Les Bitcoins et leur fonctionnement

par

Simon Bergeron (15 047 931)

Mathieu Morissette (18 105 328)

Travail présenté à

Gabriel Girard

Dans le cadre du cours

IFT630 : Processus concurrents et parallélisme

DÉPARTEMENT D'INFORMATIQUE

UNIVERSITÉ DE SHERBROOKE

12 Avril 2021

Table des matières

Introduction 3

Revue de la littérature 4

Bitcoin et la monnaie 5

- La monnaie 5
- Les caractéristiques d'une bonne monnaie 5
- Le Bitcoin 6
- Les avantages du Bitcoin 7
- Le fonctionnement général du Bitcoin 9

Le Blockchain, la technologie derrière Bitcoin 11

- Le but du blockchain 11
- Les systèmes centralisés versus décentralisés 12
- La cryptographie 14
- La structure de données 16
- Le « mining » 19
- L'algorithme 21
- Choisir la chaine « officielle » 23

Perspective future pour le blockchain et la cryptomonnaie 26

- Le Bitcoin à plus grande échelle 26
- Les autres cryptomonnaies 26
- Le blockchain dans d'autres domaines 27

Conclusion 28

Bibliographie 29

Introduction

Au moment de débuter l'écriture de ce rapport, le Bitcoin venait de franchir la barre des $60 000 USD[1], propulsé par des investisseurs de grand calibre tel que la compagnie Tesla qui a fait l'acquisition de Bitcoins pour une valeur de $1.5 milliard USD[2]. Pour une technologie obscure développée anonymement sous un pseudonyme et qui n'appartient à personne, cela peut être considéré comme tout un exploit.

La population générale commence à savoir ce qu'est le terme Bitcoin, mais ce dernier est généralement associé à de la spéculation boursière et à un mode de paiement pour des activités illicites. C'est peu surprenant, considérant la complexité de cette technologie, autant dans son fonctionnement, que dans son utilisation. Son utilité est également difficile à comprendre sans étudier le sujet plus en profondeur. En étudiant le Bitcoin dans ce document, nous verrons ses avantages uniques comme monnaie et son fonctionnement. Qu'est-ce que le Bitcoin? À quoi ça sert? Comment ça fonctionne? Les questions précédentes sont les lignes directrices de ce document.

Ce rapport s'adresse à tous ceux qui sont intéressés à avoir une réponse détaillée à ces questions. Le contenu du début et de la fin est accessible à tout lecteur, toutefois comme ce texte est fait dans le cadre d'un cours sur la programmation parallèle, la section qui s'intéresse en profondeur au fonctionnement de la technologie derrière le Bitcoin sera plus technique et pourrait être intimidante pour un lecteur ayant peu de connaissances informatiques.

Dans un premier temps, il sera question de bien présenter ce qu'est le Bitcoin. D'où vient cette technologie? Pourquoi faire une telle invention alors qu'il y a déjà plusieurs moyens de payer facilement en ligne avec des services bancaires et des programmes comme PayPal? Comment cette monnaie a-t-elle atteint ce qu'elle vaut aujourd'hui? Comment ça fonctionne de manière générale?

Ensuite, nous approfondirons d'un point de vue beaucoup plus technique le fonctionnement du blockchain, la technologie derrière le Bitcoin, en faisant des liens avec les notions de programmations parallèles étudiés dans le cadre de ce cours.

Finalement, nous conclurons avec un retour sur les perspectives futures du blockchain et de la cryptomonnaie.

[1] https://www.bloomberg.com/news/articles/2021-03-11/bitcoin-approaches-record-high-as-risk-on-rally-accelerates

[2] https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html

Revue de la littérature

Ce rapport est basé sur deux principales références, soient les livres Blockchain Basics et The Bitcoin Standard. Nous avons également le rapport du créateur des Bitcoins comme source directrice. Certains articles pris sur internet sont utilisés pour illustrer des faits avec des exemples et apporter des informations d'actualité dans le rapport.

Le document Bitcoin : A Peer-to-Peer Electronic Cash System, écrit par Satoshi Nakamoto, le créateur du Bitcoin est utilisé comme une de nos sources principales. Ce rapport est disponible à l'adresse web : https://bitcoin.org/bitcoin.pdf

Blockchain Basics est un ouvrage écrit par l'auteur Daniel Drescher et ayant comme but de présenter la technologie du blockchain en 25 étapes. Cet auteur est un banquier professionnel ayant occupé des rôles dans la sécurité informatique dans différentes banques. Il détient un doctorat en économétrie de l'Université de Berlin et une Maitrise en ingénierie logicielle de l'université d'Oxford. Son ouvrage a été révisé par Laurence Kirk, un spécialiste du blockchain ayant une maitrise en informatique. C'est dans ce livre que la majorité des notions techniques du blockchain, qui correspondent à la section deux de ce rapport ont été tiré.

The Bitcoin Standard est un ouvrage écrit par l'auteur Saifedan Ammous et ayant comme but d'étudier le Bitcoin dans une perspective plus politique et économique. Cet auteur est un professeur d'économie à l'Université libano-américaine possédant un doctorat en développement durable de l'université Columbia. C'est ce livre qui est utilisé comme référence principale pour les sections un et trois qui discutent davantage des aspects sociaux et économiques reliés au Bitcoin.

Le dernier livre qui a été consulté est Blockchain : The Next Everything écrit par le journaliste Stephen P. Williams. Il a été consulté pour consolider les informations présenter dans les deux premiers livres, mais ne représente pas une de nos sources d'informations principales.

Finalement les articles issus d'internet proviennent de sources variées dont la fiabilité est variable. Ils ne sont donc pas utilisés comme principales références, mais ont leur utilité pour apporter des informations complémentaires à celles fournies par nos deux livres de référence principaux.

Bitcoin et la monnaie

La monnaie

Pour bien comprendre l'utilité du Bitcoin, il est primordial de s'intéresser à ce qu'est la monnaie. Sans ces notions, il est difficile de cerner les avantages du Bitcoin. Quand on pense à de la monnaie, notre premier réflexe est généralement de penser aux dollars qui sont utilisés dans nos sociétés. À la base, une monnaie est une solution aux problèmes associés à l'échange de biens et de services entre des individus ou des groupes d'individus.

Parmi ces problèmes, il y a le fait que certains biens sont périssables. Un producteur maraicher ne peut se permettre d'accumuler sur le long terme ses fruits et légumes en vue de faire des échanges dans le futur, car ces produits ne se conservent pas indéfiniment. D'autres biens sont indivisibles. Comment quelqu'un qui fabrique des maisons pourra-t-il facilement échanger son bien en échange de produit comme des fruits et légumes? Il serait difficile d'échanger un millième de maison pour des pommes. Il peut également y avoir des incompatibilités entre l'offre et la demande des produits. Si le producteur maraicher souhaite échanger ses fruits et légumes contre des souliers, mais que le cordonnier n'est pas intéressé par ces biens et préfère recevoir du cuir, il sera difficile de procéder à l'échange sans passer par de nombreux intermédiaires.

C'est là que la monnaie intervient en jouant le rôle de l'intermédiaire entre les 2 parties souhaitant faire un échange. Pour que cela fonctionne, elle doit être acceptée par la grande majorité de la population dans laquelle elle est utilisée. Par exemple, si quelqu'un au Canada offrait de payer sa maison en coquillages, il y a peu de chance que quelqu'un accepte sa monnaie, mais le dollar canadien est accepté partout sur le territoire du Canada. En théorie, n'importe quoi pourrait être utilisé comme monnaie, mais comme nous le verrons dans la prochaine section, certains aspects sont importants à considérer dans le choix d'une bonne monnaie.

Comme nous venons de le voir, la monnaie est à la base un concept très simple et logique, mais il est facile de l'oublier lorsque l'on vit dans une grande économie moderne comme celle du Canada, où les dollars sont impliqués dans des échanges et transactions extrêmement complexes.

Les caractéristiques d'une bonne monnaie

Maintenant que l'intérêt d'avoir de la monnaie a été montré, il devient important de s'intéresser à quel médium utiliser comme monnaie. En réponse aux problèmes identifiés dans la section précédente, les principales caractéristiques d'une bonne monnaie sont les suivantes[3] :

- Conserve sa valeur dans le temps

[3] Informations tirées de la référence The Bitcoin Standard

- Suffisamment divisible pour représenter les rapports de valeurs entre les produits à échanger
- Facilement liquidable
- Haut ratio de stock par rapport au débit

Les trois premières caractéristiques sont relativement simples à comprendre. D'abord, une bonne monnaie se doit de se conserver dans le temps, pour permettre d'en accumuler sur une longue période de temps en minimisant le risque de perdre la valeur qui lui est associé. Elle doit être divisible pour permettre la représentation des rapports entre tous les biens présents dans l'économie. Elle doit être facilement liquidable, ce qui implique que la monnaie est globalement acceptée dans la société où elle est utilisée et permet d'obtenir facilement des biens en l'échangeant.

