que pour les kilomètres qu'ils effectuent réellement (ou Arcade City qui met directement les chauffeurs et les clients en relation, afin que ceux-ci puissent s'affranchir de la fixation centralisée des prix par Uber[43]). L'idée serait qu'une communauté, composée par exemple d'une centaine de personnes, achète quelques voitures, utilisables par tous ses membres, sans appartenir à aucun individu en particulier. »[44]. Slock.it permet d'activer un verrou digital rendant possible de louer ou vendre tout ce qui peut être sécurisé par un verrou ou cadenas. Dans chacun de ces cas, ces transactions bénéficient de la transparence, de la traçabilité et de la sécurité de la Blockchain. Slock.it est également une plateforme pour les développeurs, car elle est compatible avec *Raspberry Pi*, *Beagle Board* et *Intel*. Cela signifie que n'importe qui peut construire son application sur Slock.it. On peut concevoir ce projet comme une connexion de la Blockchain au monde réel et concret[45].

[42] URL: https://www.ethereum-france.com/slock-it-la-promesse-des-objets-connectes-sur-la-blockchain/
[43] URL: https://blockchainfrance.net/2016/03/19/arcade-city-le-uber-killer-de-la-blockchain/
[44] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p. 12
[45] https://www.youtube.com/watch?v=opPyMgK5w9g

Chapitre 3. Les applications

Dans les chapitres précédents, nous avons pu découvrir les concepts théoriques et généraux concernant les crypto-monnaies et la Bolckchain. Nous avons ainsi pu constater que les trois piliers sur lesquels repose la Blockchain sont : le réseau P2P, décentralisé, registre anonyme et public, qui permet de changer le paradigme sur lequel repose la relation de confiance établie aujourd'hui, c'est-à-dire sur les intermédiaires, institutions ou entreprises centralisés. On peut dès lors passer à un modèle de confiance basé sur le réseau et un protocole reposant sur la technologie du code et des mathématiques, modèle qui sera aux mains d'une communauté distribuée sur un maillage et non sur un serveur unique. Leurs applications peuvent être très vastes. Dans ce chapitre, je vais aborder les différents types d'utilisations concrètes ou potentielles, de manière non-exhaustive, des monnaies digitales et de la technologie qui sous-tend celles-ci, afin d'illustrer toutes les possibilités d'usages. La première Blockchain à être apparu étant celle du bitcoin, celle-ci est, dans ses fondements, liée à un aspect financier. Ainsi, dans notre premier cas d'application, nous allons tenter d'analyser comment cette dernière, pourrait révolutionner les métiers bancaires, en raison de l'enregistrement public des transactions.

3.1 La banque et les assurances

De nombreux spécialistes, dont Philippe Herlin, auteur de « *Apple, Bitcoin, PayPal, Google : La fin des Banques ?* », pensent que les monnaies numériques et la Blockchain pourraient significativement changer, voire rendre désuète la banque telle qu'on la connait aujourd'hui. Effectivement, la Blockchain, de manière inhérente, veut permettre de se passer de n'importe quel intermédiaire. On peut penser évidemment à de nombreux différents services financiers. De nombreux éléments, déjà cités dans l'introduction, peuvent nous permettre d'entrevoir que le milieu de la banque risque de voir son rôle au sein de la société et de l'économie remis en question. En effet, au fur et à mesure que les scandales touchent le milieu bancaire, que ce soit la crise de 2007, le scandale du Libor, les traders obnubilés par l'argent comme Jérôme Kerviel, ou plus récemment les Panama Papers, l'évasion fiscale planifiée par les plus grandes banques du monde, il est évident que l'image de l'industrie financière, ainsi que la confiance accordée à ses institutions, se détériorent de plus en plus. « Pour David François par exemple, Chief Technical Officer de la plateforme bitcoin *Paymium*, « Un des grands avantages de la blockchain Bitcoin, réside dans le fait qu'il n'existe aucune barrière à l'entrée : n'importe qui peut créer un service qui fonctionne sur la blockchain. En particulier, n'importe qui, moyennant un important capital confiance, peut créer une banque en bitcoins qui accepte les dépôts des clients et émet des crédits en bitcoins. C'est en ce sens que le bitcoin peut « disrupter» la banque sur l'activité de crédit, en faisant tomber cette barrière à l'entrée. … Les acteurs qui réussiront le mieux seront ceux qui auront réussi à générer un capital confiance très important et à capitaliser dessus»[46]. La légitimité des banques est de plus en plus remise en

[46] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.17

question, notamment avec les start-up qui se créent dans l'industrie de la finance, qu'on appelle « Fintech » (technologie financière). Ces start-up sont en pleine expansion et elles visent toutes des métiers traditionnels du cœur de la finance. En voici quelques exemples.

