

**20/04/2020**

**Travail personnel Hiver 2020**

**Sujet 2 : Blockchain et systèmes d’information décentralisés**

**Par :**

Fofana Moussa (1955968)

Cours : Conception Logiciel

Sigle : **LOG2410**

Présenté à : Mr Françoit Guibault

École Polytechnique de Montréal

Table des matières

[Introduction 3](#_Toc38259103)

[1- Les chaînes de blocs et ses principaux composantes 3](#_Toc38259104)

[1.1- Description générale 3](#_Toc38259105)

[1.3- La racine de Merkle 6](#_Toc38259106)

[1.4- L’horodatage 6](#_Toc38259107)

[1.5- Nonce cryptographique 6](#_Toc38259108)

[2- La preuve de travail 7](#_Toc38259109)

[2.1- Les avantages de la preuve de travail 8](#_Toc38259110)

[2.2- Les inconvénients de la preuve de travail 9](#_Toc38259111)

[3- Autres domaines d’application de la Blockchain 10](#_Toc38259112)

[3.1- Domaine de la santé et de l’industrie pharmaceutique 10](#_Toc38259113)

[3.2- Domaine de la finance des marchés 11](#_Toc38259114)

[Conclusion 11](#_Toc38259115)

[Références 12](#_Toc38259116)

# Introduction

Les transactions traditionnelles, c’est-à-dire ceux que nous effectuons dans nos activités quotidiennes comme, des échanges, des achats en ligne, des transferts d’argent à nos proches, nécessite l’intervention des institutions financières que nous considérons comme un tiers digne de confiance pour traiter nos opérations. Alors que ce système fonction très bien, il comporte plusieurs défaillances au niveau de son fonctionnement. Il est très sensible aux différentes crises financières, il est proie aux attaques cybercriminelles et aussi on note le coût élevé des frais de transactions. Au vu de tous ces failles de ce système, s’impose le besoin d’avoir un moyen de transaction plus sûr qui utilise des méthodes cryptographiques au lieu de la confiance en un tiers intervenant et qui mettra les utilisateurs à l’abri des problèmes que les mécanismes habituels rencontrent. C’est dans ce contexte qu’on a vu une émergence des cryptomonnaies dont le plus célèbres est *Bitcoin* développé en 2009 par une personne ou un groupe de personne sous le pseudonyme de Satoshi Nakamoto. Dans un email Satoshi Nakamoto affirmait « *I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party*.»[1] ce qui serait alors une première application de Blockchain appelé en français les chaine de bloc.

La technologie de la chaîne de blocs permet de se passer d’un organe central en mettant la participation des utilisateurs du réseau pour valider une transaction. La fiabilité absolue de ce nouveaux système repose sur des calcules très complexes qui nécessite une consommation et un temp élevé.

Dans ce travail nous allons voir dans un premier temp les principaux mécanismes qui sont à la base des systèmes distribué basée sur les blockchain et pourquoi ceux-ci nécessitent des calculs complexes, et ensuite nous nous pencherons sur la manière dont ces concepts pourraient être appliqués dans d’autres domaines autres la cryptomonnaies et les conditions qui feront que le temps de calculs peuvent êtres justifiés.

1. Les chaînes de blocs et ses principaux composantes
   1. Description générale

Le blockchain est une base de données partagée et sécurité où les données sont entreposées de façon chronologique comme des blocs reliés entre eux[2] dont la cohérence interne est maintenue par un consensus de tous utilisateurs qui sont actuellement sur le réseau. Il ne nécessite pas l’intervention d’une tiers personnes à qui il faut faire confiance comme les institutions financières et gouvernementale mais qui est contrôlé par tous les intervenant du réseau. Dans un tel contexte aucune transaction ne pourra être modifiée une fois effectuée. Chaque bloc est relié au bloc qui lui précède par une méthode cryptographique. La figure suivante nous montre un aperçu d’une chaîne de blocs.