Finalement, la dernière caractéristique qui est très importante à considérer pour avoir une bonne monnaie est un haut ratio de stock par rapport au débit. Cela se traduit à avoir une monnaie qui ne peut pas être créée plus facilement que sa valeur. Par exemple, si nous prenons une petite société isolée qui utiliserait des coquillages comme monnaies d'échange. Supposons que l'acquisition de 20 coquillages prend une journée de travail dans cette société. La valeur des biens de la société en coquillages sera donc adaptée en fonction de la rareté de la monnaie utilisée. Si un étranger arrive dans cette société avec une technologie lui permettant de produire 2000 coquillages par jour, il aura le pouvoir de détruire totalement cette économie primitive, car il lui sera démesurément plus facile de créer de la nouvelle monnaie que de produire des biens et de les échanger avec cette monnaie. Les habitants ayant économisé des coquillages se retrouveraient du jour au lendemain avec des artéfacts valant 100 fois moins qu'il valait auparavant.

Autrement dit, s'il est trop facile de créer de la nouvelle monnaie, cette dernière peut rapidement perdre sa valeur en cas d'une augmentation rapide de son stock. Ce phénomène sera discuté davantage dans la section des avantages du Bitcoin, car le Bitcoin a une quantité maximale fixe qui ne pourra jamais être excédée, en comparaison avec les monnaies gouvernementales qui peuvent théoriquement être imprimées à l'infini, sans que les citoyens ne puissent garantir la protection de leur monnaie face aux conséquences négatives de l'inflation.

Le Bitcoin

Le Bitcoin est une forme de monnaie digitale inventée par un individu ou un groupe d'individus anonyme connu sous le pseudonyme de Satoshi Nakomoto. Le concept a été créé en 2008 et c'est le 3 janvier 2009 que le réseau bitcoin a été déployé pour la première fois[4]. L'idée derrière cette création était de créer une monnaie décentralisée qui permettrait aux individus d'effectuer des transactions

[4] https://fr.wikipedia.org/wiki/Bitcoin

entre eux sans avoir le besoin de passer par un intermédiaire tel qu'une banque. Satoshi mentionne dans l'introduction de son document de présentation du Bitcoin que le fait de devoir dépendre d'institution financière pour faire des paiements en ligne est une faiblesse, car elle implique de devoir partager plus d'information que nécessaire à ces dernières pour pouvoir faire des transactions sécurisées et ne permet pas de garantir complètement une protection contre de la fraude et de la manipulation, notamment par de l'usurpation d'identité. Il mentionne que ces problèmes ne sont pas présents avec une monnaie physique, car elle peut être utilisée sécuritairement sans que les parties soient obligées de s'échanger d'informations personnelles, sans laisser de traces et sans obliger la présence d'un intermédiaire. Cependant, il n'existait pas d'équivalent à cette monnaie physique dans le monde virtuel. Autrement dit, il n'existait pas de mécanismes permettant de faire des paiements sur des canaux de communication sans devoir faire affaire avec un intermédiaire de confiance[5].

C'est dans le but de créer un équivalent à ce type de monnaie physique dans le monde virtuel que Satoshi a créé les Bitcoins. Sa solution était de remplacer cet intermédiaire de confiance par un réseau public basé sur la cryptographie qui garantirait la sécurité, l'intégrité des données et la protection des informations personnelles des utilisateurs. Le système qu'il présente dans son document fonctionnerait et serait sécurisé, tant et aussi longtemps qu'il y aurait plus de personnes honnêtes sur le réseau public que tout groupe qui tenterait de l'attaquer.

Le Bitcoin a commencé son ascension en popularité très lentement, surtout utilisé dans ses débuts par des adeptes de l'informatique. Le principal obstacle résidait dans la complexité de la technologie pour des personnes n'ayant pas de connaissance avancée dans le domaine. Une des premières transactions en Bitcoin a été faite en 2010 par un programmeur nommé Laszlo Hantez pour l'achat d'une pizza de Papa John pour 10 000 Bitcoins, au moment où cette monnaie n'avait pratiquement aucune valeur dans le monde réel. Cette transaction représenterait aujourd'hui l'équivalent de 613 millions pour une pizza. Ce programmeur n'a toutefois absolument aucun regret, car pour que Bitcoin se développe, il était essentiel qu'il soit utilisé dans des transactions réelles et que sans ce type de transaction jamais la valeur du Bitcoin n'aurait pu devenir ce qu'elle est aujourd'hui[6].

Les avantages du Bitcoin

Maintenant que nous avons une idée générale ce que sont les Bitcoins et des caractéristiques d'une bonne monnaie, nous discuterons des avantages de cette

[5] https://bitcoin.org/bitcoin.pdf

[6] https://www.businessinsider.com/bitcoin-surge-means-laszlo-hanyecz-paid-316-million-two-pizzas-2021-3

nouvelle forme de monnaie en le comparant avec les systèmes de monnaie moderne et ceux du passé.

Pendant des milliers d'années, l'or a été utilisé comme la référence en matière de monnaie, car elle présentait toutes les caractéristiques d'une bonne monnaie. L'or se conserve dans le temps sans se détériorer, il est extrêmement malléable et il est possible de le diviser en plus petite pièce en fonction de son poids, il est accepté universellement et il est très rare à trouver, ce qui assure un haut ratio de stock par rapport au débit. Dans le début des grandes banques, la valeur des billets de monnaie était directement indexée à l'or et était échangeable à un prix fixe. Les gens utilisaient donc encore l'or comme monnaie, mais le bien physique était abstrait par des dollars représentés par des billets de banque.

Avec le temps, de nouvelles théories économiques sont arrivées et on produit un détachement de l'indexation du dollar à l'or pour se retrouver avec de l'argent gouvernemental qui peut théoriquement être produit à l'infini et dont la valeur est fixée par différent critère comme la valeur d'échange avec la monnaie d'autres pays. Cela peut avoir des avantages, dans le sens où cela donne une marge de manœuvre au gouvernement pour tenter d'influencer les aléas de l'économie, mais cela peut être catastrophique dans le cas où ce pouvoir d'imprimer de l'argent est mal utilisé par le gouvernement. Le fait que la monnaie soit centralisée dans les mains du gouvernement et qu'elle ne soit pas directement indexée à un bien physique possédant les caractéristiques d'une bonne monnaie implique qu'à tout moment un individu pourrait perdre toute la valeur qu'il a dans ses billets de banque. Bien que ce phénomène soit moins à risque de se produire dans des sociétés plus favorisées économiquement et avec des gouvernements relativement stables, de nombreux exemples de pays ayant eu des scénarios catastrophiques d'inflation existent[7], tels que le Vénézuéla qui a eu entre 2016 et 2019 un taux d'inflation estimé à 53 798 500%, détruisant complètement toute valeur associée à sa monnaie[8].

Notre rapport n'ira pas plus loin dans les théories économiques et la politique derrière ces choix, mais le contexte est important pour bien comprendre la motivation derrière une nouvelle monnaie comme le Bitcoin. Ce qu'on doit retenir c'est que les systèmes de monnaies modernes sont pratiquement tous centralisés et sous le contrôle des gouvernements qui peuvent contrôler la quantité de monnaie, pour le meilleur et pour le pire.

C'est là qu'intervient le Bitcoin. Cette technologie possède tous les avantages d'une bonne monnaie et est complètement décentralisée. Personne ne contrôle Bitcoin, même pas son créateur. Par sa nature digitale, il se conserve indéfiniment.

---

[7] https://www.investopedia.com/articles/personal-finance/122915/worst-hyperinflations-history.asp

[8] https://en.wikipedia.org/wiki/Hyperinflation_in_Venezuela

Les Bitcoins sont aussi extrêmement divisibles. En effet, chaque Bitcoin se divise en 1 000 000 de Satoshi. Considérant qu'il y aura au final 21 millions de Bitcoins, cela donne une quantité d'unité suffisamment grande pour couvrir les besoins de l'économie mondiale et advenant le cas où ce ne serait pas suffisant, rien n'empêcherait théoriquement de rediviser en encore plus d'unité les Bitcoins, sans que cela affecte sa valeur. Comme la quantité maximale de Bitcoins est fixée à 21 millions, il n'y a aucun enjeu par rapport au ratio de stock par rapport au débit, car une fois tous les Bitcoins seront créés, il sera impossible d'en créer de nouveau, garantissant ainsi une protection contre la manipulation de la quantité de monnaie. Pour la liquidité, cela dépendra de son succès dans le futur, mais avec sa valeur actuelle il est très facile d'échanger des Bitcoins pour des dollars américains, ce qui rend cette monnaie facilement liquidable pour le moment du moins. Plus les Bitcoins seront acceptés par la population générale, plus ils seront facilement liquidables.

Le fait que les Bitcoins soient complètement décentralisés protège ses détenteurs de tout contrôle par les autorités, ce qui en fait un investissement très sécuritaire du point de vue de l'inflation et des manipulations monétaires. Toutefois, cette monnaie dépend de la participation des milliers d'ordinateurs qui en assure la survie. Sans ces ordinateurs pour maintenir le réseau Bitcoin, la monnaie ne pourrait pas exister détruisant ainsi sa valeur. Il est donc plus sage de considérer Bitcoin comme ayant le potentiel d'être une monnaie idéale, à la condition de maintenir sa popularité et ses contributeurs. Plus de grandes entreprises comme Tesla investiront dans le réseau, plus le statut des Bitcoins comme monnaie se solidifiera. Également, à mesure que les Bitcoins deviendront plus utilisés, leur valeur devrait inévitablement se stabiliser et ils devraient perdre leur statut actuel d'investissement basé sur de la spéculation.