En Suisse notamment, sur les 6 crypto-compagnies[47] les plus influentes de ce pays[48], quatre sont orientées sur la Fintech. La première dont je vais vous parler se nomme *Lykke*[49]. Cette start-up, créée en septembre 2015, veut établir une place de marché globalisé pour toutes sortes d'actifs et instruments financiers, accessibles au plus grand nombre d'utilisateurs via smartphone et fondée sur la Blockchain bitcoin. La seconde est *Xapo*[50], fondée en Californie, mais dont le siège social a été déplacé à Zurich, en raison de son cadre juridique, sa neutralité et ses hautes compétences dans le domaine de la finance. *Xapo* est une compagnie qui permet à la fois les dépôts, comme une banque, mais surtout, c'est la première à avoir développé une carte de crédit permettant d'utiliser ses bitcoins. Elle a levé un fonds de près de 40 millions de dollars fonds lors de son lancement. Ensuite, il y a *Metaco*[51], basée à Vevey, qui commercialise des solutions de négociation des contrats intelligents reposant sur la technologie Blockchain. De cette manière, les clients de *Metaco* peuvent convertir des bitcoins en monnaies traditionnelles ou en métaux précieux sur la plate-forme de courtage *Metaco*. La dernière des quatre plus influentes start-up dans le milieu de la Fintech, en Suisse, est *Monetas*[52], une plateforme développée sur le principe du notariat numérique. La plateforme permet aux utilisateurs, aux entreprises ou aux gouvernements d'effectuer des transactions dans le monde entier, qu'elles soient d'ordre juridique, public ou privé. La start-up a gagné le défi Swisscom Startup 2015 et est estimée à près de 90 millions de CHF[53]. D'autres start-up au niveau international ont pris de l'ampleur, notamment *BitTag,* qui est spécialisée dans l'étiquetage électronique, ce qui permet d'afficher le prix en dollar et en bitcoins. Néanmoins, le risque de change n'est pas supprimé. C'est pour cela que d'autres start-up se sont créées, comme *Bitpay* ou *Paymium*, qui ont développé des services dans le but de prendre en charge le risque de change. Par exemple, lorsque le vendeur, qui accepte de se faire payer en bitcoins, se fait payer en monnaie électronique, il peut soit garder les bitcoins, soit recevoir l'équivalent en monnaie nationale par l'intermédiaire de *Bitpay* ou *Paymium* qui convertit immédiatement le montant équivalent.

---

[47] URL : http://fintechnews.ch/blockchain_bitcoin/top-6-blockchain-and-crypto-companies-in-switzerland/2926/

[48] Il est important de savoir que de nombreuses start-up en lien avec les crypto-monnaies et la blokchain sont venues s'installer en Suisse, notamment grâce à un cadre juridique favorable et surtout non contraignant. URL : http://www.bilan.ch/argent-finances-plus-de-redaction/bitcoin-scene-suisse-start-effervescence

[49] URL : https://lykke.com/

[50] URL : https://xapo.com/

[51] URL : https://metaco.com/

[52] URL : https://monetas.net/

[53] URL : http://fintechnews.ch/blockchain_bitcoin/top-6-blockchain-and-crypto-companies-in-switzerland/2926/

Nous pouvons constater que les métiers traditionnels de la banque subissent différentes formes de pression par rapport auxquelles elles doivent s'adapter rapidement et non sans mal. Néanmoins, sur le court terme, la banque n'a pas à craindre ces technologies qui possèdent également leurs limites techniques. Comme je l'explique dans le chapitre suivant notamment, les sept transactions par seconde possibles sur la Blockchain bitcoin ne peuvent rivaliser avec les centaines de milliers de transactions par seconde sur les marchés financiers traditionnels qui existent aujourd'hui.

Les banques ne restent pas les bras croisés. Cette technologie ne pourrait pas que leur faire du tort et elles semblent d'ailleurs l'avoir déjà compris, puisqu'en septembre 2015, un consortium composé des 9 plus grandes banques de Wall Street est créé, afin de faire de la recherche et de développer la Blockchain, dans le système financier. Ce consortium compte actuellement plus de 42 institutions bancaires les plus importantes au monde, dans le but de « définir les standards communs de mise en place de blockchains interbancaires »[54]. A terme, l'objectif est de remplacer le standard SWIFT utilisé actuellement dans les transactions interbancaires par la Blockchain pour certifier les transactions. La coopération des différentes banques est orientée sur le développement de « chaine de blocks » privée ; ainsi, l'attrait du milieu bancaire pour cette technologie a pour but de diminuer les coûts de « compliance » ou conformité, en français. « Selon un rapport de la banque Santander, l'utilisation de la Blockchain pourrait faire économiser aux banques 15 à 20 milliards de dollars par an d'ici 2022, grâce à la réduction des « coûts d'infrastructure liés aux paiements internationaux, au trading et à la mise en conformité »[55].

On pourrait également imaginer le développement par les banques de toutes sortes de produits dérivés, dans l'optique de pouvoir prendre diverses positions sur ces devises numériques, sur le Forex par exemple, le marché sur lequel les devises nationales s'échangent, ou une plateforme spécialisée dans ce domaine. On peut notamment penser au *Swap* de change, soit « la conclusion, par deux parties et simultanément, de la vente (ou de l'achat) de devises au comptant et de l'achat (ou de la vente) de ces mêmes devises à terme. Pour la Banque nationale, cette opération prend la forme d'un échange de francs contre une autre monnaie »[56]. Ou on peut penser encore à d'autres produits dérivés, comme les contrats à terme, *forward, et options* dans une perspective de couverture face aux différents risques de change. Dans son étude, D. Yermack[57] démontre que, puisque le Bitcoin et or sont décorrélés (-0.088), cela représente un élément intéressant, comme les matières premières, pour diversifier un portefeuille de marché.