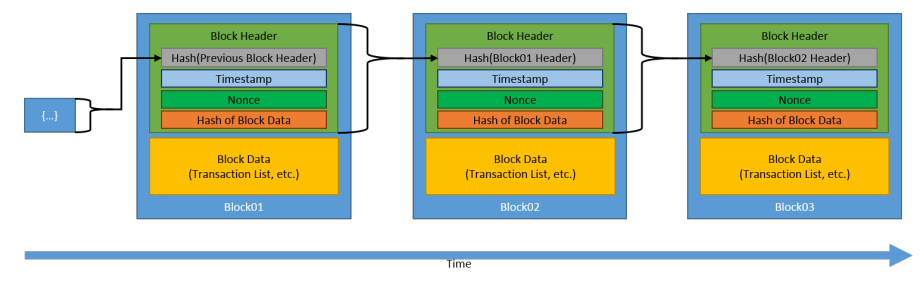


Figure 1: un exemple de chaines de blocs [3]

La structure des chaînes de blocs comportes plusieurs composantes complexes qu’on peut observer sur cette figure.

* 1. La fonction de hachage

La fonction de hachage est la composante la plus importante de la technologie de chaînes de blocs. Il consiste à appliquer une fonction de hachage de la cryptographie sur une donnée et produit un message en sortie qu’on appelle *digest*. Quelque soit la taille de la donnée passée à la fonction elle fournit une fixe pour la sortie. La blockchain du bitcoin utilise l’algorithme SHA-256 comme algorithme de hachage, cet algorithme fournie une valeur hash de sortie dont la taille est fixe et représentée sur 256 bits pour n’importe quelle taille de la donnée passé à l’algorithme, ceci dit, il existe 2256 1077 valeurs possibles qui presque le nombre d’atome dans l’univers. La valeur hash représente *une empreinte digitale* de la donnée ayant fournie cette valeur et elle est unique. Tout changement à la donnée input entraine une valeur hash totalement différente. Le valeur hash est très aléatoire et n’a aucun lien avec l’entrée qui lui est associé de ce fait il est impossible de l’anticiper. La table suivante nous des exemples de valeurs hash associée à des entrées fournies un petit programme que vous trouverez en annexe 1.

**Tableau 1 : Quelques valeurs hachage produites par SH-256 associées à des entrées**

|  |  |
| --- | --- |
| Entrées | La valeurs Hash |
| Moussa Fofana | 719f754bd51f695f44b6b4fc41ba2ba076c8ed3a4555daabf3ab53647361b8d5 |
| moussa Fofana | aac8870567847236adcadba8ada5b29f877d700c2fe54feab163010008de3bc2 |
| Moussa fofana | 2ec41817f609fcfc0733eb802eff6f8dcc65f5f80384c105e45a5f378b2a8d71 |
| a | ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb |
| les chaines de blocs sont des technologies merveilleuses | e3043e0e15b4dcf0bec7d99a6e4e48c37c20ca398c9523435384cd1ed6baf0de |

Dans ce tableau la sortie a une taille fixe peu importe la taille l’entrée et tout changement même mineur entraine une sorties totalement différente.

Les fonctions de hachages ont des propriétés très importantes qui garantissent leurs niveau de sécurité que sont :

Resistance à la préimage : Cette propriété garantit le fait qu’il est impossible de trouver un message associé à une valeur hachage donnée par exemple pour une valeur hachage h donnée trouver m tel que hachage(m)=h. Cela signifie que les fonctions hachages sont à sens unique.

Resistance à la seconde image : Cette propriété stipule que pour un message donné il est impossible de trouver un autre message qui produit la valeur hachage que le premier.

Resistance à la collision : En cryptographie, on appelle collision, le fait d’avoir la même valeur hachage associée à plusieurs entrées. D’où cette propriété nous garantit qu’il impossible de trouver deux messages qui soient associés à la même hachage par exemple trouver x, y tel que hachage(x)=hachage(y).

