République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Larbi Tébessi - Tébessa

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie

Mémoire de fin d'étude

Pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et informatique

Filière : Informatique

Option : Réseaux et sécurité informatique

Thème

Analyse de la sécurité de la crypto-monnaie

Réalisé par :

Zeghdoudi Dounia

Devant le jury :

Mr. Gharbi Abdelhakim	MAA	Université Larbi Tébessi	Président
Mr. Mahmoudi Rachid	MAA	Université Larbi Tébessi	Examinateur
Dr. Mekhaznia Tahar	MCA	Université Larbi Tébessi	Encadreur

Date de soutenance

13/06/2022

Remerciement

Tout d'abord, je remercie Dieu le Tout-Puissant de m'avoir donné la force morale et physique et de m'avoir permis d'accomplir ce travail.

Je tiens à remercier mon encadrant ***Dr. Mekhaznia Tahar****, pour m'avoir dirigé dans ce travail. Je le remercie pour sa*

Disponibilité, son suivi, ses précieux conseils et son aide.

Je tiens également à exprimer ma gratitude à Monsieur le Président du jury, ***Gharbi Abdelhakim****, et à Monsieur examinateur* ***Mahmoudi Rachdi****, pour l'honneur qu'ils m'ont fait en acceptant d'être porteur de ce modeste ouvrage dont les commentaires et suggestions permettront d'améliorer la qualité de ce manuscrit.*

Merci à mon père, à ma mère, à mes sœurs, à mes frères, pour leur compréhension, leur patience et leur soutien. Alors, à toute ma famille.

Ils ont toujours été la source de mon succès, pour cela je ne saurai jamais comment les remercier.

Je prie Dieu de me les garder le plus longtemps possible

Dédicace

A mes chers parents,

Que nulle dédicace ne puisse exprimer ce que je leurs dois, pour leur bienveillance, leur affection et leur soutien…Trésors de bonté, de générosité et de tendresse, en témoignage de mon profond amour et ma grande reconnaissance « Que Dieu vous garde ».

A mes chères et sœurs

(Yasin, Mohcin, Warda, Jihen)

En témoignage de mes sincères reconnaissances pour les efforts qu'ils ont consenti pour l'accomplissement de mes études. Je leur dédie ce modeste travail en témoignage de mon grand amour et ma gratitude infinie.

A tous mes amis

Pour leur aide et leur soutien moral durant l'élaboration du travail de fin d'études.

A tous ma Famille

A tous ceux dont l'oubli du nom n'est guère celui du cœur…

« De l'union « si » avec « mais » naquit enfant nommé « jamais » »

« Il n'y a pas de « si »ni de « mais », il faut réussir »

DONIA

Résumé

La crypto-monnaie est apparue comme un système de transaction réseau peer-to-peer, utilisant le décryptage pour le créer et le distribuer, il s'appuie sur la blockchain.

Cela garantit un degré élevé de transparence et de vérification de toutes les transactions individuelles à l'aide de mineurs et d'algorithmes de consensus qui s'appuient sur les travailleurs pour vérifier les transactions et leur validité.

Le but de cette recherche est d'expliquer les crypto-monnaies et les transactions de manière sécurisée et d'essayer d'implémenter la blockchain en Java et minimiser le temps de construction de blocs et ce, en se basant sur la POW.

Mot clés : Crypto-monnaies, Blockchain, Bitcoin, Clé publique, Clé privée, Portefeuille électronique.

Abstract

Cryptocurrency emerged as a peer-to-peer network transaction system, using decryption to create and distribute it, it relies on blockchain.

This ensures a high degree of transparency and verification of all individual transactions using miners and consensus algorithms that rely on workers to verify transactions and their validity.

The purpose of this research is to explain crypto-currencies and transactions in a secure way and to try to implement blockchain in Java and minimize block construction time based on POW.

Keywords: Crypto-currencies, Blockchain, Bitcoin, Public key, Private key, electronic wallet.