Finalement, le Bitcoin est très sécuritaire, car c'est un réseau de milliers de machines qui exécute le code en parallèle et donc il n'y a aucun point de défaillance unique et autant de sauvegarde de sureté qu'il y a de machines. Aussi, il est impossible de trafiquer quoique ce soit sans posséder plus de 51% du réseau. Même si c'était le cas, le fait de « pirater » Bitcoin lui ferait perdre toute sa valeur et enlèverais l'intérêt de le faire dans le but de voler de l'argent. Dans le début, ce risque était réel et plus probable, mais avec les milliards de dollars investis dans le réseau et les innombrables machines honnêtes et motivés par le maintien de l'intégrité du réseau dans lequel ils sont investis, il est extrêmement peu probable qu'une attaque de ce type se produise.

Le fonctionnement général du Bitcoin

Le fonctionnement du Bitcoin sera traité en profondeur dans la suite de ce rapport, toutefois avant de rentrer dans les détails techniques, commençons par se donner une idée globale et générale du fonctionnement de cette technologie.

Une unité de monnaie Bitcoin n'a aucune forme physique « détachable », même dans le monde virtuel. Ce que nous voulons dire par là est qu'un Bitcoin fait partie d'une énorme agglomération de donnée et ne peut en être détaché, car son existence dépend de tout le reste de la chaine de données. Bien que cette affirmation puisse sembler évidente, il est important de bien comprendre ce concept, car certaines personnes pourraient penser à tort que c'est l'équivalent d'un fichier ou d'un artéfact informatique virtuel qu'on peut voir ou manipuler. La définition non officielle que nous donnons au Bitcoin dans ce rapport est la suivante : Le Bitcoin est une unité monétaire virtuelle abstraite définie à partir d'un historique de transaction maintenu dans un registre public dont l'intégrité est assurée par la technologie du blockchain.

Autrement dit, la quantité de Bitcoins qu'un individu possède est calculée en regardant l'historique de toutes ses transactions. C'est le montant de Bitcoin reçu moins le nombre de Bitcoins envoyés. Les nouveaux Bitcoins sont créés à partir d'une récompense qui est donnée aux ordinateurs qui assurent le maintien et l'intégrité du registre de Bitcoin. Jusqu'à ce que les 21 millions de Bitcoins aient été « créé », chaque ordinateur qui ajoute un bloc de transactions valide au registre reçoit de nouveaux Bitcoins dans son compte. En plus de cette récompense, les ordinateurs qui ajoutent des blocs de transactions reçoivent un paiement de la personne qui souhaite transférer ses Bitcoins, ce qui assure que les ordinateurs resteront motivés à « miner » des Bitcoins, même lorsque tous les nouveaux Bitcoins auront été créés. Le terme « miner » des Bitcoins, qu'on entend couramment, correspond donc à connecter des ordinateurs et offrir des ressources informatiques au réseau public du Bitcoin en échange d'une compensation qui est payée directement en Bitcoins. Maintenant que nous avons une idée générale du fonctionnement du Bitcoin et de son but, il est temps de plonger dans les détails de sa technologie.

Le Blockchain, la technologie derrière Bitcoin

Le but du blockchain

Derrière Bitcoin se cache le blockchain, la technologie qui rend cette monnaie décentralisée possible en offrant des solutions à des obstacles majeurs issus des enjeux de la programmation parallèle dans un système décentralisé ouvert au public. Le terme blockchain est utilisé pour décrire à la fois la technologie en soi et la structure de donnée qui est utilisée par cette technologie. En général, le terme blockchain dans ce rapport sera utilisé pour faire référence à la technologie et il sera explicitement mentionné lorsqu'on fait référence à la structure de donnée.

En soi, le blockchain a comme simple but fondamental de permettre le maintien d'un registre. En général, l'utilité d'avoir un tel registre dans la vie courante est de protéger la propriété privée. En cas de doute sur la propriété d'un bien, la consultation du registre permet de déterminer qui en est le véritable propriétaire. Toutefois, quand le registre est maintenu par une entité centrale, il y a un risque réel que ce registre soit altéré pour une multitude de raisons. Supposons par exemple une dictature qui confisquerait les fonds de ses opposants politiques, celui qui contrôle le registre peut en faire ce qu'il veut. Dans un monde idéal, le meilleur registre est celui qui est public, donc tout le monde peut le voir et constater toute tentative de manipulation, et décentralisée, personne ne peut modifier ce registre sans que la majorité soit d'accord avec la modification.

C'est ce type de registre que le blockchain implante. Il est à noter que par la nature publique de ce « registre idéal », il est de base beaucoup mieux adaptée conservée des données de nature publique, comme la monnaie. Bien que l'identité des personnes sur le registre puisse être masquée par des pseudonymes, si les « éléments » inscrits dans le registre ne sont pas des transferts de monnaie et ont plutôt un caractère sensible, le fait que le registre soit public peut être problématique. C'est entre autres pourquoi le blockchain est surtout utilisé dans le cas de la monnaie en ce moment, car la monnaie en soi n'est pas une donnée sensible, surtout quand les personnes impliquées dans la transaction sont seulement identifiées par un pseudonyme.

Dans le cas du Bitcoin, ce registre contient la totalité des transactions de Bitcoins effectuée depuis sa création. Malgré que l'idée du registre paraisse relativement simple, c'est le fait de vouloir déployer ce registre sur un réseau « peer to peer » purement distribué qui donne toute la complexité à cette technologie. La prochaine section décrira plus en détail la nature de ce type de réseau.

Ce qu'il faut comprendre c'est que le registre du Bitcoin est public et accessible à tous. Chaque personne possédant un ordinateur peut se connecter au réseau et commencer à interagir avec lui. Il n'y a aucune centralisation, autrement dit, aucun ordinateur du réseau, appelé nœud, n'est supérieur aux autres nœuds en termes de droits et d'accès. Cela implique qu'il n'y a pas de copie « maitre » du registre,

chaque nœud possède sa copie du registre, qui est la structure de données appelée le blockchain. Les nœuds se partagent des informations par message en échangeant des informations avec leur voisinage et éventuellement chaque nœud finit par recevoir toutes les informations, mais pas en même temps ni dans le même ordre. Cela implique que l'algorithme du blockchain est exécuté en parallèle sur des milliers de machines qui ne possèdent aucun chef d'orchestre pour les synchroniser. Également, comme le réseau est public, chaque nœud peut modifier le registre et partager ses modifications au reste du réseau, même si ce dernier a des intentions malicieuses. Heureusement, la technologie du blockchain offre une solution à tous ces problèmes et rend une invention comme le Bitcoin possible.

Les principaux enjeux que le blockchain cherche à résoudre pour permettre l'implantation de son registre dans un réseau décentralisé sont les suivants :

- Un nombre inconnu de nœuds connectés au réseau
- Une identité inconnue des nœuds connectés au réseau
- Une fiabilité inconnue des nœuds connectés au réseau
- Aucune centralisation
- Assurer l'intégrité et la confiance dans un réseau avec les difficultés précédentes

Ces enjeux sont intimement liés à la programmation parallèle, car la nature du réseau du blockchain est d'exécuter ce programme sur des milliers des nœuds en même temps d'une manière qui fonctionne et qui assure l'intégrité des données. Les prochaines sections permettront de montrer comment le blockchain fonctionne en détail et solutionne les enjeux qui ont été soulevés.

Les systèmes centralisés versus décentralisés

Il existe plusieurs architectures de réseaux et de systèmes informatiques. Pour les raisons présentées dans la partie sur le contexte du Bitcoin, avoir un système centralisé pour gérer la monnaie n'est pas toujours souhaitable, car il nécessite inévitablement de faire confiance à l'entité qui contrôle le système. Deux des grandes catégories de réseaux sont les réseaux centralisés et ceux décentralisés.

Comme leur nom l'indique, les réseaux centralisés sont des réseaux possédant une entité centrale. Cette entité centrale est le cœur du système et les autres machines servent à interagir ou effectuer des tâches pour cette entité. Ces réseaux ont plusieurs avantages, il leur est facile de maintenir l'intégrité de leurs données, car les modifications aux données sont contrôlées par l'entité centrale. Ce n'est pas n'importe qui qui peut interagir avec les données et on peut s'assurer que les transactions soumises sont valides et cohérentes sans trop de difficulté, car la copie « Maitre » contient toutes les données officielles et peut faire les vérifications nécessaires avant de modifier ses données. Quand on paye avec notre carte de débit, la transaction est envoyée dans le système central de notre banque qui valide qu'on a le montant nécessaire pour faire la transaction avant de

procéder au transfert de fonds. Mais comment faire ces vérifications, dans un système qui n'a pas cette entité centrale? Qu'est-ce qui empêche à une personne d'effectuer une transaction sans avoir les fonds en utilisant un nœud malicieux ou de s'ajouter de l'argent dans son compte? Comment peut-on faire confiance à un système qui n'a pas de centralisation?

Dans un réseau complètement décentralisé, chaque machine est égale en termes de droit et d'accès et elles doivent s'entendre et se synchroniser pour fonctionner ensemble. Dans le contexte de la monnaie, cela représente une difficulté au niveau de l'intégrité et de la cohérence des données, surtout dans le cas d'un réseau public « peer to peer » purement distribué où tout le monde peut se joindre au réseau et personne n'a vraiment le contrôle ou le pouvoir de faire quoi que ce soit pour corriger manuellement les données. C'est sur ce type de réseau que la technologie du blockchain est faite pour fonctionner.

