We-Search

POURQUOI MISER SUR L'AVENIR DU BITCOIN ET DE LA CRYPTOMONNAIE EN GÉNÉRAL ?

Alexandre MILLET *

We-Search Journal I Revue 2022

2022 I pages 66-69

ISSN : 2684-596

Pour citer cet article :

MILLET, Alexandre, « Pourquoi miser sur l'avenir du Bitcoin et de la cryptomonnaie en général ? », in *We-Search Journal*, 2022, pp. 66-69

http://www.we-search.be/

* Étudiant de rhéto à Notre-Dame des Champs (Uccle)

Alexandre Millet

POURQUOI MISER SUR L'AVENIR DU BITCOIN ET DE LA CRYPTOMONNAIE EN GÉNÉRAL ?

On entend souvent parler de cryptomonnaies de Bitcoin et de Blockchain, des termes qui nous sont pour la plupart inconnus mais qui ont pourtant l'air si important. Un certain nombre de questions sont liées au monde des cryptomonnaie et la plupart de ces questions rentrent dans la problématique « Pourquoi miser sur l'avenir du Bitcoin et de la cryptomonnaie en général ? », c'est donc la problématique de mon travail.

Qu'est-ce que le Bitcoin ?

Le Bitcoin est une monnaie décentralisée qui repose sur la technologie blockchain et sur un large réseau d'ordinateurs connectés via internet. Ce réseau se base sur un programme informatique en P2P, « *peer-to-peer* » ou « pair-à-pair ». Un réseau en peer-to-peer est définit comme « un modèle de réseau au sein duquel chaque point de connexion est à la fois un client et un serveur »[1]. Grâce à ce réseau, le Bitcoin peut se passer d'entité régulatrice : contrairement aux banques, il est décentralisé.

Ce logiciel est dit « *open source* », ce qui veut dire que n'importe qui peut voir le code et y apporter des modifications s'il le désire. Ce logiciel est donc constamment amélioré par des développeurs bénévoles mais ces derniers ne font que proposer leurs modifications et chacun est libre d'utiliser la version du logiciel qu'il préfère. On considère qu'une modification est adoptée lorsque plus de 50% des utilisateurs utilisent la version comprenant ladite modification.

Technologie blockchain

La blockchain (ou « chaîne de bloc » en français) est une sorte de registre public listant les transactions dans des blocs. N'importe qui peut consulter ce registre public à n'importe quel moment. Les blocs de la blockchain peuvent être considérés comme les pages de ce livre de compte. Un bloc contient son empreinte numérique, l'empreinte numérique du bloc précédent et un certain nombre de transactions. Le bloc n'est valide que si plusieurs blocs y sont rattachés.

Les transactions dans la blockchain se font d'adresse électronique à adresse électronique, avec cette adresse est créée une clef privée qui permet au réseau de vous identifier. Ainsi pour envoyer un bitcoin, il faut se connecter à son adresse électronique : le réseau détectera alors que c'est vous via votre clef privée, et vous indiquez ensuite l'adresse à laquelle vous désirez faire un virement et le nombre de bitcoin que vous voulez envoyer. Vous pouvez bien sûr envoyer un demi,

---

[1] BELFIORE, Guillaume, « P2P, qu'est-ce que c'est ? » https://www.futura-sciences.com/tech/definitions/internet-p2p-1924/ définition peer-to-peer

un dixième, un centième, un millième de bitcoin voir même un Satoshi qui est la plus petite unité liée au Bitcoin : il faut en réunir 100 millions pour obtenir un bitcoin entier. Dans la blockchain, chaque transaction est visible de tous, il est possible de voir l'adresse qui envoie des bitcoins, combien elle en envoie et à quelle adresse.

Grâce à la technologie blockchain le Bitcoin est décentralisé, on supprime la nécessité d'avoir un tiers de confiance entre acheteur et vendeur. Lorsque vous faite un virement à un vendeur, l'information passe d'abord par la banque et celle-ci exécute ensuite le virement en envoyant l'argent au vendeur. De plus il faut payer la banque pour ses services. Or en utilisant le Bitcoin et donc la blockchain, la transaction se fait directement entre acheteur et vendeur.