ملخص

ظهرت العملات المشفرة كنظام معاملات شبكة نظير إلى نظير، باستخدام فك التشفير لإنشائه وتوزيعه، وهو يعتمد على blockchain.

وهذا يضمن درجة عالية من الشفافية والتحقق من جميع المعاملات الفردية باستخدام عمال المناجم وخوارزميات الإجماع التي تعتمد على العمال للتحقق من المعاملات وصلاحيتها.

الغرض من هذا البحث هو شرح العملات المشفرة والمعاملات بطريقة آمنة ومحاولة تنفيذ blockchain في Java وتقليل وقت إنشاء الكتلة استنادًا إلى POW.

الكلمات المفتاحية : العملات المشفرة, البلوكشين, البتكوين, المفتاح العام, المفتاح الخاص, المحفظة الالكترونية.

Table de matière

Chapitre 03 : Etude expérimentale

Chapitre 04 : Tests et résultats

Conclusion générale

Liste des figures

Listes de tableaux

Liste des abréviations

POW	Proof of work
POS	Proof of stake
P2P	Peer to peer

Introduction générale

1 Introduction générale

Les crypto-monnaies sont un nouveau monde qui peut être défini au sens large pour décrire toute la monnaie électronique, y compris les monnaies virtuelles et les crypto-monnaies, qui peuvent être obtenues par voie électronique et numérique et ne sont pas considérées comme des actifs incorporels comme le papier-monnaie ou les pièces.

En 2008, le programmeur Satoshi Nakamoto a annoncé la première crypto-monnaie "Bitcoin".

Les nouvelles crypto-monnaies "Litecoin" et "Ethereum" apparues en 2015 ont levé 75 millions de dollars.

En 2019, Facebook a fait connaître sa célèbre monnaie, Libra, qui devrait être utilisée à partir de 2020.

Notre objectif dans cette recherche est d'analyser la sécurité des monnaies numériques, de comprendre comment les clés sont créées et leur rôle dans la confidentialité des transactions et le chiffrement des données, ainsi que le rôle des algorithmes de consensus, en particulier la protection numérique Proof of Work et Proof of Stake.

Cette thèse se compose de quatre chapitres :

Dans le premier chapitre, nous avons introduit les différents concepts liés aux Monnaie numérique et le deuxième chapitre est intéresser par processus d'extraction de monnaie numérique

Ensuite troisième chapitre est consacré à l’étude expérimentale au sein de laquelle plusieurs tests relative à la block chaine ont été opérés en vue de vérifier sa solidité envers les attaques.

Enfin, le dernier chapitre sera celui qui est appliqué et la simulation avec une discussion des résultats obtenus.

Chapitre 01
Monnaie numérique

1 Introduction

Dans ce chapitre, on parle d'abord ce qu'est une monnaie numérique, son histoire, ses caractéristiques, ses types et ses transactions en monnaie numérique. Enfin on parle du portefeuille de monnaie numériques et de ses types.

2 Monnaie numérique

2.1 Définition

La monnaie numérique est un type de monnaie cryptée qui est stockée sur divers dispositifs de mémoire électroniques. Les paires de trading sont autorisées. [1], Le bitcoin est l'une des monnaies numériques les plus utilisées.

2.2 Historique et origine

Le concept de crypto-monnaie est apparu pour la première fois à la fin des années 1980. L'idée était de créer une monnaie pouvant être envoyée de manière sécurisée et fonctionnant sans l'utilisation d'entités centralisées (telles que les banques). David Chaum, un cryptographe américain, a créé digicash, une monnaie cryptographique électronique anonyme, en 1995.

Il s'agit d'une forme précoce de paiement cryptographique électronique qui nécessitait à la fois un logiciel convivial pour retirer des fonds d'une banque et des clés cryptées uniques pour envoyer des fonds à un destinataire. Nick Szabo a créé Bit Gold en 1998, qui est souvent désigné comme le précurseur immédiat du Bitcoin. Il était nécessaire que les utilisateurs utilisent la puissance de traitement de leur ordinateur pour résoudre des énigmes cryptographiques, et ceux qui réussissaient étaient récompensés. Une récompense a été donnée à ceux qui ont résolu les énigmes. Si vous combinez les notions de Chaum et de Szabo, vous aurez quelque chose qui ressemblera à Bitcoin.