Ses difficultés sont toutefois son avantage unique : personne n'a le contrôle du réseau et personne ne peut modifier les règles. Comme nous l'avons vu précédemment, les manipulations de monnaie sont fréquentes dans le monde réel et les modifications aux règles du jeu comme l'injection de nouvelle monnaie dans l'économie peuvent venir détruire la valeur de la monnaie déjà possédée par les individus. Avec ce type de système, ces manipulations sont théoriquement impossibles.

Pour pouvoir travailler ensemble, les différentes machines qui composent le réseau du blockchain doivent avoir un moyen de se parler. C'est la communication « peer to peer » par envoi de message qui est la solution utilisée par le blockchain pour assurer la communication entre les différents nœuds du réseau. Chaque nœud voulant se joindre au système du blockchain explore le réseau autour de lui pour se construire un voisinage « d'amis » appelé « peer » en anglais. Une fois cette étape d'exploration terminée, il peut recevoir et envoyer des messages aux membres de son voisinage. Les nœuds finissent tous par être connectés indirectement, par les voisinages de leurs nœuds voisins. Ce système permet à tous les nœuds de s'envoyer des messages via leur « peer ». Toutefois, cette manière de communiquer n'est pas vraiment structurée, étant donnée sa nature décentralisée, et implique que les messages ne sont pas reçus à la même vitesse et dans le même ordre pour chacun des nœuds. Ce sont donc des éléments qui sont nécessaires à prendre en considération dans la réalisation d'un algorithme qui s'exécute en parallèle sur tous les nœuds.

Pour réussir à faire fonctionner ce type de réseau dans le contexte de la monnaie et atteindre le registre idéal décrit précédemment, il est nécessaire de mettre en place un certain nombre d'éléments qui permet à chaque nœud de travailler en parallèle, tout en maintenant l'intégrité des données, la cohérence et la synchronisation. La suite servira à présenter comment chacun de ces enjeux de programmation parallèle est pris en charge par la technologie du blockchain. Ces

éléments sont la cryptographie, la structure de données du blockchain et son algorithme.

La cryptographie

Pour assurer l'intégrité du blockchain, la cryptographie est essentielle. Comment s'assurer que la transaction à ajouter est réellement faite par les personnes concernées? Dans la vie de tous les jours, nous nous identifions pour nos transactions bancaires avec un NIP. Les détails de notre transaction avec notre NIP sont envoyés à la banque centrale qui effectue la transaction dans son registre maitre en s'assurant que nous avons les fonds nécessaires et que notre NIP est le bon. Les transactions font donc affaire avec un intermédiaire, dans ce cas la banque, pour assurer la validité de la transaction à ajouter. Dans un réseau comme Bitcoin, il n'y a aucune autorité centrale pour s'assurer de la validité des transactions. En plus de cet enjeu, de validation d'identité et de transaction, il y a également celui de s'assurer que le registre des Bitcoins ne puisse pas être trafiqué par des nœuds malveillants. Il faut donc s'assurer d'implanter des mécanismes fiable et sécuritaire pour pouvoir fonctionner sans cette autorité. La base de ces mécanismes réside dans la cryptographie.

La principale technique cryptographique utilisée par le blockchain pour assurer l'intégrité de la chaine est appelée hachage. Cela consiste à prendre un ensemble de données et de lui appliquer une fonction unidirectionnelle générant une valeur unique pseudo aléatoire appelé code de hachage. Cette valeur générée n'offre aucun moyen au sens logique de récupérer les données initiales. Par exemple, si on prend la chaine « Hello world! » et qu'on la hache avec l'algorithme sha256 : on obtiendrait le code de hachage suivant : *9ea88f41b044…* À partir de ce code, il n'est pas possible de récupérer les données d'origine.

Cette technique est utilisée dans bien des domaines de l'informatique, notamment dans la protection des mots de passe, mais dans le blockchain elle est utilisée plus spécifiquement comme une étiquette de référence à des données. Par la nature du hachage, modifier les données de la source crée un code de hachage complètement différent. Il est donc possible pour vérifier si des données ont été altérées de créer une étiquette unique associée à ces données qui est le code de hachage. Ensuite, lorsqu'on veut vérifier l'intégrité des données, on a qu'à exécuter la fonction de hachage et à comparer le code obtenu avec le l'étiquette attendue. Si le résultat est différent, cela signifie qu'il y a eu des modifications et que les données ne correspondent pas à l'étiquette. Nous verrons dans la prochaine section comment ces concepts s'appliquent dans la structure de données du blockchain pour garantir l'intégrité de la chaine.

Pour ce qui est de la gestion des signatures digitale, le blockchain utilise une deuxième méthode cryptographique appelée la cryptographie asymétrique. Cette technique consiste à avoir 2 clés partenaires. Chaque clé est en mesure de décoder les messages encodés par l'autre clé. Dans leur utilisation pratique, les

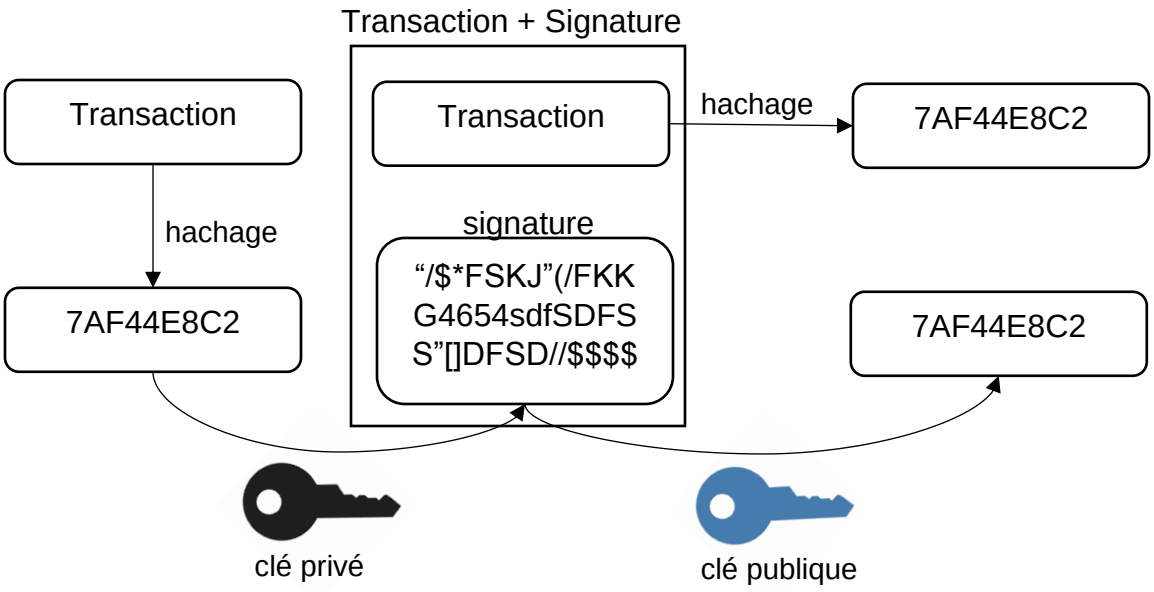
clés sont couramment appelées clé privée et clé publique. La clé privée est seulement connue de son propriétaire et la clé publique est visible aux yeux de tous. Pour envoyer un message privé à quelqu'un, il suffit d'utiliser sa clé publique pour encoder notre message et seul le destinataire sera en mesure d'accéder au contenu de notre message en le décodant avec sa clé. Dans le sens inverse, si le propriétaire souhaite envoyer un message prouvant qu'il en est l'auteur, il encode ce dernier avec sa clé privé et tout le monde pourra décode le message en utilisant sa clé publique, ne prouvant pas le fait même qu'il en est réellement l'auteur.

C'est cette dernière technique qui est utilisée pour la signature digitale dans le blockchain. Les « comptes » de Bitcoin sont identifiés par des clés publiques, connues de tous, dont seul le propriétaire du compte connait la clé privée. Cette clé est le seul moyen de gérer les Bitcoins d'une personne. C'est un mécanisme extrêmement sécurisé, dont les seules faiblesses résultent de l'erreur humaine, soit perdre ou oublier sa clé, ou se la faire voler en dehors du réseau Bitcoin.

Toutes les transactions de Bitcoin doivent être initiées par le propriétaire du compte qui transfère ses Bitcoins vers un autre compte. Il n'y a aucune signature requise pour recevoir des bitcoins à notre adresse publique. Quand un individu souhaite effectuer une transaction sur le réseau, il débute par remplir les détails de sa transaction et génère un code de hachage avec les données de la transaction. Ensuite, il utilise sa clé privée sur ce code de hachage pour générer sa signature qu'il ajoute « en annexe » à sa transaction.

Pour vérifier la signature de la transaction, les nœuds effectuent les opérations suivantes. Ils hachent les données de la transaction à l'exception de la signature. Ensuite, ils utilisent la clé publique du compte d'où proviennent les fonds, qui de manière extrêmement pratique est contenu dans les détails de la transaction, et décode la signature. Si le hachage des données et le décodage de la signature donnent le même résultat, le nœud peut être certain de l'intégrité du message ainsi que de la signature du propriétaire du compte.