Le secteur des assureurs, en même temps que celui de la banque, s'est très rapidement intéressé au phénomène de la Blockchain. On peut citer, par exemple, Axa, qui a annoncé avoir capitalisé 55 millions de dollars dans la start-up *Blockstream,* dont le but est de rendre interopérables différentes

[54] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.19
[55] Ibid
[56] URL : http://www.snb.ch/fr/ifor/public/qas/id/qas_swaps
[57] Yermack, David. Is Bitcoin a Real Currency ? An Economic Appraisal.2014, p.22

Blockchains. Les assureurs portent une attention singulière à cette nouvelle technologie, car elle «a le potentiel de faire disparaître les phases de déclaration et de faire naître de nouveaux systèmes d'assurances en ligne sans intermédiaire »[58]. En outre, les bitcoins 2.0 que sont les *smart contracts* permettraient d'automatiser tout le processus. Des entités spécifiques appeléess « oracles », qui traitent les données des *smart contracts*, pourraient, par exemple, sans qu'il y ait d'interactions entre l'assuré et l'assureur, déclencher automatiquement le versement d'une indemnisation lorsque les conditions du contrat sont remplies. Un exemple cité fréquemment est celui de l'assurance indicielle, c'est-à-dire un contrat d'assurance basé sur les précipitations sur un mois. Une indemnité pourrait être versée directement à l'agriculteur après 20 jours sans pluie[59]. Cependant, une des grandes problématiques liées à ce type de contrat est évidemment celle de la régulation, sujet abordé au chapitre suivant. Ce type de *smart contract* lié aux assurances a un immense potentiel de croissance, lié conjointement à l'apparition de l'internet des objets.

3.2 L'énergie

Le secteur de l'énergie a vu apparaître de nombreux projets autour de la Blockchain, en raison du grand nombre d'applications dans ce domaine. Notamment des *smart-grids*, des réseaux d'électricité locaux intelligents, permettant l'optimisation de la production et de la distribution, rendant possible le stockage d'électricité dans le but d'améliorer l'efficience énergétique du réseau.

Un des premiers projets, qui a fonctionné, est le *SolarCoin*, une devise basée sur l'électricité produite à partir de l'énergie solaire. Cette start-up a pour but de promouvoir l'exploitation et la consommation des énergies renouvelables, en remplacement d'énergies fossiles très polluantes. Le principe est le suivant : chaque propriétaire de panneaux solaires peut revendre le surplus de sa production via la Blockchain, sans passer par l'intermédiaire du distributeur étatique, par exemple, à Genève, les SIG. Pour chaque MWH d'énergie solaire produite, le producteur reçoit 1 *SolarCoin*. « Ces jetons s'échangeront ensuite sur une place de marché, rendant liquide et efficient l'échange de ce qui est finalement une garantie d'origine 2.0 »[60]. Ethereum a également développé une application de la sorte, basé évidement sur la Blockchain de cette plateforme : *Grid-Singularity*.

Un autre projet significatif, illustrant la parfaite application de la Blockchain à l'énergie, a pris forme avec Transactive Grids. Ce projet est le fruit d'un partenariat entre *LO3 Energy*, producteur de réseau d'énergie solaire et *Consensys*, une start-up développant des applications sur la Blockchain. « Son objectif réside dans la réappropriation, par les citoyens, de leur production énergétique autonome ; pour cela des capteurs enregistrent l'historique de la création énergétique à un point précis et l'enregistrent aussitôt sur la Blockchain

[58] URL : http://www.journaldunet.com/economie/expert/64912/quel-potentiel-pour-la-blockchain-dans-l-assurance.shtml
[59] URL : https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/
[60] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.20

Ethereum. Des *smart contracts* pourront ensuite régir les règles d'utilisation de cette énergie, et, naturellement, tes tarifs des producteurs »[61]. Un projet pilote a été mis sur pied à Brooklyn où 5 maisons productrices d'énergies solaire revendent leur production à 5 logements. L'Allemagne, également, n'est pas en manque. Le conglomérat RWE s'est lié à la start-up *Slock.it* pour développer le projet *Blockcharge*, dans le but de créer de nouvelles bornes de recharge pour voitures électriques permettant également de traiter la facturation[62].

3.3 Le cadastre

Une autre application concrète de ces technologies est le suivi des titres fonciers. En effet, la Blockchain étant transparente, infalsifiable et sécurisée, des pays comme le Ghana ou la Géorgie se sont intéressés à elle afin de mettre en place un cadastre numérique ; cela mettra un terme aux litiges fonciers de certains pays, notamment en voie de développement.

Au Ghana, l'ONG et start-up *Bitlands* est engagée à régulariser et enregistrer les titres de propriétés sur la Blockchain. Seul 20% des terres sont enregistrées dans une base de données officielle, pourcentage qui représente les terres appartenant au gouvernement ghanéen ; un nombre important de citoyens n'ont pas d'adresse officielle. Pour le reste, c'est le droit coutumier qui prévaut, engendrant de nombreux problèmes administratifs et économiques, puisque ce n'est évidemmentt pas propice aux investissements. Chris Bates, Chief Security Officer de *Bitland,* fait part de ses convictions : « Notre plus grande ambition serait de contribuer à faire en sorte que le Ghana et l'Afrique développent leurs terres grâce à des registres transparents, des systèmes écologiques, et en coopération avec les gouvernements. Le but est de créer un système capable de réduire la corruption humaine dans les conflits fonciers. Ce projet dépasse largement *Bitland*. Les citoyens ont besoin d'un système qui empêche leur gouvernement de profiter d'eux injustement. Le projet pourrait apporter de la richesse à des communautés entières, pas seulement aux mains de quelques-uns »[63].