Cependant, Szabo n'a pas été en mesure de résoudre le problème de la double dépense (les données numériques peuvent être copiées et collectées) sans l'intervention d'une autorité centrale. L'histoire de Bitcoin et des crypto monnaies qui vont lui succéder commence une décennie plus tard, lorsqu'une mystérieuse personne (ou un mystérieux groupe de personnes) utilisant le pseudonyme « Satoshi Nakamoto » publie un livre blanc intitulé Bitcoin – A Peer to Peer electronic Cash (Bitcoin : un système de paiement électronique pair à pair) en 31 octobre 2008, décrivant les caractéristiques du réseau blockchain Bitcoin. Satoshi a

commencé à travailler sur le projet Bitcoin le 18 août 2008, lorsqu'il a acheté le nom de domaine Bitcoin.org.

L'histoire de Bitcoin battait son plein. Satoshi Nakamoto a miné le premier bloc du réseau Bitcoin le 3 janvier 2009. Sur le premier bloc, il intègre un gros titre du New York Times afin de continuer à évoquer les réalités économiques qui ont conduit à la technologie Bitcoin. Le Genesis Block (bloc de la Genèse) est désormais le nom du premier bloc de 50 Bitcoins.[2]

2.3 Caractéristiques

Parmi ses caractéristiques les plus marquantes :

- **Décentraliser :** Il n'est sous le contrôle d'aucune organisation ou personne.
- **Anonyme :** Il est possible pour l'utilisateur d'avoir des adresses qui ne sont pas associées à ses informations personnelles.
- Permet un échange sécurisé sans avoir besoin d'un contrôle central. [3]

2.4 Types de monnaie numérique

Parmi les types de monnaie numérique

- **Bitcoin :**

C'est une monnaie numérique qui dépend du crypto dans son émission et sa circulation, elle est décentralisée et personne ne sait qui a inventé le bitcoin. Connu uniquement sous son nom de plume Satoshi Nakamoto. Un Satoshi peut être une personne ou un groupe de programmeurs.

Bitcoin est basé dans sa structure sur un système de monnaie électronique peer-to-peer (P2P). Les bitcoins sont formés dans un processus appelé minage, le nombre total de bitcoins pouvant être produits est limité depuis le début de l'introduction de la monnaie pour laquelle il a été créé (21 millions de pièces) et pas plus que ce qui peut être produit, seulement c'est échangé. [4]

Le prix de la monnaie numérique Bitcoin BTC a récemment baissé de 2,05 % pour atteindre 39977,14 $. En 19 février 2022. [5]

Figure 1: Logo de bitcoin [6]

- **Ethereum :**

Ethereum est basé sur une plateforme décentralisée lancée en 2015 par le jeune programmeur Vitalik Buterin qui utilise la technologie blockchain pour traiter ses transactions, tandis qu'Ethereum utilise le concept bitcoin Proof of Work pour prouver les transactions. [7]

Ethereum diffère de Bitcoin de plusieurs manières, notamment : le temps de génération de bloc dans Ethereum est plus court que dans Bitcoin, il est de 14-15 secondes, contre 10 minutes dans Bitcoin. [7]

Le prix de la monnaie numérique Ripple a récemment baissé de 1,28 % pour atteindre 0,7798 $. En 19 février 2022. [5]

Figure 2: Logo d'Ehtereum [6]

- **Ripple :**

Ripple, anciennement connu sous le nom d'Open Coin, est une société privée qui développe un réseau de paiement et d'échange (RippleNet) basé sur les données d'un registre décentralisé (XRP Ledger). L'objectif principal de Ripple est de connecter les banques, les fournisseurs de services de paiement et d'échanger des actifs numériques afin que les paiements puissent être effectués plus rapidement et à moindre coût dans le monde entier.