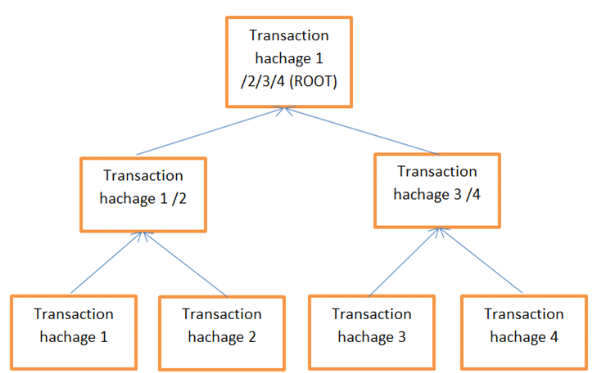
* 1. La racine de Merkle

Figure 2: un arbe de Merkle[4]

L’arbre de Merkle ou arbre de hachage est une structure de donnée inventé en 1979 par Ralph Merkle. Il permet de structurer un grand nombre de données en vue de les accéder et de les vérifier aisément et plus rapidement. Les données sont hachées et combinées entre elle jusqu’à ce qu’on une hachage commune au groupe ce qui est appelée la racine de Merkle. La figure ci-contre nous montre une petite illustration.

* 1. L’horodatage

L’horodatage est le fait d’associer un évènement, une information et une donnée à une date et une heure, en vue de les localiser dans le temps. Le principal objectif de l’horodatage est de vérifier l’intégrité des blocks minés. Ainsi lorsque l’horloge du mineur est dérégler le block est rejeté au-delà d’une certaine marge d’erreur.

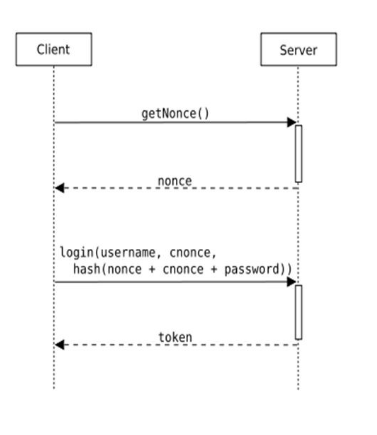
* 1. Nonce cryptographique

Figure 3 : Diagramme d’interaction pour trouver nonce[5]

Nonce cryptographique qui est l’en anglais de «*Number only used once »* est un nombre arbitraire qu’on utilise une et une seul fois il est combiné avec l’entrée pour produit une valeur hachage unique par conséquent on peut représenter la fonction par l’équation suivante : hachage(input+Nonce)=digest. Tous les mineurs de la blockchain se lancent une course pour trouver le nonce qui satisfait une condition particulière, tel nonce est appelé ***Golden Nonce***. Un mineur qui trouve un tel nonce aura le droit d’ajouter le bloc à la chaîne et gagne une récompense en bitcoin. Pour trouver ***Golden Nonce*** les mineurs testent et rejettent environ un million de Nonce chaque seconde. Le processus pour trouver le golden nonce est la Preuve de travail que nous verrons en détail plus tard. La figure ci-contre nous montre un diagramme d’interaction pour trouver le nonce.

1. La preuve de travail

La preuve de travail permet à un utilisateur d’ajouter un block à la chaîne de blocs après avoir résolu une casse-tête informatique et mathématique très complexe et aléatoire. Le mineur qui trouve la solution à cette casse-tête *« la preuve »* est récompensé de son effort et des ressource qu’il a consommé. Il s’agit pour les mineurs de trouver le golden nonce comme annoncé précédemment. Une fois le bon nonce trouvé, la vérifie une processus très facile et ne nécessite pas la consommation de ressource. Il s’agit de résoudre le problème des ***« généraux de Byzantins ».***