En Géorgie, le projet, à la différence de celui du le Ghana, est un partenariat, fondé à la demande du gouvernement, entre l'entreprise *BitFury,* spécialisée dans le bitcoin, et l'agence Nationale du Registre Public, afin que les citoyens puissent enregistrer leur propriété sur la Blockchain. Selon le directeur de *BitFury*, la Blokchain « permettra de sécuriser les données pour qu'elles soient incorruptibles. Ensuite, elle donnera la possibilité de réaliser un audit public quasiment en temps réel : l'utilisateur pourra auditer le registre, non pas une fois par an, mais toutes les 10 minutes par exemple. Enfin, elle réduira la friction dans l'enregistrement et le coût d'enregistrement des droits de propriété,

---

[61] Ibid

[62] http://www.energystream-wavestone.com/2016/06/blockchain-quelless-opportunites-lenergie-decentralisee/

[63] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.23 et URL : http://geopolis.francetvinfo.fr/le-blockchain-la-technologie-qui-pourrait-donner-vie-a-des-cadastres-virtuels-95941 et

puisque les citoyens pourront utiliser le service sur leur smart phone. La Blockchain sera ainsi utilisée comme un service de notariat »[64].

3.4 Le covoiturage

J'en ai déjà parlé précédemment (cf. page 18) mais les projets, tel qu'*Arcade City*, sont des projets étendards illustrant parfaitement comment la Blockchain a les capacités de révolutionner les modèles économiques de plateformes telles qu'Uber*, Booking.com* ou *Airbnb*. Leur point commun est leur modèle économique, qui centralise l'information, ainsi que les échanges entre utilisateurs, de manière à ponctionner une valeur des échanges[65]. Le fondateur d'Arcade city, Christopher David, était un ancien chauffeur d'*Uber* ; ce qui l'a poussé à créer cette start-up c'est qu'*Uber* décidait arbitrairement des prix ainsi que les 20 % de commission prélever sur chaque transaction. « Le talon d'Achille d'*Uber* est son management centralisé des prix. Chaque jour, les chauffeurs d'*Uber* se préoccupent de la diminution des prix fixés de façon centralisée au QG d'*Uber* à San Francisco, ou de la prochaine action coercitive menée par un gouvernement centralisé contre des échanges pair-à-pair. « En décentralisant la décision pour la porter au niveau du chauffeur et du passager, *Arcade City* libère le chauffeur et permet au passager d'avoir le contrôle sur l'expérience entière de son trajet »[66] explique le fondateur d'*Arcade City*.

3.5 Le cloud

Le *cloud computing*[67] n'est pas non plus épargné par l'euphorique engouement Blockchain. On peut citer différents types de services du cloud computing : *Infrastructure as a service (IaaS), Platform as a Service (PaaS),* et *Software as a Service (SaaS).* La fonction IaaS est d'héberger des données. La fonction du PaaS permet de disposer des services et applications sur Internet, alors que le SaaS met à disposition des logiciels. Ces services sont de plus en plus utilisés, car ils permettent d'accéder à ces systèmes, sans avoir à acheter le matériel informatique, ou à devoir l'entreposer dans l'entreprise. Cependant, ce système pose un problème majeur, concernant la confidentialité et la sécurité des données, notamment à propos des entreprises américaines qui possèdent leurs serveurs sur le territoire américain. De nombreuses start-up pensent que la Blockchain pourrait y remédier[68].

Une course contre la montre est lancée entre Microsoft qui s'est allié à Ethereum dans le but de pouvoir utiliser sa plateforme Cloud, nommée Azur, et IBM qui veut en faire de même. Le but serait de permettre l'accès direct et bon

---

[64] Ibid
[65] Ibid
[66] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.24
[67] « Le cloud computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. » URL : http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/informatique-cloud-computing-11573/
[68] Blockchain France. *La blockchain décryptée.* Lens : Netexplo, mai 2016, p.26

marché à toutes les Blockchains depuis une plateforme cloud, qui pourrait être nommée *Blockchain as a service*[69].

Comme dit précédemment, pour remédier à la centralisation des données, une starp-up a vu le jour : *Storj* qui revisite le principe du cloud en utilisant la Blockchain. C'est une alternative à *Dropbox*. C'est aussi une solution de stockage sur le cloud distribuée. Quel est le principe de *Storj* ? Louer l'espace libre du disque des utilisateurs qui n'en ont pas besoin. Afin que le fichier ne soit utilisable que par son propriétaire, il est fragmenté et dispersé sur plusieurs serveurs ; la reconstitution du document n'est possible uniquement qu'avec le système clé privée de la Blockchain. En contrepartie, les individus mettant à disposition leurs espaces de stockage seraient rémunérés. Ces nouvelles conceptions de mettre en lien l'offre et la demande, dans ce cas précis demande de stockage et l'offre d'entreposage, permettent d'envisager un cloud dans le futur, moins onéreux, plus sûr et plus efficient[70].

Les exemples cités précédemment ne sont pas exhaustifs. Les applications des crypto-monnaies et de la Blockchain peuvent s'appliquer à la santé, au sport, au vote en ligne, etc. Ce qu'il est important de retenir, c'est qu'elles peuvent permettre de s'affranchir de la plupart des tiers de confiance centralisés comme, par exemple, les métiers de la banque ou du notariat, et de les remplacer par des protocoles numériques décentralisés.

[69] Ibid
[70] URL : http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/informatique-cloud-computing-11573/

Chapitre 4. Les risques, les limites et les enjeux éthiques, juridiques et politiques

Bien que le bitcoin et la Blockchain aient de nombreux avantages et perspectives d'avenir, leur utilisation peut néanmoins s'avérer risquée et possède également leurs limites. Tous ces atouts de la Blockchain font qu'elle peut être appliquée à un panel très large d'activités, comme à la banque et à la finance, au vote en ligne, au covoiturage, aux assurances, à l'immobilier, à l'éducation, aux réseaux sociaux, à la santé, à l'internet des objets ou encore au stockage sur le cloud. Les crypto-monnaies et la Blockchain soulèvent de nombreuses questions notamment au niveau éthique, juridique, politique et possèdent également leurs risques et leurs limites[71].