Ripple a été créé pour la première fois en 2004 par Ryan Fugger, qui a créé le premier prototype de Ripple en tant que système de monnaie numérique décentralisé (RipplePay). Le système a été mis en service en 2005 et visait à fournir des solutions de paiement sécurisées au sein d'un réseau mondial. [8]

Fugger a confié le projet à Jed McCaleb et Chris Larsen en 2012. Ils ont fondé OpenCoin, une société technologique basée aux États-Unis, en équipe.

Ripple a commencé à prendre forme en tant que protocole axé sur les solutions de paiement pour les banques et autres institutions financières au moment où OpenCoin a été renommé Ripple Labs en 2013, puis Ripple en 2015. [8]

Le prix de la monnaie numérique Bitcoin BTC a récemment baissé de 2,05 % pour atteindre 39977,14 $. En 19 février 2022. [5]

Figure 3: Logo de Ripple [6]

2.5 Fonctionnement de la cryptomonnaie

2.5.1 Blockchain

Les blockchains sont une base de données sécurisée qui permet de stocker et d'échanger des valeurs en ligne sans avoir besoin d'un intermédiaire central. C'est le réseau décentralisé et la finance décentralisée qui en découle. C'est la technologie ou l'infrastructure qui prend en charge le fonctionnement des monnaies numériques. [9]

2.5.2 Structure de blockchain

a. Bloc

Un bloc est un enregistrement dans la blockchain qui contient et confirme de plusieurs données ou transactions en attente. [9]

Chaque bloc est composé de plusieurs champs :

- **Bloc :** l'indice de bloc.
- **Hash du bloc précédent :** Le champ contient le hash du bloc précédent (le bloc avec le numéro d'indice 91 dans notre exemple (Figure 4).
- **Transaction :** La partie qui contient la liste des transactions.
- **Horodatage :** heure de création du bloc.
- **Hash :** l'identifiant du bloc actuel.

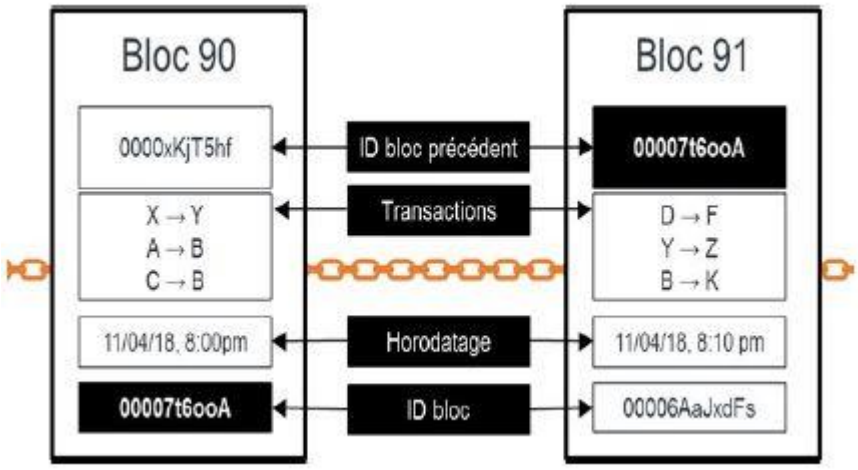

Figure 4: Exemple de bloc [9]

b. Chaine

Un hash qui relie un bloc à un autre, les « enchaînant » mathématiquement. [9]