En effet, une méthode commune de cette casse-tête est de trouver une valeur hachage qui soit inférieure à une valeur cible donc une valeur qui commence par un certain nombre zéro. Pour trouver cette valeur cible, les mineurs procèdent à une variation de nonce, il faut qu’il trouve un nonce parmi 232 valeurs possibles qui vérifie la condition posée par la casse-tête. Cette variation entraine des valeurs hachages totalement différente du block et cette multiple variation des valeurs hachage des blocs devient un processus très intense et coûteux en terme d’énergie et de temps. Il faut noter aussi que la valeur cible peut être modifiée pour ajuster la difficulté du casse-tête afin de trouver une la valeur hachage adéquate chaque dans un intervalle de temp souhaité et cela peut être fait en augmentant ou en diminuant la valeur cible c’est-à-dire en augmenter ou en diminuant le nombre de zéros par lequel elle commence. Dans le cadre du bitcoin, cette difficulté est réajuster chaque 2016 blocks pour que le temps d’addition de block soit 10 minutes en moyenne[6].

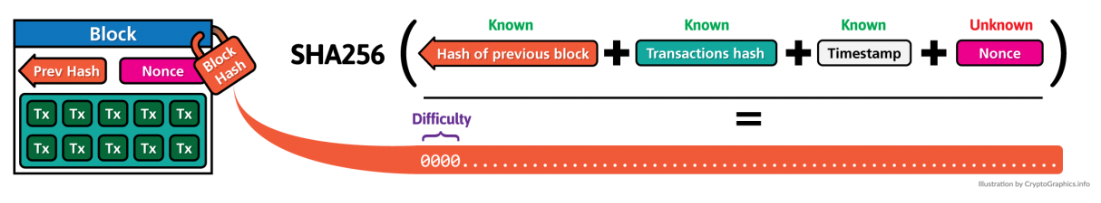


Figure 4: une preuve de travail pour ajouter un bloc à la chaine [7]

Par exemple pour trouver une valeur hachage associée au mot ‘Blockchain’ qui commence par sept 0 c’est-à-dire ‘0000000’ prendrait 934 224 175 nombres de nonce d’essaies dans un vieux système. En effet le mineur commence à tester des nonces à la fois en commençant par 0 jusqu’à trouver le bon nonce. La résolution de ce problème peut prendre presque 1 heure 18 minutes dans le même système[8].

Après la preuve de travail, le mineur soumet le block ainsi trouvé au nœud du réseau. Une vérification sera effectuée par l’ensemble des utilisateurs du réseau. Donc la validation d’un block à la chaîne est constitué de deux grandes étapes que sont : La preuve du travail (PoW) très complexe en terme de calcul et gourmand en énergie et une étape de vérification simple. On peut alors résumer le processus en cette équation : **consensus= preuve de travail+ vérification.**

En somme la preuve de travail est l’organe centrale qui garantit à la blockchain sa sécurité à travers un processus très complexe et coûteux qui demande d’investir beaucoup de temps. Mais tout le monde ne voit pas ce moyen comme avantageux bien qu’il donne un niveau de sécurité considérable, il est aussi sujet à des critiques sur son gaspillage d’énergie. Nous allons voir en détail les avantages et les inconvénient dans les paragraphes qui suivent.

* 1. Les avantages de la preuve de travail

Le principal avantage de la preuve de travail est qu’elle offre un niveau de sécurité très accru à la chaîne de blocks. En effet, pour falsifier un block N dans la chaine, faut recalculer la valeur hachage du block N et ensuite le chiffré avec le block suivant car nous avons dit que chaque block dans la chaîne contient la valeur hachage du block qui lui précède, ce qui requiert donc un travail très coûteux en terme de calcule. Alors la falsification devient très difficile voire même impossible. En plus de cela,elle donne la possibilité à tout le monde de participer à la résolution du puzzle ce qui fait que la blockchain est démocratisée.

* 1. Les inconvénients de la preuve de travail

Le processus de validation d’un blocs est très complexe et génère une dépense énergétique très énormes souvent comparable à celle d’un pays entiers. En effet, la création d’un block implique que tous nœuds du réseau se lancent dans une compétition de force brute en faisant tourner leurs serveurs et carte graphique a une forte consommation de puissance énergétique et le bloc miné est le résultat du travail d’un seul mineur gagnant et donc des autres mineurs perdants ce qui constitut un gaspillage énorme d’énergie. La courbe suivant nous montre une estimation de consommation d’énergie par le bitcoin.