4.1 Les risques et limites

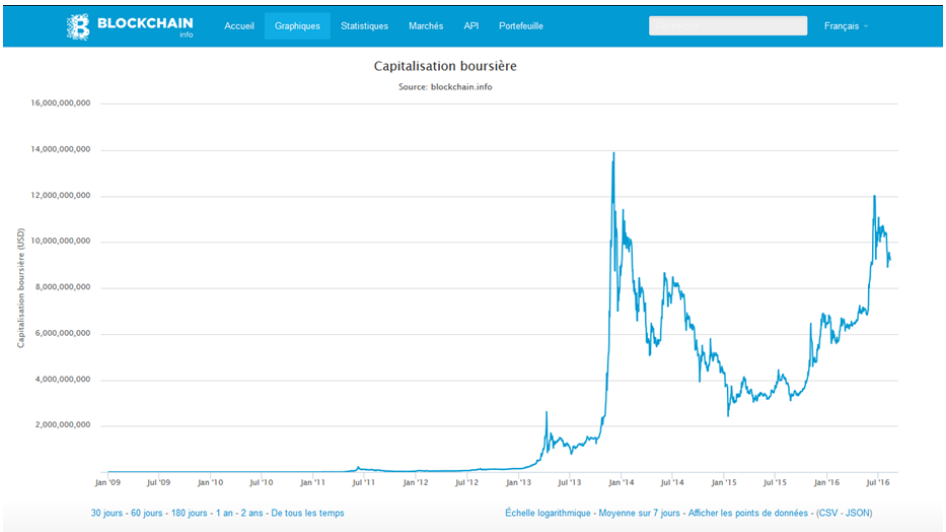
Le Bitcoin est de l'argent liquide numérique, ou tend à l'être, et son utilisation est extrêmement facile ; par conséquent, il est aussi important de prendre toutes les mesures nécessaires afin de sécuriser au maximum son portefeuille. Un premier risque non négligeable est la volatilité de son cours. En raison de sa courte existence, celui-ci peut augmenter ou diminuer brutalement en très peu de temps. Ainsi, un ménage n'est que faiblement incité à posséder ou épargner des bitcoins, car son pouvoir d'achat est extrêmement variable par rapport à une monnaie traditionnelle, et cela même si les coûts de conversion sont faibles. Le Bitcoin présente un autre inconvénient : son marché est très peu liquide en comparaison des marchés traditionnels ; cela est dû à sa masse monétaire limitée. Autre point dont il faut également être conscient, c'est que les transactions sont irréversibles ; le remboursement pour une quelconque erreur dépend de la bonne foi de la personne à qui on verse l'argent ! Une grande confiance entre les partenaires commerciaux est donc nécessaire. L'anonymat des utilisateurs est aussi relatif : la Blockchain étant publique, n'importe qui peut consulter le solde de votre compte et connaître vos dernières transactions. L'identité de l'utilisateur reste confidentielle, tant qu'elle n'est pas révélée lors d'un achat par exemple. Ensuite, les transactions qui ne sont pas encore confirmées sont vulnérables, car elles sont encore réversibles. En outre, le nombre de transactions par seconde ne peut pas aller au-delà de sept transactions par seconde[72], ce qui est infinitésimal par rapport aux transactions des marchés financiers traditionnels qui sont de l'ordre de plusieurs centaines de milliers par seconde. Finalement, le principal point faible du bitcoin est son écosystème : si le réseau lui-même est à l'abri, étant donné que la Blockchain est immuable, les intermédiaires que sont les sociétés de services autour du bitcoin, sont, elles, vulnérables à des hackers, comme nous le verrons plus loin avec *MT Gox* et *Bitfinex* notamment. Enfin, il faut savoir que cette nouvelle monnaie n'est aujourd'hui nulle part considérée comme une devise officielle. Malgré tous ces points, il est important de garder en tête que le bitcoin est

---

[71] Blockchainfrance. « C'est quoi la blockchain ? » URL : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[72] URL : http://blogchaincafe.com/la-limite-des-nombre-de-transactions

relativement nouveau et encore en développement: des améliorations peuvent encore y être apportées[73].



Source : URL : https://blockchain.info/fr/charts/market-cap?timespan=all

Elles sont d'ailleurs nécessaires, au vu des récents faits illustrant les limites de cette nouvelle technologie et les dérives de ses utilisateurs. Le 2 octobre 2013, notamment, les autorités américaines ont fermé le site « *Silk Road* », implanté sur le « *dark web* »[74]. Ce site spécialisé dans la vente de drogue et de toutes formes d'autres produits et services illicites avait la particularité de percevoir tous ses paiements en bitcoin, étant donné que cette monnaie est non nominative et hors du système bancaire international. L'utilisation du bitcoin ne sert donc pas que les nobles causes. En outre, la sûreté du Bitcoin n'est pas non plus totalement fiable. La preuve avec le cas *MT Gox*, la plus grosse bourse sur laquelle était traité le bitcoin, jusqu'à sa faillite, en février 2014, lorsque 650'000 bitcoins ont disparu, ce qui représenterait au cours du marché actuel, l'équivalent de 384'104'500 millions de dollars[75]. On ne sait toujours pas si le CEO a mis en place un système de Ponzi, tout comme Madoff, et est parti avec le magot, ou bien si la plateforme s'est fait hacker et subtiliser les bitcoins[76]. Plusieurs autres plateformes de portefeuilles numériques ont été la cible de hackers, étant donné que la Blockchain est jugée inaltérable, les intermédiaires sont des cibles privilégiées. Dernièrement, le 2 août 2016, *Bitfinex*, qui était