Le minage et les mineurs

Les blocs de la blockchain sont minés. Là où les banques fabriquent leur monnaie avec des planches à billet ou via des crédits, le Bitcoin lui créé de la monnaie via le minage. Il est défini comme ceci : « le minage désigne le procédé de validation des transactions faites sur une blockchain »[2].

Les mineurs sont des personnes qui fournissent leur puissance informatique au réseau de la *blockchain* pour calculer le hachage, effectuer la preuve de travail et ainsi valider des transactions dans « l'archive publique ». En échange de leur puissance, le réseau les récompense en bitcoin (le nombre évolue mais aujourd'hui on parle de 6,25 bitcoins par bloc validé). La création de bitcoins a donc pour but de financer le minage et donc assurer le bon fonctionnement du réseau. Sachant qu'un bloc est miné toutes les dix minutes, la création monétaire du Bitcoin est transparente. De plus, il a été décidé à la création du Bitcoin qu'il n'en existerait jamais plus de 21 millions, potentiellement dans le but de créer de la rareté.

Systèmes de sécurité

Le réseau Bitcoin est sécurisé par 3 grands mécanismes :

1) Le hachage est une empreinte digitale unique créée lors de la création d'un bloc, ce hachage contient donc les informations du bloc précédent mais également les informations contenues dans le bloc, si quelqu'un tente de modifier les informations du bloc son hachage changera également et il sera invalidé par le réseau qui remarquera ce changement.

2) La preuve de travail (*Proof-of-Work* ou PoW) consiste en bref à prouver que votre ordinateur a travaillé à la création d'un bloc, cette preuve prend près de dix minutes par bloc ce qui rend donc la manipulation de ces blocs encore plus difficile car si un individu désire manipuler un bloc existant il devra recalculer toutes les preuves de travail des blocs suivant.

3) Finalement, une des meilleures sécurités de la blockchain est que c'est un réseau *peer-to-peer*. Le « registre » est public et tout le monde peut y avoir accès à n'importe quel moment. De plus lorsque

---

[2] GAYTE, Aurore, « Qu'est-ce que le minage de crypto-monnaie, exactement » https://www.numerama.com/tech/791931-quest-ce-que-le-minage-de-cryptomonnaie-exactement.html

qu'un nouveau bloc est créé il est automatiquement envoyé et vérifié par toutes les personnes du réseau.

Pour manipuler la blockchain, il faudrait donc recalculer le hachage ainsi que la preuve de travail de chaque bloc suivant celui qu'on veut manipuler mais il faut également que la majorité des Membres du réseau considère votre bloc comme légitime (ou 51% de la puissance totale du réseau). Il est donc pratiquement impossible de manipuler la blockchain aujourd'hui, c'est d'ailleurs pour ça que les seuls piratages liés au Bitcoin se sont toujours faits en piratant des plateformes d'échanges ou en tout cas des intermédiaires et jamais la blockchain directement.

Altcoin

Dans le monde des cryptomonnaies il n'existe pas que le Bitcoin mais également les Altcoins. Le terme Altcoin désigne littéralement toutes les cryptomonnaies qui ne sont pas le Bitcoin. La première Altcoin à avoir été créé fut le Namecoin mais la plus connue à l'heure actuelle est l'Ethereum qui est aujourd'hui la deuxième cryptomonnaie la plus importante en termes de capitalisation boursière. En 2020 il existait plus de 2000 Altcoins et aujourd'hui on estime qu'il en existe plus de 5000[3]. Ce qu'il faut comprendre avec les Altcoins est que celles-ci ne cherchent pas toujours à être des concurrents directs au Bitcoin car certaines de ces cryptomonnaies sont spécialisées dans d'autres domaines. Il existe donc différentes utilités (tellement qu'il me serait impossible de toutes les citées) certaines utilités peuvent être surprenantes, en voici une liste non-exhaustive :

1) Il y a les cryptomonnaies qui ont le rôle de monnaie (BTC). Ces cryptomonnaies ont vocation à être utilisées comme n'importe quelle monnaie, pour payer des biens et services et faire des virements.

2) Ensuite il y a les cryptomonnaies spécialisées dans la vie privée (XMR), elles rendent l'utilisateur encore plus anonyme qu'il ne l'était déjà avec le Bitcoin.