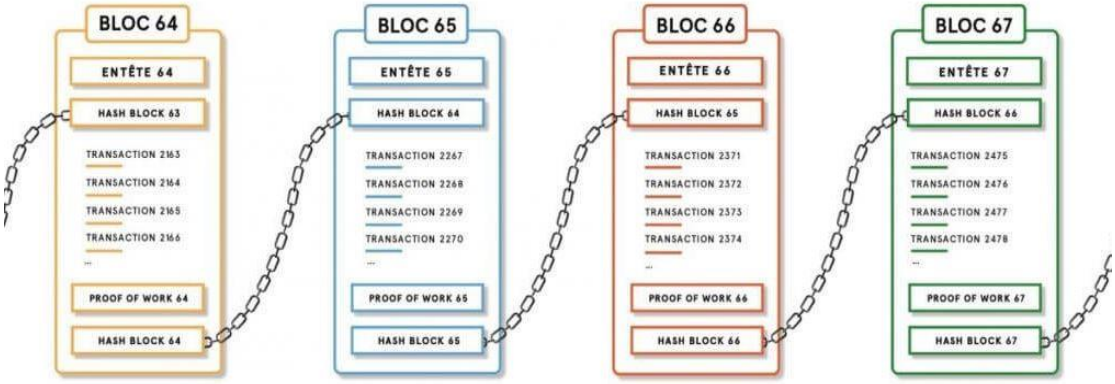

Figure 5: Exemple de chaine [10]

c. Réseau

Le réseau est constitué de "nœuds complets" comme des ordinateurs exécutant des algorithmes qui protègent la sécurité du réseau. Chaque nœud contient un enregistrement complet de toutes les transactions qui ont été enregistrées dans cette blockchain.

Les nœuds sont répartis dans le monde entier et n'importe qui peut le faire fonctionner. [9]

2.5.3 Transaction

La transaction est la manière de transfert de données numériques entre deux entités virtuelles au sein de la blockchain. Similaire à une transaction bancaire ou il y a un débiteur et un créditeur, la transaction de la cryptomonnaie nécessite également un débiteur et un créditeur virtuels représentés par leurs portefeuilles.

a. Portefeuille de monnaie numérique

Est une plate-forme matérielle ou logicielle qui vous permet de stocker, d'envoyer et de recevoir des crypto-monnaies. Pour diverses transactions, les portefeuilles de crypto-monnaie interagissent avec les blockchains. [11]

Les portefeuilles Blockchain fonctionnent selon un mécanisme similaire en utilisant une clé publique et une clé privée ensemble. Une clé publique est similaire à une adresse e-mail, car elle peut être donnée à n'importe qui. Lorsque le portefeuille est créé, une clé publique est

générée et vous pouvez partager la clé publique avec n'importe qui pour recevoir des fonds. [11]

- **Adresse**

L'adresse du portefeuille est créée en appliquant un algorithme à la clé publique pour dériver l'adresse connue de l'utilisateur. [12]

Dans Bitcoin, les adresses ressemblent généralement à ceci :

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

- ## Fonctionnement de portefeuille

Il se compose de deux parties principales, clé publique et clé privée, pour envoyer et recevoir en toute sécurité des transactions de crypto-monnaie après avoir vérifié la validité de la transaction. [11]

La clé privée établit la propriété des paramètres liés à la clé publique.

- **La clé publique**

Est une adresse électronique composée d'une série de chiffres et de lettres. Elle correspond à l'adresse du portefeuille sur la blockchain. [11]

- **La clé privée**

Comme mot de passe. Permet d'accéder aux fonds conservés dans la blockchain, de faire des transactions sur votre portefeuille. [11]

Figure 6: Exemple de clés [13]

- **Type de portefeuille**

Portefeuilles froids

Les portefeuilles froids sont ceux qui offrent un niveau de sécurité plus élevé. Parce qu'ils fonctionnent en dehors des lignes, il n'y a aucun risque de se faire voler. [14]

Portefeuille papier

Il repose sur la présence de codes spécifiques écrits sur une feuille de papier, car ces codes peuvent être utilisés pour effectuer des transactions. [15]

Figure 7: Exemple de papier [16]

Caractéristique

- Moins vulnérable aux cyberattaques. [15]

- La possibilité de dommages physiques au papier contenant ces codes, ou un défaut lors de l'impression, et l'utilisateur doit maintenir la confidentialité des codes qu'ils contiennent afin qu'ils ne soient pas utilisés par d'autres parties. [15]

➢ **Portefeuille matériel**

Ces portefeuilles se présentent sous la forme de pièces jointes ou d'appareils qui se connectent à un ordinateur sous forme de clé USB.