[73] Bitcoin.org. « Vous devez savoir ». URL : https://bitcoin.org/fr/vous-devez-savoir et I. de L. « Bitcoin et autres monnaies virtuelles : attention danger ! » URL : http://moneystore.be/2014/placements/bitcoin-monnaies-virtuelles-attention-danger, Jan. 14, 2014

[74] lemonde.fr. « Le site Silk Road, « l'e-Bay » de la drogue », fermé par le FBI ». *Le Monde.* Sept. 02, 2013

[75] URL : https://www.coinbase.com/charts (650'000 bitcoins multiplié par 590.93 dollars, cours du 9 août 2016)

[76] Nessim Ait-Kacimi. « Bitcoins : Derrière la faillite de MTGox l'ombre de Charles Ponzi ». *Les Echos. Aou. 07, 2015*

jusque-là la plus importante plateforme de change des monnaies fiat[77] vers le bitcoin, s'est fait subtiliser, 119'756 bitcoins, pour une valeur de marché de plus de 66 millions de dollars[78]. Les bitcoins 2.0 ne sont pas non plus à l'abri des attaques. En effet, le 17 juin 2016, *The DAO*, premier fond d'investissement décentralisé, (créé par la société *Slock.it)*, qui a lancé la plus grande campagne de financement participatif visant à promouvoir des projets d'internet des objets(OIT), s'est fait dérober près de 3.6 millions d'*Ether*, pour une valeur de marché de l'ordre de 53 millions de dollars. Soit plus d'un tiers des fonds levés lors du *crowdfunding*[79]. Le préjudice est autant financier que moral. Une des solutions pour récupérer les *ethers* volés seraient l'utilisation d'un hard fork[80], qui signifierait modifier le code du afin de les récupérer puis les redistribuer à leurs propriétaires. La confiance a été transférée des humains vers la technologie qui est le code. Le problème est qu'il s'agirait de « faire une entorse à l'une des valeurs fondamentales de la Blockchain qui veut que le code et l'automatisation l'emportent sur l'intervention humaine (*Code is law*). Ces derniers jours, les investisseurs ce sont donc retrouvés face à un dilemme: perdre leur mise ou accepter, à contrecœur, de modifier manuellement un code réputé inviolable pour faire rebasculer les fonds en lieu sûr »[81]. « La faille du système réside essentiellement dans sa gouvernance (inexistante ou incertaine). La question ne se poserait pas dans une Blockchain non publique (de consortium ou privée), dans la mesure où la sécurité, le contrôle et les décisions relèveraient de l'organe central (une personne morale) investi de la gouvernance, mais aussi qui engagerait sa responsabilité» [82] . Tous ces événements alimentent les discours des détracteurs du Bitcoin et de la technologie née conjointement, ternissent leur images, leur réputation et surtout, portent atteinte à la confiance accordée à ces nouvelles technologies par les investisseurs et utilisateurs et entraver, voire stopper leur développement. Finalement, un nouveau type de techno-banditisme émerge avec le bitcoin: pratiquant l'extorsion de fonds et des demandes de rançons en bitcoin, des *ransomware*[83]. Par exemple, en février 2016, lorsque la prise d'otage numérique d'un hôpital s'est terminée par le versement d'une rançon de 17000 dollars en

[77] Monnaie fiat : monnaie » classique dont la valeur est donnée par la loi ou la régulation gouvernementale (euro, dollar…) URL : https://blockchainfrance.net/le-lexique-de-la-blockchain/

[78] URL : http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/

[79] Financement participatif

[80] Logiciel développé en réutilisant le code source d'un logiciel existant. URL : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26529122

[81] URL : http://www.lefigaro.fr/secteur/high-tech/2016/06/27/32001-20160627ARTFIG00068-dans-la-blockchain-le-code-ne-fait-plus-la-loi.php

[82] URL : http://www.usine-digitale.fr/article/la-blockchain-pose-de-serieux-problemes-de-confiance-de-droit-et-de-securite.N401527

[83] Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. URL : http://www.altospam.com/glossaire/ransomware.php

bitcoins[84]. De même à Genève, récemment, lorsqu'une régie s'est fait attaquer par des hackers exigeant 1800CHF en bitcoin par ordinateur infecté[85].

4.2 Les enjeux éthiques

En plus leurs risques et de leurs limites, le Bitcoin et la Blockchain soulèvent également des dilemmes éthiques. Dans le domaine du social et des places de travail, même si les perspectives de services entourant le bitcoin et les crypto-monnaies en général ont un potentiel énorme et que l'univers digital en soit va créer de nombreux emplois, on pense néanmoins que la digitalisation de la société risque de cannibaliser plus de postes de travail qu'elle va potentiellement en créer. Selon Jacques Favier, auteur de *La voix du Bitcoin* « les économies réalisées ne vont guère au-delà des perspectives de licenciements» [86]. De plus, les caractéristiques propres au bitcoin et à la Blockchain remettent fondamentalement en question le rôle des tiers de confiance ou, plus simplement, des intermédiaires. Ce principe intrinsèque à ces technologies, on peut l'appeler la désintermédiation ou la décentralisation. Le bitcoin a une capacité de rupture égale à celle d'*Uber* par rapport aux modèles économiques traditionnels, que certains experts pouvaient évoquer, en 2015, comme « l'uberisation de la société », car il s'appuie sur les mêmes caractéristiques que sont la décentralisation, internet et la distribution numérique, capable de bouleverser notre économie et notre société. Le bitcoin innove sur un point, par rapport à *Uber et Airbnb*, c'est qu'il veut se passer de tous les intermédiaires centralisés et d'un système hiérarchique horizontal, en le remplaçant par des systèmes informatiques distribués, alors même que ses plateformes servant d'intermédiaires sont le centre même de la révolution technologique de ces dernières années. Ainsi, comme nous l'avons vu précédemment avec *Arcade City*, *Uber* pourrait se faire uberiser.