3) Les Cryptomonnaies en tant que plateforme (ETH). Celles-ci fournissent la technologie blockchain à d'autres cryptomonnaies en leur donnant accès à leur propre blockchain.

4) L'utilisation dans le but de stockage dans un cloud (SWM). Avec ces cryptomonnaies vous pouvez acheter de l'espace de stockage décentralisé à votre guise.

Polémiques autour des cryptomonnaies

Le Bitcoin et les différentes cryptomonnaies font parfois l'objet de doutes ou de remises en question. Ces remises en question sont parfois très pertinentes et servent à faire évoluer le monde des cryptomonnaies. Voici donc certaines de ces remises en question et doutes ainsi que leurs réponses.

Pollution

---

[3] BELFIORE, Guillaume, « Altcoin: qu'est-ce que c'est ? », Définition | Altcoin - Alternative coin | Futura Tech (futura-sciences.com)

Un des aspects le plus souvent reprochés aux cryptomonnaies est leur impact sur l'environnement. Il est vrai que le Bitcoin pollue énormément, cette pollution vient essentiellement du système de *proof-of-work* qui est très énergivore. En effet le système *proof-of-work* implique qu'un grand nombre d'ordinateurs tente de résoudre des calculs très complexes en espérant trouver la solution en premier.

Pour résoudre ce problème de pollution, un nouveau système est envisagé pour remplacer le *proof-of-work*, il s'agit du *proof-of-stake* (preuve d'enjeu). Le *proof-of-stake* n'incite pas les mineurs à effectuer de puissants calculs constamment pour espérer trouver un bloc. Avec un système de *proof-of-stake*, l'utilisateur doit mettre en jeu ses tokens, ou jetons, de la cryptomonnaies en question. Ce montant est considéré comme une « preuve de participation », un montant minimal requis et ce dernier varie selon les *blockchains*. Le *proof-of-stake* repose sur l'idée qu'une personne en possession d'une grande quantité de tokens a intérêt à ce que la *blockchain* de cette cryptomonnaies soit sécurisée. Ainsi, plus un mineur met en jeu un grand nombre de tokens, plus il a de chances d'être sélectionné pour découvrir le prochain bloc et ainsi récupérer la récompense comme pour les mineurs.

Ce système à l'avantage d'être largement moins énergivore mais il est également moins sécurisé, raison pour laquelle il n'est pas adopté par toutes les *blockchains* bien que Ethereum ait prévu de l'utiliser dans la prochaine mise à jour qui se met en place petit à petit mais pour laquelle nous n'avons pas de date précise.

Ordinateur quantique

Ces temps-ci, on entend parfois parler d'ordinateurs quantiques et de comment ils pourraient détruire tout le réseau de n'importe quelle cryptomonnaie. Bien que nous n'ayons pas encore atteint la suprématie quantique (maîtrise de la puissance d'ordinateurs quantiques), il est possible que nous l'atteignions avant 2140, date à laquelle on estime que les 21 millions de bitcoins auront été minés. Un ordinateur quantique est un ordinateur qui effectue des opérations en parallèle plutôt que l'une après l'autre comme nos ordinateurs classiques, ce qui leurs offre une puissance de calculs largement supérieure à ce qui existe aujourd'hui.

Un ordinateur quantique pourrait donc trouver n'importe quel mot de passe via le brut-force. Le brut-force est une technique consistant à tester toutes les combinaisons possibles jusqu'à trouver la bonne, théoriquement un ordinateur quantique pourrait également réunir assez de puissance pour égaler 51% de la puissance total du réseau Bitcoin et donc en prendre le contrôle.

À première vue ce problème parait insurmontable mais en réalité la blockchain resterait visible de tous donc tous les participants assisteraient à la fraude et le Bitcoin perdrait toute sa valeur car les utilisateurs ne pourraient plus lui faire confiance. Quelqu'un en possession d'un ordinateur quantique n'aurait donc aucun intérêt à vouloir pirater la blockchain Bitcoin puisqu'il serait devenu le maitre d'un Bitcoin ne valant plus rien.