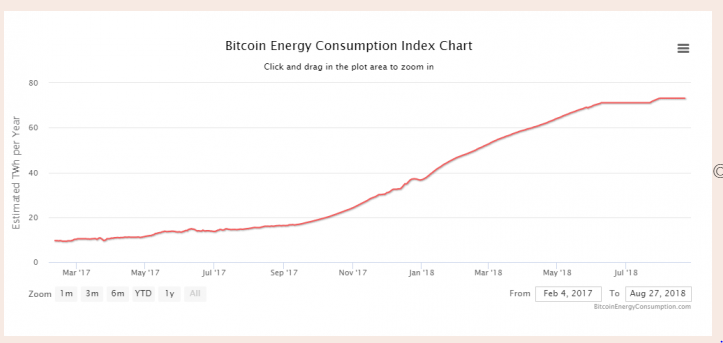


Figure 5: estimation de la consommation d’énergie par le bitcoin [9]

On peut remarquer sur la courbe que le minage de bitcoin a actuellement une consommation annuelle d’environ 73 Twh, un chiffre comparable à celle de la Finlande[9].

Nous assistons à une coopération des mineurs pour former des ferme de minage (*mining pools)* qui dispose d’une très grande puissance de calcul, donc sont privilégié par rapport au particuliers. Cela entraine une centralisation de la blockchain qui peut exposer la blockchain a une attaque de type 51%.

Enfin, le mineur gagnants est récompensé de son travail en équivalent de bitcoin, ce qui peut entrainer une inflation de la crypto-monnaie. Les mineurs ont très souvent tendance à vendre le crypto-monnaie pour combler le déficit créé par la consommation d’énergie.

Nous pouvons donc résumer les inconvénients de la preuve de travail en ces trois points suivants :

* Impact écologique négatif
* Centralisation du réseau
* Inflation et dévaluation de la crypto-monnaie

1. Autres domaines d’application de la Blockchain
   1. Domaine de la santé et de l’industrie pharmaceutique

Le domaine de la santé est un secteur qui peut trouver des améliorations considérable grâce à la blockchain. D’abord, vu sa transparence et son niveau de sécurité accrue, la blockchain peut constituer un outil très robuste pour la traçabilité et l’authentification des médicament, des ordonnances médicale et brevet. L’organisation mondiale de la santé (OMS) a constaté un nombre de personne morte important lié à la prolifération des faux médicament dans les pays de tiers-monde, dans ce contexte la lutte contre les médicaments falsifiés constitut un enjeu majeur pour l’industrie pharmaceutique et la blockchain peut servit comme un moyen très efficace pour lutter contre ce fléau. En effet, la blockchain à travers son modèle consensuel qui est la preuve de travail (PoW) peut permettre d’authentifier, de valider et d’enregistrer un médicament grâce à un réseau de laboratoire ou de pharmacie. Ainsi tous les acteurs peuvent vérifier la provenance et l’intégrité des médicaments.

La blockchain peut permettre de protéger les données médicales des patients qui sont des proies importants des attaques des hackers car présentent une valeur très élevées dans les marché noirs. Grâce à la décentralisation et l’inaltérabilité, la blockchain peut assurer d’une manière plus sûr l’intégrité des données des patients. Cela a été mis en pratique déjà en Estonie par la start-up Guardtime, près d’un million de registres patients a été sécurisés par l’enregistrement des empreintes sur la blockchain en vu de garantir l’intégrité des dossiers[10].

En somme, ces accommodations que bénéficie l’industrie pharmaceutique peuvent justifiées le coût de calcul complexe auquel la blockchain fait recours.