Ces appareils, alors qu'ils ne sont pas connectés à Internet, créent des codes d'utilisation pour leurs détenteurs. [15]

Figure 8: Exemple de matériel (USB) [17]

Caractéristique

- Moins vulnérable aux cyberattaques. [15]
- Pas gratuit et le prix est trop élevé. [15]

Portefeuilles chauds

Ils sont plus adaptés aux opérations quotidiennes. En raison de leur connexion constante à la blockchain, et donc à Internet, ils sont plus vulnérables aux cyberattaques. [14]

Tels que le portefeuille en ligne et le portefeuille logiciel.

➢ **Portefeuille en ligne**

Il s'agit de l'un des types de portefeuilles électroniques les plus flexibles, car le portefeuille électronique peut être créé en se connectant à partir de n'importe quel ordinateur connecté à Internet. [15]

Caractéristique

- Simple et facile à utiliser. [18]
- Facilite les transactions basiques. [18]
- Nul besoin d'installer une application ou un logiciel pour utiliser le portefeuille. [18]
- Il peut être moins sécurisé car les comptes des portefeuilles électroniques peuvent être piratés en profitant de la saisie d'informations confidentielles à partir de l'ordinateur lui-même. [18]

➢ **Portefeuille logiciel**

Un portefeuille crypto monnaie logiciel est un portefeuille disponible à partir d'un logiciel sur ordinateur par exemple Breadwallet, Jaxx, Copay. Donc, pour avoir accès au portefeuille, vous devez d'abord télécharger le logiciel. [18]

Caractéristique

- Meilleur niveau de sécurité par rapport au portefeuille web. [18]
- Contrôle de vos clés privées. [18]
- Nécessité de protéger son appareil. [18]
- Le portefeuille n'est disponible qu'après l'avoir téléchargé et installé. [18]

b. Regroupement de transaction

La transaction commence par l'envoi de Bitcoin ou d'une autre devise de l'utilisateur A à l'utilisateur B.

Initialement, un bloc représentant cette transaction sera créé, et une fois qu'un bloc est créé, la transaction demandée est diffusée sur un réseau peer-to-peer (p2p). [19]

c. Validation de bloc

La vérification se fait en saisissant une signature numérique et une clé publique dans le programme Bitcoin. Par conséquent, si la clé privée correspondant à la clé publique est utilisée pour signer, le programme peut vérifier la transaction sans révéler la clé privée. [20]

Une fois les vérifications effectuées , le bloc contenant la transaction entre l'utilisateur A et l'utilisateur B est validé par les mineurs à l' aide de procédures de consensus qui varient selon le type de blockchain et permettent un consensus distribué , ou un consensus entre les nœuds

sur l' état actuel du réseau .Pour ce faire, les mineurs doivent utiliser une procédure cryptographique connue sous le nom de calcul de hash de bloc .Dont chaque bloc possédé un identifiant qui prend la forme d'un hash permettant de relier les blocs les uns aux autres. Cet hash est toujours le résultat du hash du bloc précédent. [19]

d. Insertion de bloc

Lorsqu'un bloc est validé, il est daté et ajouté à la blockchain accessible à chaque utilisateur. [19]

e. Réception de la transaction

Enfin, l'utilisateur B reçoit la transaction de l'utilisateur A. [19]