Piratage

Certaines personnes craignent de se faire pirater et de perdre toutes leur cryptomonnaie. Il faut savoir que la blockchain n'a jamais été piratée, tous les piratages se sont toujours faits via des

tiers (plateforme d'échange, téléphone volé, etc.). Quelqu'un qui suivrait les recommandations de sécurité ne risque à priori rien ou pas grand-chose.

État et cryptomonnaie

Les relations entre États et cryptomonnaies sont compliquées. D'un côté il y a ceux qui désirent limiter, contrôler, voir interdire les cryptomonnaies, et d'un autre, il y a ceux qui misent dessus pour l'avenir voire même qui en feraient leur monnaie nationale.

Un certain nombre de pays ont tenté de faire interdire le Bitcoin, si aucun n'a réussi jusqu'à maintenant c'est parce qu'interdire le Bitcoin est quasiment impossible. Pour bloquer le Bitcoin il serait envisageable d'interdire toutes les plateformes d'échanges en ligne mais cette manipulation ne marcherait que si tous les pays décidaient simultanément d'interdire les plateformes d'échanges. Il est donc très peu probable que des pays comme les États-Unis, la Russie, la Chine, le Japon et l'Europe se mettent tous d'accord sur le sujet. Si un pays décidait seul de bannir les plateformes d'échanges ça n'aurait pratiquement pas d'impact. Cette réticence des pays vis-à-vis des cryptomonnaies peut avoir plusieurs explications : pollution, méconnaissance de la technologie, risques... Cependant je pense que ce qui fait pencher la balance est le fait que les pays ne veulent pas perdre la souveraineté sur la monnaie utilisée dans leur pays.

Pour ce qui est des pays favorables aux cryptomonnaie il y a deux cas intéressant à analyser. Comme mentionné plus tôt, et cela pourrait en surprendre plus d'un, un pays a bel et bien reconnu le Bitcoin comme monnaie légale. Il s'agit du Salvador qui a reconnu le Bitcoin comme l'une de ses monnaies légales le 9 juin 2021. Dans ce pays, près de 30% de la population est dite « dé-bancarisée », ce qui veut dire qu'elle n'a pas de compte en banque et donc pas de carte bancaire. Ainsi 30% des habitants ne pouvaient transmettre de la valeur qu'avec de la monnaie fiduciaire (monnaie physique), le Bitcoin règle donc ce problème en facilitant les échanges de valeurs. Ce problème d'échanges de valeurs n'existe pas qu'au Salvador mais aussi dans un certain nombre de pays d'Afrique pour qui le Bitcoin pourrait également être une solution.

Ensuite, avec la situation actuelle en Ukraine, les cryptomonnaies ont un rôle important à jouer. Le compte Twitter officiel de l'Ukraine a fait un appel aux dons en bitcoin. La population fait également appel aux individus en leur demandant des dons en cryptomonnaies car la quantité d'argent qu'ils peuvent retirer de leurs comptes bancaires est limitée, par exemple le Bitcoin a permis à des Ukrainiens de quitter le pays en achetant une voiture en bitcoins.

De potentiels impacts politiques

D'un point de vue politique le Bitcoin pourrait également avoir un rôle à jouer. D'abord il pourrait être un substitut au dollar dans les cas de « dollarisation de l'économie ». C'est un phénomène qu'on observe lorsque la population d'un pays n'a plus confiance en la monnaie de ce dit pays, les citoyens n'en veulent plus, les commerçants ne l'acceptent plus et elle perd énormément de valeur. Aujourd'hui lorsque ce genre d'événement se produit, l'opinion publique a tendance à se diriger vers le dollar américain pour remplacer leur monnaie, mais on peut imaginer que dans le futur, le Bitcoin aura un rôle à jouer dans ce genre de situation.

Ensuite certains pays moins développés économiquement que les pays occidentaux ont parfois un fort taux de population dé-bancarisée. Le Bitcoin pourrait régler ce problème par la même occasion comme évoquer précédemment car pour utiliser le Bitcoin il ne faut qu'un accès à internet. Nous avons également pu observer que le Bitcoin pouvait jouer un rôle dans des guerres comme avec le conflit entre l'Ukraine et la Russie.