Exemple de transaction signé et de sa vérification



Avec ces techniques cryptographiques, nous avons montré qu'il est possible de garantir l'intégrité d'une transaction, d'une manière semblable au travail que fait une banque lorsqu'elle valide le NIP qu'on a entré pour s'identifier, mais sans avoir besoin de la banque. Pour que cela fonctionne, il est essentiel d'avoir une majorité de membres honnêtes sur le réseau qui s'assure de n'accepter que des transactions valides. La validation de la signature digitale est un bon début pour assurer l'intégrité de la chaine et de protéger les comptes d'usurpation. Toutefois, ce n'est pas suffisant, il faut pouvoir s'assurer que la personne qui envoie des Bitcoins a réellement les fonds suffisants et aussi s'assurer que les transactions antérieures ne puissent pas être modifiées. La solution à ces derniers éléments réside dans la structure de données du blockchain ainsi que dans son algorithme.

La structure de données

La structure de données du blockchain est construite à partir des éléments cryptographiques présentés dans la section précédente. Elle consiste en une liste chainée de blocs contenant une référence au bloc précédent. Un bloc est un en-tête contenant les informations suivantes :

- Adresse du bloc précédent
- Estampille
- Racine de l'arbre de Merkel contenant les transactions
- Solution au puzzle de hachage
- Difficulté

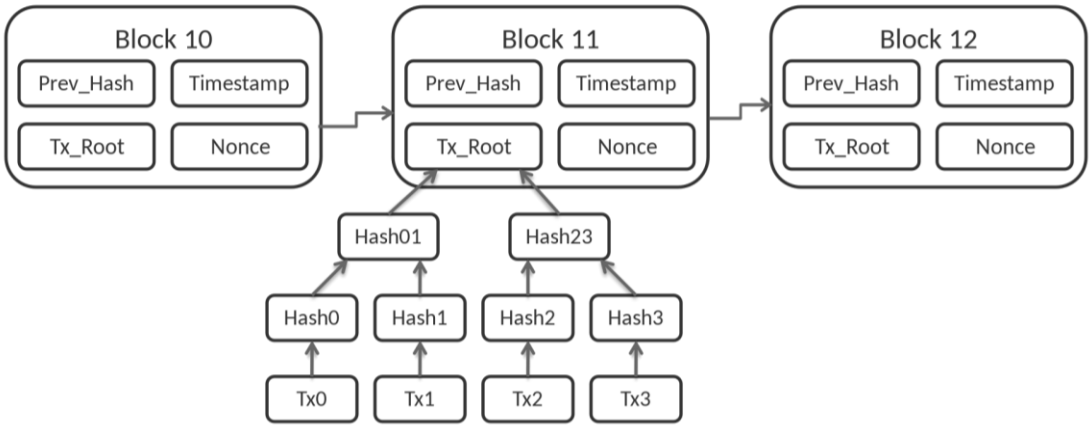
L’estampille correspond à une indication du moment ou le bloc a été créé et permet aux nœuds de déterminer l’ordre de création des blocs de la chaine. Les données de transaction ne sont pas contenues directement dans un bloc, c’est seulement la racine de l’arbre de Merkel associé à ces transactions qui est conservé dans l’en-tête. Cette racine permet de retrouver les transactions associées aux blocs, sans alourdir inutilement la chaine.

Autrement dit, plutôt que d’inclure les transactions directement dans la chaine, seul un code de hachage de référence aux données de transactions est inclus dans l’en-tête. La structure de données pour conserver les données de transactions se nomme un arbre de Merkel. Comme le graphique ci-dessous le montre, il s’agit d’appliquer successivement une fonction de hachage aux transactions, ce qui a pour effet de lier tout le contenu ensemble et de pouvoir identifier toutes modifications aux données à partir du code de hachage de sa racine[9]. Cette méthode permet de vérifier facilement l’intégrité des transactions associées à un bloc. Pour vérifier si les transactions ont été modifiées depuis l’ajout du bloc, il suffit de refaire le processus de hachage successif sur les transactions et de comparer la racine obtenue avec celle qui est indiquée dans le bloc. Si la valeur est différente, les données de transactions ont été altérées.

Chaque en-tête de bloc doit aussi contenir une solution à un puzzle de hachage pour être considéré valide, le champ « Nonce ». Le niveau de difficulté du puzzle est également inclus dans le bloc. Résoudre ce puzzle demande de vraies ressources informatiques et prend du temps. Cela implique que créer un nouveau bloc représente une difficulté qui est nécessaire pour garantir l’intégrité de la chaine, comme nous le verrons plus tard. Les détails de ce puzzle seront donnés dans la section suivante.

[9] https://www.investopedia.com/terms/m/merkle-tree.asp

Représentation graphique de la structure de donnée du blockchain



Source : https://en.wikipedia.org/wiki/Blockchain#/media/File:Bitcoin_Block_Data.svg

Les blocs sont identifiés par un code de hachage obtenu en fonction de leur contenu. Comme nous l'avons vu précédemment, si la moindre modification est faite aux données, ce code de hachage change complètement. C'est ici que la cryptographie vient s'intégrer à la structure de donnée pour permettre la protection de l'intégrité du registre dans son ensemble. La particularité de cette chaine est que, comme un bloc pointe toujours vers son prédécesseur, et que son propre identificateur dépend de l'adresse du bloc précédent, toute modification à la chaine rend toute la suite de la chaine incohérente et invalide.

En effet, modifier le contenu du bloc 10 dans le schéma ci-dessus changerait son code de hachage. Ensuite, comme le bloc 11 contient une référence à ce code de hachage dans son contenu, cela signifie que le bloc 11 contiendra des valeurs légèrement différentes et aura donc lui aussi un nouveau code de hachage. Finalement, le bloc 12 se retrouve dans la même situation que le bloc 11 et doit mettre à jour son code de hachage. On voit donc rapidement que toute tentative de modification d'un bloc rend tous les blocs qui le suivent incohérents.

Les blocs sont donc intimement liés les uns aux autres, il n'y a donc aucune suppression ou modification discrète possible dans cette chaine de données. Supprimer un élément ou modifier ne serait-ce qu'un seul caractère revient à reconstruire toute la chaine à partir du bloc modifié. Comme la création de cette chaine demande de résoudre un puzzle de hachage demandant de vraies ressources énergétiques pour l'ajout de chaque bloc à reconstruire, ce processus devient rapidement impensable à mesure que de nouveaux blocs sont ajoutés par-dessus le bloc qu'on souhaiterait trafiquer. C'est là l'utilité de ce puzzle, qui empêche la reconstruction rapide d'une nouvelle chaine avec des informations trafiquées.

La chaine a donc un caractère permanent, qui enracine de plus en plus les anciennes transactions à mesure que de nouveaux blocs sont ajoutés par-dessus. Cela assure le fait que personne ne peut y apporter de modification ou la trafiquer discrètement. Pour renverser une transaction valide, le seul moyen est de créer une nouvelle transaction valide dans le sens inverse.

Si des nœuds ont mal vérifié ou n'avaient pas assez d'informations pour vérifier l'erreur et qu'ils ont ajouté de nouveaux blocs qu'il pensait valides à la suite de la chaine, tous les blocs qui avaient été créés à la suite du bloc fautif sont perdus. C'est pourquoi comme on le verra dans la section présentant l'algorithme, les nœuds ont tous avantage à bien vérifier les transactions de leurs « peer » pour maximiser la quantité de récompenses qu'ils pourront obtenir et éviter de travailler dans le vide. En pratique, un bloc valide contenant une transaction qui se révèle plus tard comme invalide à la réception d'autres transactions qui avait été effectuée avant n'est pas supprimé. Il est marqué comme invalide, ce qui fait en sorte que les nœuds ignorent est contenu et les transactions sont remises dans la liste à traiter et intégré à de nouveaux blocs. Cela évite de reconstruire la chaine pour des raisons de mauvaise synchronisation et la protection de l'intégrité est tout de même maintenue avec ce processus. Autrement dit, les références dues à ce bloc invalide restent valides, mais les transactions à l'intérieur sont ignorées, ce qui permet de continuer la construction de la chaine.

Bref, la structure de données du blockchain fait un excellent travail pour maintenir l'intégrité des données sur un réseau public constitué de nœud dont on ne connait pas la fiabilité. Le seul moyen de trafiquer la chaine serait d'être prêt à payer un énorme coût en temps et ressource énergétique et de se préparer à convaincre 51% du réseau d'abandonner leur chaine et d'accepter la nouvelle chaine trafiquer, ce qui est hautement improbable.

Le « mining »

On entend souvent le terme miner des Bitcoins. C'est un terme qui est très peu compris par la population en général. Le « mining » fait référence à la récompense obtenue par un nœud lorsqu'il ajoute avec succès un nouveau bloc de transaction à la structure de donnée blockchain. Cette récompense est nécessaire pour motiver les nœuds du réseau à fournir des ressources énergétiques qui sont essentiels pour sa survie.

Pour décourager l'ajout de blocs invalide et assurer la sécurité du réseau en rendant toute modification à la chaine coûteuse en énergie, les nœuds doivent résoudre un puzzle de hachage pour soumettre un bloc à leur voisinage.