* 1. Domaine de la finance des marchés

Les chaînes de bloques sont des technologies qui fascinent plusieurs secteurs d’activité et la finance ne reste pas en marge de cette opportunité puisque la première utilisation de ces technologies ont permis de faire des transactions de manière sécurisée. La blockchain peut permettre de sécuriser les dérivées OTC et des « *securitie finance »,* elle va permettre une gestion plus transparente en se proposant elle-même comme « *trade repository »* ce qui va permettre de supprimer le flou sur l’identité des régulateurs. En plus la blockchain permet d’enregistrer et d’effectuer des échanges de gré-à-gré entre les entreprises moins cotées en bourse, de cette façon elle donne un moyen de contournement des commissions que ces entreprises devraient s’acquitter. Enfin la blockchain pourrait permettre un assouplissement des financements du commerce international grâce à un « *smart contract »* ceci pourra alors automatiser les paiements des transactions internationales[11].

# Conclusion

La blockchain ou la chaîne de blocs est un registre implémenté dans un modèle distribué. Elle fonction sans l’intervention d’une autorité absolue tel que la banque ou le gouvernement. Elle permet au communauté d’utilisateur d’enregistrer des transactions après un travail très fastidieux en terme de calcul. La technologie de la blockchain fut combinée avec plusieurs autres concepts en informatique pour créer des cryptomonnaies en 2008 dont la première fut le bitcoin. La gestion et le maintien du registre se fait par un groupe d’utilisateur à travers des mécanismes cryptographiques très complexe qui lui confère un niveau de sécurité satisfaisant.

La validation d’un bloc au sein de la chaîne passe par un mode consensuel où les mineurs doivent montrer une preuve de travail. Les mineurs doivent résoudre un casse-tête(puzzle) en utilisant des fonctions de cryptographies dans l’objectif d’avoir des récompenses en cryptomonnaies. Ce mode d’opération met souvent en cause l’importance de cette technologie car elle est jugée non écologique pour sa consommation excessive d’énergie.

Aujourd’hui la technologie de chaîne de blocs va au-delà du contexte de sa première utilisation qui est la cryptomonnaie. Elle s’applique dans plusieurs autres domaines comme dans le domaine de la santé et de la finance des marchés.

Au terme de ce travail, nous avons vu les différents mécanismes à la base de la technologie de la blockchain et comment les calculs complexes font partir intégrante de la solution. Nous avons par la suite vu des exemples d’utilisation dans l’industrie pharmaceutique et dans la finance des marchés. Sachant que la blockchain supprime l’intervention des autorités donc une manière d’éviter les taxes et quelques frais liés au service de transfèrement de fond on peut poser la question à savoir quel sera l’impact sur l’économie mondiale si tout le monde migre sur cette technologie ?

# Références

[1] ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ Satoshi Nakamoto, en ligne <https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/1/>

[2] chaînes de blocs, *Le grand dictionnaire terminologique* , en ligne <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26531717>

[3] NISTIR 8202, *Blockchain technologie overview* , publié en octobre 2018, disponible via <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>

[4]

[5] Frida C., *Salt, Nonces and IVs.. What’s the difference?* En ligne <https://medium.com/@fridakahsas/salt-nonces-and-ivs-whats-the-difference-d7a44724a447> consulté le 16/04/2020

[6]

[7] Proof-of-Work(PoW), disponible [en ligne ] <https://cryptographics.info/cryptographics/blockchain/consensus-mechanisms/proof-of-work/> consulté le 18/04/2020

[8] NISTIR 8202, *Blockchain technologie Overview,* octobre 2018, p. 21

[9] Business AM, *Qu’est-ce que la preuve de travail dans la blockchain?* [En ligne] <https://fr.businessam.be/quest-ce-que-la-preuve-de-travail-dans-la-blockchain/> (consulté 18/04/2020)

[10] Blockchain Partner, *Blockchain et Santé,* [en ligne], <https://blockchainpartner.fr/wp-content/uploads/2017/06/Santé-Industrie-Pharmaceutique-Blockchain.pdf> p.4

[11] Floriane Bobée, *Blockchain et Finance : les cas d’application,* publié le 03 juillet 2019 [en ligne] via <https://bitconseil.fr/blockchain-finance-cas-application/> consulté 19/04/2020