Conclusion

Je reconnais le fait que le sujet ne soit pas le plus facile à aborder et à comprendre pour la majorité des gens et qu'il faille fournir un effort pour pouvoir entrer dans le monde des cryptomonnaies. J'admets également que les cryptomonnaies ne sont pas sans défaut, que ce soit la pollution occasionnée, les risques d'arnaques ou de vols si la technologie n'est pas bien maîtrisée.

Malgré tout, les cryptomonnaies apportent plus de bénéfices qu'elles ne causent de problèmes. Ces dernières apportent avec elles de nouvelles technologies révolutionnaires et peuvent régler un certain nombre de nos problèmes actuels, que ce soit la dé-bancarisation, le manque de confiance en un pouvoir central ou simplement l'envie de transparence et de liberté.

Les cryptomonnaies sont porteuses d'innovations et ont le potentiel de révolutionner des domaines aussi variés que la monnaie, l'art, les transactions bancaires ou le stockage de données et notre manière de penser internet de manière générale. Petit à petit, le Bitcoin se fait une place dans nos vies et commence à être utilisé par d'importants acteurs économiques mais est surtout de plus en plus accepté par la population à travers le monde, et on observe l'apparition de commerces acceptant d'être payé en bitcoin. Bien sûr, quand je dis qu'il faut miser sur l'avenir du Bitcoin et de la cryptomonnaie en général je ne veux pas dire qu'il faut investir toutes ses économies dans le Bitcoin mais plutôt qu'il faut garder un œil sur les avancées dans le domaine, et pousser pour que ces technologies soient reconnues à leur juste valeur et pas simplement vues comme des escroqueries.

En conclusion, malgré leurs défauts, je pense qu'il faut miser sur l'avenir du Bitcoin et de la cryptomonnaie en général, ces dernières répondent à certains problèmes actuels et permettent à la société d'évoluer dans des domaines variés

---

BIBLIOGRAPHIE

Articles et ouvrages

ACCO, Laurent, « Ordinateur quantique : qu'est-ce que c'est ? », *Futura Sciences,* https://www.futura-sciences.com/

AMMOUS, Saifedean, *L'Etalon-Bitcoin : L'alternative décentralisée aux banques centrales*, Dicoland (LMD), 2019, 318 pages

BELFIORE, Guillaume, « P2P, qu'est-ce que c'est ? », *Futura Sciences*, www.futura-science.com.

BELFIORE, Guillaume, « Altcoin: qu'est-ce que c'est ? », *Futura Sciences*, www.futura-science.com.

GAYTE, Aurore, « Qu'est-ce que le minage de crypto-monnaie, exactement », *Numerama*, https://www.numerama.com/

HELBIG, Jens, *De la blockchain à crypto-investisseur : Comprendre la technologie blockchain et investir stratégiquement dans le Bitcoin, l'Ethereum, le Ripple & Co.*, GbR C. Klein & J. Helbig, 2019, 148 pages

LA CALME, Stéphane, « Le bitcoin a consommé plus de 134 TWh en 2021 », 3 janvier 2022, *Developpez,* https://www.developpez.com/

QUOISTIAUX, Gilles, « Bitcoin la nouvelle religion », *Trends Tendances*, 21 octobre 2021, https://trends.levif.be

RAY, « Bitcoin : le point sur l'anonymat », *ContrePoints*, 2 juin 2014, https://www.contrepoints.org/

ROUKINE, Serge, *Comprendre et utiliser le Bitcoin*, 19 éditions, 2013, 124 pages

LARS, Ludovic, « Clés privées, clés publiques et adresses dans Bitcoin », *Cryptoast*, 10 novembre 2018, https://cryptoast.fr/

s.a., « Miner des bitcoins, rentable ? », *BitcoinCours*, https://www.bitcoincours.com/

s.a., « Qu'est-ce que la blockchain », *Blockchain France*, https://blockchainfrance.net/

s.a, « Proof of Stake, le consensus idéal ? », *Greenbull Campus,* https://greenbull-campus.fr/

Vidéos

Cryptoast, « COMPRENDRE LA BLOCKCHAIN EN 7 MINUTES », 8 mai 2019, YouTube (vidéo), https://youtu.be/6uYRN6b5EMU

HASHEUR, « Le BITCOIN reconnu comme MONNAIE légale | El Salvador », 9 juin 2021, YouTube (vidéo) https://youtu.be/YC9wEyaOi3s