Ce puzzle consiste à ajouter un chiffre à la suite de l'en-tête qui, une fois hachée, donne un résultat commençant par un nombre de 0 équivalent à la difficulté courante du réseau. Exemple si les données du puzzle étaient le simple message « Hello World! » avec une difficulté 3, le nœud ajouterait un chiffre à la suite du

message ainsi : « Hello World! 0 ». Il hacherait ensuite le message composé, vérifierait si le résultat du hachage commence par 000 et recommencerait jusqu'à obtenir la chaine souhaitée. Dans ce cas, c'est « Hello World! 614 » qui serait la première chaine solution donnant le résultat commençant par trois zéros : 00068A3C…[10] Trouver le chiffre 614, appelé en anglais « Nonce » demande beaucoup de puissance de calcul, surtout avec des difficultés plus élevées. Par contre, vérifier la validité de cette solution est extrêmement simple pour les autres nœuds qui n'ont qu'une seule opération de hachage à faire.

Comme cette opération de force brute est aléatoire et facilement exécutable en parallèle, elle explique en partie l'engouement pour les cartes graphiques dans les dernières années qui sont grandement utilisées dans ce domaine[11]. Résoudre plus de puzzles plus rapidement signifie de meilleures chances d'ajouter plus de blocs et obtenir plus de récompenses en Bitcoin. Les cartes graphiques sont conçues de manière à avoir une très grande quantité (souvent dans les milliers) d'unités de calcul appelé cœurs. Une grande quantité de cœurs permet un meilleur traitement en parallèle des milliers de pixels et polygones dans le domaine de l'infographie. Par contre, ces cœurs peuvent être utilisés à d'autres effets, comme des opérations de force brute. En comparaison avec une carte graphique, un processeur d'ordinateur possède en ce moment généralement entre 2 et 8 cœurs. Les cœurs d'un processeur sont moins nombreux, mais beaucoup plus rapides et performants que ceux d'une carte graphique. Toutefois dans le cas d'une opération simple comme la force brute, la parallélisation sur plusieurs cœurs a un impact beaucoup plus significatif sur les performances du programme que d'avoir un plus petit nombre de cœurs extrêmement performant. Les « mineurs » qui investissent dans des cartes graphiques ont donc en pratique un meilleur rendement de récompense en Bitcoin que ceux qui utiliseraient seulement les processeurs de leur ordinateur.

Suite à cette constatation, il peut paraitre inutile de se lancer dans le « mining » si l'on est mal équipé. Cependant, comme la résolution du puzzle complètement aléatoire et que chaque nœud peut tenter d'ajouter un bloc qui est différent l'un de l'autre, toutes les machines du réseau ont une chance de soumettre des blocs valides. Par exemple, avec le message présenté précédemment, il aurait fallu 614 essais pour trouver la solution. Supposons qu'un petit ordinateur portable cherche la solution à ces données et qu'il compétitionne avec un nœud ultra spécialisé qui tente de trouver une solution à un message légèrement différent lui demandant 1 000 000 000 d'essais. Même si ce dernier a une puissance de calcul beaucoup plus élevé, cela ne lui garantit pas de toujours gagner la compétition, car chaque nœud construit des blocs légèrement différents les uns des autres selon l'ordre

[10] Exemple tiré de la référence *Blockchain Basics* à la page 91.

[11] https://www.forbes.com/sites/erikkain/2021/01/06/bad-news-graphics-card-prices-are-skyrocketing-and-theres-no-end-in-sight/?sh=61e06aa5594d

dans lequel ils reçoivent les informations de transaction. Cette manière de fonctionner assure une certaine équité entre les nœuds et encourage les petits joueurs à participer au tout plutôt que ce soit juste des personnes ayant investi des milliers de dollars dans leurs équipements informatiques qui amassent des récompenses.

Dans la pratique, les nœuds sont souvent séparés en catégorie où les nœuds complets utilisent des nœuds partiels ou de mineurs pour effectuer certaines tâches de l'algorithme. Dans ce rapport, on parle toujours de nœud complet, mais rien n'empêcherait par exemple à un nœud complet de regrouper un ensemble de petits ordinateurs « mineur » à son service pour résoudre les puzzles de hachage plus rapidement et de se séparer les profits[12].

L'algorithme

Maintenant que nous avons une bonne idée des composantes de la technologie du blockchain, il est temps de s'intéresser au programme que chaque nœud connecté exécute. En intégrant tous les mécanismes présentés jusqu'à maintenant dans cet algorithme, on verra que la synchronisation et l'intégrité du réseau de blockchain sont possibles, même dans des conditions difficiles comme un réseau composé d'un nombre indéterminé de nœuds dont leur fiabilité est inconnu.

L'algorithme qui est exécuté en parallèle sur chaque machine connectée à un réseau du blockchain fonctionne en 2 temps. À tout moment, les nœuds sont soit en train de valider la soumission d'un bloc effectué par un de leur « peer » dans le but de l'ajouter à leur chaine, ou en train d'essayer de créer un nouveau bloc à ajouter à la chaine à partir des transactions qu'ils reçoivent en continu de leur voisinage.

La compréhension de cet algorithme est le cœur du fonctionnement du blockchain et il fait le lien avec tout ce qui a été présenté précédemment pour offrir une solution à ce problème de programmation parallèle. Voici les étapes de cet algorithme[13] :

1. Les nouvelles données de transaction ainsi que les nouveaux blocs sont transmis à tous les nœuds en continu, à partir de l'envoi de messages au voisinage dans le réseau « peer to peer ». Après un certain temps, tous les nœuds connectés aux réseaux finissent par recevoir toutes les données.
2. Chacun des nœuds récupère les nouvelles transactions dans sa « boite aux lettres » et les sélectionne en vue de les traiter (de créer un nouveau bloc contenant ces transactions pour les ajouter à la chaine)

[12] https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/

[13] Étapes tirées de la référence Blockchain Basics aux pages 159-160.

3. S’ils reçoivent plutôt un nouveau bloc dans leur boite aux lettres, ils commencent immédiatement à le traiter en priorité absolue.
    a. Le traitement d’un nouveau bloc consiste à valider trois éléments :
        i. La solution du puzzle de hachage
        ii. La signature digitale est valide
        iii. La transaction est cohérente avec le reste de la chaine (donc le compte qui veut transférer ses bitcoins a les fonds suffisants)
    b. Si le bloc est invalide, il est rejeté par le nœud qui retourne à sa tâche de créer des nouveaux blocs
    c. Si le bloc ne contient pas d’erreur, le nœud l’ajoute à sa copie de la chaine.
        i. Le nœud retire les transactions contenues dans le bloc valide de sa « boite aux lettres », car ces transactions sont déjà traitées.
4. Lorsque le nœud n’est pas en train de vérifier de nouveaux blocs soumis par ses « peer », il se concentre à la création de son propre bloc.
    a. D’abord, il analyse les transactions en s’assurant qu’elles sont valides.
        i. La signature digitale est valide
        ii. La transaction est cohérente avec le reste de la chaine
    b. Si une transaction est invalide, elle est rejetée.
    c. Le nœud construit ensuite un arbre de Merkel avec les transactions valides (Tel que présenté dans la section sur la structure de donnée)
    d. Le nœud se met ensuite à créer son nouveau bloc à ajouter en tentant de résoudre le puzzle de hachage (Tel que présenté dans la section sur le « mining »)
    e. Dès que le puzzle est résolu, il envoie le nouveau bloc créé à tous les autres nœuds du réseau, par le même type de communication par message qui est utilisé pour partager les transactions à tout le réseau.
    f. Si le bloc est valide et accepté par les autres nœuds, le nœud ayant construit le nouveau bloc recevra le montant des frais pour chacune des transactions contenu dans son bloc comme récompense.
5. Si plus tard, un bloc ajouté à la chaine est identifié comme invalide (par exemple, supposons qu’un nœud ait traité une transaction qui lui paraissait valide avec les informations qu’il avait entre ses mains, mais qu’une transaction incohérente avec son bloc ayant eu lieu avant est reçue dans le mauvais ordre. Par exemple, la transaction ayant eu lieu avant fait en sorte que le compte est vide et ne peut effectuer la transaction qui a été soumise et validée dans le bloc)

a. le bloc est marqué comme invalide dans la chaine, il n'est pas réellement supprimé , mais le fait de le marquer invalide fait en sorte que ses transactions sont ignorées par les nœuds.
b. Les transactions associées aux blocs sont remises dans « la boite aux lettres » des nœuds.
c. Le nœud ayant ajouté le bloc rendu invalide perdra sa récompense.

C'est avec cet algorithme que les Bitcoins sont possibles. Une de ses particularités est qu'il résout le problème du « double spending », qui a été illustré dans l'exemple donné à l'étape 5. Ce problème se présente dans le cas où on pourrait dépenser de l'argent qu'on ne possède pas en raison de la nature décentralisée du réseau. On verra dans la prochaine section que la chaine finit par converger après un certain temps et que tous les messages et blocs finissent par être reçus par tous les nœuds. Toutefois, il y a un délai avant d'obtenir cette convergence qui pourrait normalement être exploitée par un individu mal intentionné. Supposons qu'on a un compte avec 100 Bitcoins, et qu'on effectue 2 transactions consistant à transférer 100 bitcoins vers un autre compte dans deux régions éloignées du réseau. Lorsque les régions respectives feront leur traitement de la transaction, ils verront que la transaction est valide, car le compte contient la quantité de Bitcoins nécessaire pour faire la transaction et aura le temps d'ajouter un bloc à la chaine. Toutefois lorsque toutes les transactions auront été reçues par tous les noeuds, l'incohérence sera détectée. En effet, seule la première des deux transactions (identifié avec une estampille permettant d'identifier l'ordre) sera considérée valide et la deuxième devra être abandonnée.