Lorsque l'on évoque le bitcoin, par ailleurs, on touche inévitablement sur un problème écologique, voire moral. Une récente étude, menée par des chercheurs Zurichois, montre que le processus du minage de bitcoin, c'est-à-dire la validation et l'enregistrement dans la Blockchain des transactions, a consommé autant que 620'000 ménages, soit l'équivalent de la centrale nucléaire de Mühleberg[87]. Le protocole est ainsi conçu : plus la puissance de calcul augmente, plus l'algorithme complexifie les problèmes à résoudre afin de valider les transactions, provoquant une nécessité accrue en ressource énergétique. Selon Sebastiaan Deetman, d'ici 2020, si le réseau Bitcoin poursuit

---

[84] lemonde.fr. « Un hôpital américain paye une rançon à des pirates informatiques ». *Le Monde*. Fev. 12, 2016

[85] FXinter.net. « Une régie se fait rançonner ses données en bitcoin » URL : https://www.fxinter.net/analyse-forex.aspx?ID=120224&direct=Une+r%C3%A9gie+se+fait+ran%C3%A7onner+ses+donn%C3%A9es+en+bitcoin, Avr. 20, 2016

[86] URL : https://www.letemps.ch/economie/2016/05/29/blockchain-va-affoler-intermediaires-financiers

[87] rts.ch. « Le bitcoin a consommé en 2015 autant d'énergie que 620'000 ménages ». URL : : http://www.rts.ch/info/sciences-tech/7674767-le-bitcoin-a-consomme-en-2015-autant-d-energie-que-620-000-menages.html, Avr. 26, 2016

la même expansion que jusqu'à présent, il pourrait consommer autant que le Danemark[88].

4.3 Les enjeux juridiques et politiques

Les réglementations gouvernementales et la taxation du Bitcoin sont très disparates selon les pays et il n'existe pas d'accord entre ceux-ci visant quand à anticiper son évolution afin d'établir un cadre légal commun. Pourtant, les différentes mesures qu'entreprendront les Etats pour réglementer l'usage des crypto-monnaies auront un impact certain quant à leur développement. De fait, sans un cadre juridique établi, il est peu probable que les crypto-monnaies soient utilisées de manière généralisée. Néanmoins, il est évident que plus les gens utiliseront ces monnaies digitales, plus les Etats s'intéresseront au sujet. Comment les différents pays pourront réguler les différentes monnaies numériques ? La Blockchain pose de véritables interrogations quant à la responsabilité de celui qui rédige le code et des contrats « apatrides ». Les premiers pays à avoir pris des mesures concernant les crypto-monnaies ont été le Canada et les Etats-Unis. Le Canada a décidé de taxer les crypto-monnaies si celles-ci devenaient une source de revenu : par exemple, une augmentation significative du cours du bitcoin par rapport à la date d'acquisition devrait être déclarée au fisc[89]. Les Etats-Unis ont décidé de taxer les plus-values[90]. Cependant il peut exister des divergences entre Etats, étant donné que chacun a sa propre jurisprudence. Néanmoins, au niveau national, depuis 2015, du moins, le bitcoin est classé comme une commodité, une marchandise. La Banque Centrale Européenne considère, elle, le bitcoin comme une monnaie virtuelle convertible décentralisée[91] ; cependant, les réglementations nationales, au sein de l'Europe, restent divergentes. En octobre 2015, la Cour Européenne de Justice a déterminé que les transactions en bitcoin seront exemptées de taxes, comme le cash traditionnel finalement[92]. Selon les juges, les transactions en bitcoin doivent être exemptées de taxes, car le bitcoin doit être considérer comme un moyen de paiement[93]. En Chine, alors que les particuliers peuvent en détenir et « trader » en bitcoin, la Banque Populaire de Chine a parallèlement décidé d'interdire aux institutions financière du pays d'en faire autant[94]. En Suisse, le Conseil fédéral préfère n'entreprendre aucune mesure et attend de voir comment ces inventions vont se développer avant de légiférer. « Au regard de la politique monétaire, les monnaies virtuelles ne sauraient donc menacer, à

[88] URL : http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
[89] URL : http://www.internationaltaxreview.com/Article/3343959/Latest-News/Bitcoin-users-face-a-global-patchwork-of-inconsistent-tax-treatment.html
[90] URL : http://aleny.net/la-reglementation-du-bitcoin-au-canada-et-aux-usa/
[91] URL : http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[92] URL : http://www.reuters.com/article/us-bitcoin-tax-eu-idUSKCN0SG0X920151022
[93] URL : http://www.bloomberg.com/news/articles/2015-10-22/bitcoin-virtual-currency-exchange-is-tax-free-eu-court-says-ig21wzcd
[94] URL : http://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions

brève échéance, la stabilité des prix et celle du système financier de la Suisse. L'évolution à plus long terme, dans ce domaine, est toutefois difficilement prévisible. Aussi le Conseil fédéral et la BNS continuent-ils à observer la situation afin de pouvoir identifier un besoin d'action éventuel en temps opportun »[95]. La Russie, elle, semble beaucoup plus réfractaire à l'adoption de toutes formes de crypto-monnaies. En effet, elle en a tout simplement interdit la possession ou l'utilisation sur son territoire, les définissant comme illégaux[96]. Ainsi le véritable défi pour les gouvernements des différentes pays est de savoir comment réguler les crypto-monnaies sans en entraver leur développement ni leur adoption. « Les standards devront être définis par les régulateurs, les grands acteurs, ainsi que les utilisateurs conscients du potentiel de cette technologie. Les régulateurs doivent d'abord comprendre et observer la technologie avant de se déterminer. Mais ils ne pourront avoir la main lourde. « On a connu des industries qui ont fini par quitter le pays dans lequel elles sont nées en raison des interventions excessives de leur Etat d'origine », observe Pierre-Edouard Wahl[97].