L'étape 5 est cruciale dans la mesure où elle offre une solution au fait que les nœuds ne soient pas tous synchronisés et reçoivent les messages dans des ordres différents. Il faut remarquer que par la nature de la structure de données du blockchain, il est toujours possible de reconstruire l'historique de toutes les transactions et de détecter les incohérences qui peuvent apparaitre avec les nouvelles transactions. Autrement dit, cet algorithme règle le problème inhérent de la synchronisation entre différentes machines qui s'envoient des messages de manière non ordonnée lors de l'exécution en parallèle du programme de blockchain. Il reste cependant un dernier élément à expliquer, comment les nœuds s'entendent-ils sur la version officielle de la chaine à développer quand chacun travaille sur sa propre copie locale?

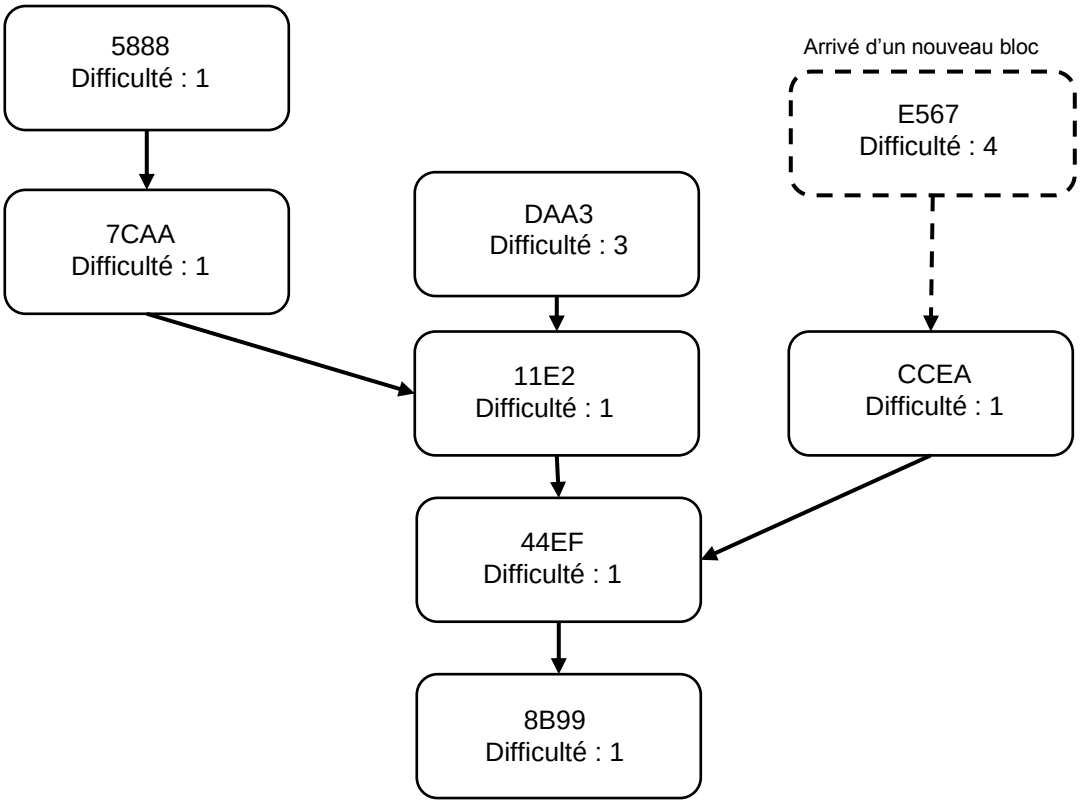
Choisir la chaine « officielle »

Avec le fonctionnement de l'algorithme présenté précédemment et la nature d'un réseau « peer to peer » purement distribué, il est possible, voire inévitable, que différentes versions locales de la chaine émergent. Cela se produit quand deux blocs valides sont intégrés à la chaine dans différentes parties du réseau. Comme il n'y a pas d'unité centrale pour décider quelle version de la chaine sera celle qui

sera poursuivie, les nœuds sont en théorie libres de continuer sur la branche qu'ils veulent. Toutefois, la récompense de la transaction ne peut être donnée plus d'une fois et les nœuds n'ont donc pas intérêt à continuer à consacrer leur temps de calcul dans une branche qui sera abandonné par la majorité des autres nœuds.

Pour régler ce problème de branches multiples, les nœuds, lorsque vient le temps de compétitionner pour ajouter un nouveau bloc à la chaine, choisissent toujours la branche la plus « lourde », c'est-à-dire la branche avec le plus haut degré de difficulté total pour résoudre le puzzle de hachage, ce qui représente aussi, dans la réalité, la branche ayant nécessité le plus d'électricité à générer.

Exemple de chaine avec plusieurs branches



Supposons qu'un nœud se connecte au réseau et obtient par message de son voisinage la chaine ci-dessus. Le nœud a théoriquement 3 choix de branches sur lesquels il peut travailler à créer et ajouter un nouveau bloc à la chaine : 5888, DAA3 et CCEA. Toutefois en calculant le poids des branches disponible, la branche centrale qui a comme tête DAA3 est la plus « lourde » avec un poids de 6 et a le plus de chance d'être celle que les autres nœuds continueront de développée également. Il est donc judicieux de se concentrer sur cette branche et d'ignorer les 2 autres qui seront probablement abandonnés. Par contre, supposons que le nœud reçoit une nouvelle information qui indique que le bloc E567 a été ajouté à la chaine. Après avoir vérifié la validité du nœud avec l'algorithme décrit précédemment, le nœud aura avantage à changer de branche

et tentera de faire progresser la nouvelle branche qui est la plus lourde maintenant la plus lourde avec un poids de 7[14].

Cela a l'effet de l'équivalent d'un vote de la majorité sur la chaine « officielle » à utiliser. Après un certain temps, le fait que la majorité des nœuds sont honnête et « penses » de la même façon amènera la convergence vers une même branche et les autres seront abandonné créant des blocs orphelins. Ces blocs ne sont pas supprimés de la chaine, ils sont juste marqués comme invalides et ignorés par la suite. Comme les récompenses des transactions sont inscrites directement dans les blocs ajoutés, les récompenses associées à ceux qui sont abandonnés par la majorité disparaissent. Comme les nœuds ayant ajouté les blocs maintenant orphelins n'auront pas leur paiement d'inscrit dans la chaine principale, ils devront retenter leur chance sur la nouvelle branche la plus lourde pour ajouter des blocs. Les nœuds, motiver par l'obtention de récompenses en Bitcoin, ont donc intérêt à suivre le choix de branche de la majorité pour espérer faire des profits. Cela implique que pour compromettre l'intégrité de la chaine et forcer une branche qui pourrait contenir des informations invalides, il faudrait posséder plus de 51% des nœuds, ce qui aurait théoriquement été possible dans les débuts de Bitcoin, mais qui est fortement improbable dans un réseau de l'ampleur de Bitcoin aujourd'hui.

Pour ce qui est des transactions, l'algorithme garantit qu'aucune transaction ne soit oubliée et que chacune finisse par être intégrée à la chaine. Comme ces dernières possèdent des estampilles, il est toujours possible de reconstruire l'ordre de toutes les transactions effectuées, même si les transactions peuvent apparaitre dans un ordre différent dans la chaine. Autrement dit, cette logique pour choisir la chaine officielle vient régler le dernier problème non résolu identifié au début de ce chapitre, soit celui de synchroniser les versions locales des chaines que les nœuds conservent. Il n'y a donc explicitement en soi aucune chaine « maitre », mais comme la majorité des nœuds sont honnêtes et motivés par les récompenses en Bitcoin ils finissent tous par s'entendre implicitement sur la version officielle de la chaine.

Avec tous ces mécanismes garantissant l'intégrité des données et la synchronisation, il devient possible d'exécuter le programme en parallèle sur des milliers de machines, dans un réseau où personne ne se connait et où personne n'a besoin de se faire confiance. Avec la cryptographie, la structure de donnée blockchain et l'algorithme, les machines réussissent à se synchroniser sans avoir besoin de coordination centrale, et fournissent un registre dont l'intégrité est protégée par une majorité bienveillante et motivée par le succès de Bitcoin qui est la monnaie qui sert directement à payer pour leur contribution.

[14] Exemple base sur la référence Blockchain Basics à la page 72.

Perspective future pour le blockchain et la cryptomonnaie

Cette courte section servira à discuter de quelques enjeux attachés aux Bitcoins, mais hors du but principal de ce rapport.

Le Bitcoin à plus grande échelle

Un des enjeux pour le futur du Bitcoin est sa capacité à être utilisée à une plus grande échelle. Actuellement, le réseau bitcoin est limité à ajouter des blocs de 1 méga-octet toutes les 10 minutes. Cela représente une capacité de traitement dans les environs de 400 000 transactions par jours, ce qui pourrait devenir problématique si cela devenait la monnaie la plus utilisée au monde.

Certaines propositions pour régler ce problème, comme celle d'augmenter la taille des blocs ont été soumises, mais pour changer quoi que ce soit au réseau Bitcoin, il est nécessaire d'avoir plus de 51% des nœuds qui acceptent le changement. Comme l'augmentation des tailles de blocs pourrait avoir des impacts négatifs sur les récompenses en Bitcoin des mineurs, aucune tentative d'augmenter la taille des blocs n'a réussi jusqu'à maintenant.

Une autre solution envisagée est d'utiliser les Bitcoins comme une monnaie sur lesquels les banques baseraient leur réserve d'argent. Dans ce scénario, les Bitcoins seraient principalement utilisés pour les gros échanges entre les banques et la majorité des gens continuerait à utiliser des billets de banque pour leurs transactions quotidiennes. C'est un principe qui est déjà mis en place sur des sites de loterie qui accepte le Bitcoin comme paiement. L'utilisateur utilise ses Bitcoins pour s'acheter de la monnaie sur le site et utilise la monnaie du site pour la loterie. À la fin, il échange cette monnaie pour des Bitcoins. Cela limiterait beaucoup le nombre de transactions de bitcoin effectué par jours.

Bref, il y a plusieurs solutions possibles pour régler cet enjeu et seul le futur pourra nous dire laquelle sera utilisée.

Les autres cryptomonnaies

Un autre aspect intéressant à considérer est le fait que plusieurs cryptomonnaies se développent autour de Bitcoin. Certaines utilisent même directement le code du Bitcoin adapté à leur monnaie. En soi, la différence entre le Bitcoin et les autres cryptomonnaies réside principalement dans l'ampleur des infrastructures qui les gardent actives. La plus grande force de Bitcoin est qu'il y a déjà énormément de ressources et d'investissement sur le réseau, ce qui lui donne un avantage significatif sur les autres au niveau de sa légitimité et de son utilisation. Le Bitcoin est probablement la cryptomonnaie la plus facilement liquidable sur le marché présentement et s'il continue à se développer à son rythme actuel, il y a de bonnes chances qu'il demeure au sommet.

Aussi, certaines cryptomonnaies ne respectent pas parfaitement le principe de décentralisation totale ou n'ont pas une quantité fixe. Les créateurs de la

cryptomonnaie Ethereum en 2015 ont renversé une transaction considérée comme une attaque sur leur réseau, ce qui a causé la création de deux réseaux distincts. Ceci est un exemple d'un cas où une cryptomonnaie n'est pas complètement décentralisée étant donné que ses créateurs ont pu renverser une transaction faite sur le réseau. Il est clair que dans ce cas, c'était une attaque, mais il demeure que cela brise le principe original du Bitcoin de n'avoir aucun élément de centralisation et aucun pouvoir d'altérer le registre[15].

Certaines cryptomonnaie comme le Dogecoin n'ont tout simplement pas de quantité maximale, donc elles perdent certains des avantages qui font du Bitcoin une excellente monnaie. Le fait d'avoir une quantité illimitée peut être un pari risqué au niveau de l'inflation comme il a été discuté dans la première partie de ce rapport[16]. Bref, le Bitcoin, étant la première cryptomonnaie et la plus acceptée, lui donne d'excellentes chances de demeurer la référence en la matière, surtout qu'elle commence à être utilisée par de grandes entreprises comme Tesla.

Le blockchain dans d'autres domaines

La technologie du blockchain inspire beaucoup d'autres utilisations possibles dans d'autres domaines, mais il demeure qu'elle a été créée pour les Bitcoins et c'est dans le domaine de la monnaie qu'elle excelle. Les principaux obstacles à son utilisation résident dans le fait que maintenir un réseau blockchain est très couteux et qu'un registre public et visible aux yeux de tous n'est pas toujours souhaitable.

Dans le réseau Bitcoin, les nœuds sont motivés à fournir leur ressource informatique, car ils reçoivent une compensation en Bitcoin directement à partir du réseau auquel ils contribuent, ce qui les motive encore plus à continuer à ce dernier. Dans d'autres types d'utilisation non reliés à la monnaie, il pourrait être difficile de récompenser les nœuds, mais certaines idées verront probablement le jour pour solutionner ce problème.

Finalement, la nature des transferts de monnaie n'est pas quelque chose qui est privé en soi, mais dans des scénarios ou le blockchain serait utilisé pour des transactions contenant des données sensibles, la nature publique du registre pourrait devenir problématique. Certaines solutions imaginent de changer la nature du blockchain à cet effet, ce qui peut être une bonne idée dans certains cas, mais à ce moment-là, certains pourraient considérer qu'on parle d'une technologie différente du blockchain. Bref, le blockchain est optimisé pour la monnaie et bien que la technologie inspire plusieurs domaines, il demeure incertain de l'impact qu'il aura sur ces derniers.

---

[15] https://levelup.gitconnected.com/how-ethereum-reversed-a-50-million-dao-attack-cee528d8c030

[16] https://medium.com/@decryptmedia/what-is-dogecoin-and-should-it-be-taken-seriously-b71d7e11105f

Conclusion

En conclusion, le Bitcoin est une invention ayant le potentiel de révolutionner le monde de la monnaie. Dans le premier chapitre, nous avons présenté les raisons qui font du Bitcoin une excellente monnaie et les motivations derrière sa création.

Dans le deuxième chapitre, nous avons présenté le fonctionnement du blockchain et montré que cette technologie permet d'assurer l'intégrité et la confiance dans un réseau purement distribué, même dans les pires conditions. Les enjeux de la programmation parallèle qui est omniprésente dans ce type de réseaux ont été soulevés et liés avec les solutions offertes par cette technologie. Pour la communication entre les programmes parallèles, le blockchain utilise les messages transmis dans un voisinage par une méthode « peer to peer » qui assurent que tous les nœuds finissent par recevoir tous les messages après un certain temps. Pour la synchronisation, le blockchain ne tente pas de synchroniser tous les nœuds pour effectuer l'ajout de toutes les transactions dans le bon ordre, comme le ferait une banque, mais offre plutôt une manière algorithmique et propre à la structure de donnée du blockchain pour corriger les erreurs issues de la synchronisation telles que le problème du « double spending ». Au niveau de l'intégrité des données et de la sécurité, nous avons présenté les méthodes cryptographiques utilisées dans cette technologie .

Finalement, dans le troisième chapitre, nous avons discuté de certains sujets connexes qui dérivent de l'invention du Bitcoin. Avec tout l'engouement actuel pour les Bitcoins, il sera très intéressant de suivre son développement dans les prochaines années. Est-ce que Bitcoin réussira à devenir le nouveau standard monétaire comme l'or l'a été pendant de longues années? Seule l'épreuve du temps nous le dira.

Bibliographie

Livres:

1. Daniel Drescher. *Blockchain Basics : A Non-Technical Introduction in 25 Steps*. Apress, 2017.
2. Saifedean Ammous. *The Bitcoin Standard : The Decentralized Alternative to Central Banking.* Wiley, 2018.
3. Stephen P. Williams. *Blockchain: The Next Everything.* Scribner, 2019.

Articles sur internet:

1. Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf, 2008.
2. Olivia Raimonde. *Bitcoin Hits Another Record and Leaves Other Asset Classes Trailing. https://www.bloomberg.com/news/articles/2021-03-11/bitcoin-approaches-record-high-as-risk-on-rally-accelerates,* 2021.
3. Steve Kovach. *Tesla buys $1.5 billion in bitcoin, plans to accept it as payment*. https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html, 2021.
4. Anonyme. *Bitcoin.* https://fr.wikipedia.org/wiki/Bitcoin, 2021.
5. Anonyme. *Hyperinflation in Venezuela.* https://en.wikipedia.org/wiki/Hyperinflation_in_Venezuela, 2021.
6. Zahra Tayeb. *Bitcoin's surge beyond $60,000 means the famed programmer Laszlo Hanyecz effectively paid $613 million for 2 pizzas.* https://www.businessinsider.com/bitcoin-surge-means-laszlo-hanyecz-paid-316-million-two-pizzas-2021-3, 2021.
7. Matthew Johnston. *Worst Cases of Hyperinflation in History.* https://www.investopedia.com/articles/personal-finance/122915/worst-hyperinflations-history.asp, 2019.
8. Jake Frankenfield. *Merkle Tree.* *https://www.investopedia.com/terms/m/merkle-tree.asp.* 2020.
9. Erik Kain. *Bad News: Graphics Card Prices Are Skyrocketing And There's No End In Sight. https://www.forbes.com/sites/erikkain/2021/01/06/bad-news-graphics-card-prices-are-skyrocketing-and-theres-no-end-in-sight/?sh=61e06aa5594d.* 2021.
10. Matthew Beedham. *All you need to know about Bitcoin network nodes.* https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/, 2019.
11. Spreeha Dutta. *How Ethereum Reversed a $50 Million DAO Attack!.* https://levelup.gitconnected.com/how-ethereum-reversed-a-50-million-dao-attack-cee528d8c030. 2019.
12. Decrypt. *What is Dogecoin and should it be taken seriously?. https://medium.com/@decryptmedia/what-is-dogecoin-and-should-it-be-taken-seriously-b71d7e11105f, 2020.*