[95] URL : https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf
[96] URL : http://www.cnbc.com/2014/12/17/russians-move-into-bitcoin-as-ruble-tanks.html
[97] URL : https://www.letemps.ch/economie/2016/05/29/blockchain-va-affoler-intermediaires-financiers

Chapitre 5. Conclusion

Dans ce travail, j'ai tenté d'expliquer pourquoi ces innovations technologiques fascinantes que sont les crypto-monnaies et la technologie qui en découle, la Blockchain, sont bien plus que une révolution technologique et monétaire. En effet, dû à leurs caractéristiques inédites fondées sur des méthodes cryptographiques en pair-à-pair, ces innovations bousculent les formes traditionnelles d'organisation, de validation des transactions et sont une opportunité pour la création de nouveaux services, de nouvelles applications et le développement de start-ups faisant émerger une nouvelle forme d'économie. Les champs d'applications sont immenses et les exemples cités pour illustrer le sujet sont loin d'être exhaustifs.

Ces innovations permettent un changement de paradigme majeur :

Auparavant, les gens faisaient entièrement, voire aveuglément confiance aux institutions hiérarchisées.

Avec les nouvelles technologies, la confiance est accordée au système « pair-à-pair », supprimant du même coup celle qui existait entre les individus, éliminant les interactions et, par la même occasion, tous les intermédiaires de confiance. Cela peut rendre possible des applications et des échanges entre individus qui ne se connaissent pas, qui n'était pas envisageables auparavant. L'engouement autour de ces phénomènes est compréhensible lorsque l'on pense à leur potentielle utilisation :

- par exemple, la suppression des certificats et des intermédiaires de certification, notamment à l'aide des smart contracts, qui présentent quasiment aucun risque.
- Des services futurs, encore à créer, et dont on n'a même pas encore l'idée.

Néanmoins, pour l'agence Gartner, les crypto-monnaies et la Blockchain se trouvent actuellement au pic de la Courbe de la Hype, moment où des start-ups se développent dans le but de commercialiser la technologie. Toutefois, c'est aussi le stade où les espérances sont exagérées, suralimenté par l'emportement médiatique, débouchant sur des attentes irréalistes. L'analogie peut être faite avec la bulle spéculative d'internet de 2000. En effet, on est à la genèse de cette technologie et il ne faut pas négliger les défis à relever, avant que cette technologie soit mature et puisse se démocratiser à une plus grande échelle.

La Blockchain de Bitcoin, par exemple, présente des contraintes techniques qu'elle devra surmonter si elle veut un jour pouvoir un jour se développer massivement. Les 10 minutes d'attente nécessaires à ce qu'un block soit validé, sont préjudiciables à son développement, tout comme le nombre limite de 7 transactions à la seconde. Un autre enjeu, celui-ci non spécifique au Bitcoin, mais à la Blockchain en général, est d'ordre environnemental. Effectivement les « chaînes de blocks » utilisant la technologie de « proof-of-work », sont

extrêmement énergivores. Les développeurs doivent absolument prendre ce paramètre en compte et y remédier, si cette technologie compte un jour se populariser. En outre, des problèmes sont survenus, comme cités précédemment, avec les cas de MT Gox ou Bitfinex, illustrant le fait que l'écosystème de cette technologie n'est pas encore complètement sûr. La sécurité est essentielle pour gagner la confiance d'un grand nombre d'utilisateurs et de garantir sa pérennité du système. Sans cela, il restera à un stade marginal.

Enfin, les incertitudes juridiques qui règnent autour de ces technologies ne favorisent pas leur adoption. En effet, il est impossible d'imaginer vouloir appliquer le droit traditionnel, comme certains gouvernements tentent de le faire, par analogie à l'environnement numérique. Ainsi, ce flou juridique enveloppant ces innovations peut être extrêmement dommageable, car pourrait pousser les Etats à appliquer les lois traditionnelles qui pourrait limiter, voire supprimer le potentiel de ces technologies en pleine expansion. Des interrogations quant à la responsabilité également émergent. Inéluctablement, un cadre juridique spécifique à l'environnement du cyberespace doit être établi, sans quoi l'incertitude quant au futur de ces technologies sera inévitablement un frein à leur utilisation.

Nous sommes en train d'assister à la naissance de systèmes techniques pouvant révolutionner la société, comme Internet dans le passé. Cependant, des questions légitimes peuvent se poser : -Qui bénéficiera de ces technologies !

- Qui y aura accès !
- Seront-elles bénéfiques à la société ?

Nous vivons un moment crucial, et les décisions prises prochainement détermineront le futur de cette technologie, et de notre monde lui-même.

La Blockchain et ses potentielles applications

André Ribeiro

Projet de recherche en gestion d'entreprise
Baccalauréat universitaire en économie et management

Sous la supervision de
Prof. Dimitri Konstantas
Université de Genève
Geneva School of Economics and Management
Information Science Institute

Information Science Institute
Battelle
7 rt de Drize
CH-1227 Carouge
http://isi.unige.ch/