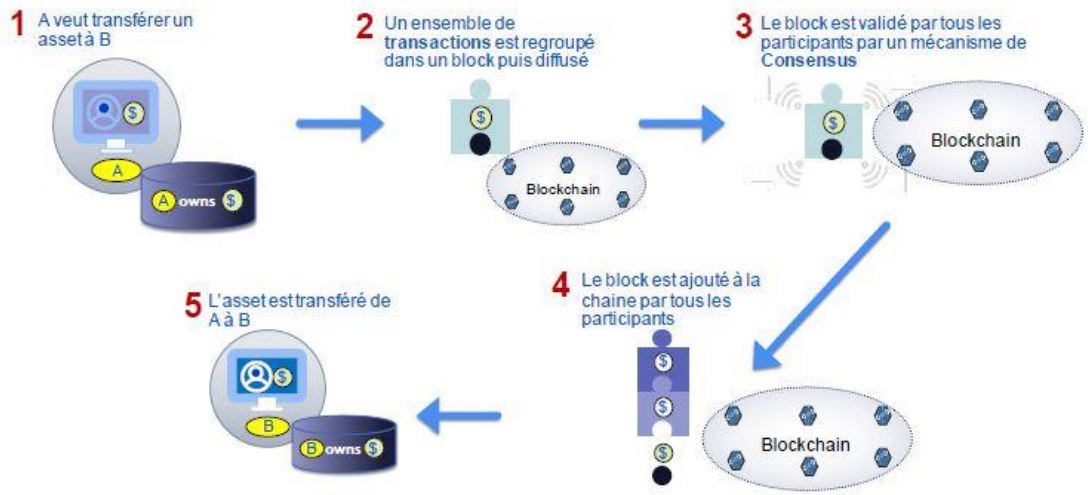

Figure 9: Transaction de la monnaie [19]

2.5.4 Minage

C'est le processus de documentation des transactions effectuées par crypto-monnaie par d'autres utilisateurs, pour lequel l'individu travaillant dans l'exploitation minière est récompensé et tire un profit supplémentaire de cette monnaie numérique, En résolvant des équations mathématiques complexes à l'aide d'ordinateurs aux capacités extraordinaires.

De nouveaux monnaies sont générés chaque fois qu'un utilisateur trouve une solution à un nouveau bloc, car le nouveau bloc est ajouté et publié sur le réseau blockchain. [19]

a. Principe

- Toutes les transactions qui arrivent sur la blockchain, les mineurs s'assurent de cette transaction. [19]
- Crée un bloc représente toutes les transactions. [19]
- Les mineurs résolvent des problèmes mathématiques ou des algorithmes de preuve de travail. [19]
- Le premier mineur à trouver la solution recevra une récompense après avoir examiné la solution et le nouveau bloc. [19]

b. Algorithme de consensus

Il s'agit d'un mécanisme spécifique par lequel la blockchain prend une décision unique.

Et comme la blockchain n'est pas centrale, tous les nœuds du réseau doivent convenir que la transaction est correcte, c'est là qu'intervient l'algorithme de consensus.

Son rôle est de s'assurer que les transactions se déroulent en toute sécurité. [21]

Il y a beaucoup types d'algorithme de consensus : POW, POS, DPOS, POET, POI. [19]

Parmi ces algorithmes les plus utilisé la preuve de travail (POW) et la preuve de jeux (POS).

➢ Preuve de travail (Pow)

La preuve de travail est un protocole qui empêche le piratage et les attaques en épuisant les ressources du système informatique.

La preuve de travail est utilisée pour vérifier les transactions ils sont regroupés en blocs, qui sont liés entre eux pour former une blockchain. [22]

Fonctionnement de Pow

- Pour ajouter un bloc de transactions à la blockchain, les participants à la blockchain (mineurs) doivent résoudre une puzzle mathématique. [22]
- Les mineurs sont responsables de l'ajout de nouveaux blocs à la blockchain. Pour ce faire, les mineurs doivent essayer de déduire un nombre aléatoire fictif (Nonce). Lorsque ce nombre est combiné avec les données fournies dans le bloc et transmis Avec une fonction de hachage, doit produire un résultat qui correspond à la condition

Données, par exemple, un hachage commençant par quatre zéros. [22]

- Lorsque ce nombre est combiné avec les données fournies dans le bloc et transmis via une fonction de hachage telle que l'algorithme SHA-256. [22]
- Lorsqu'un résultat correspondant aux données est trouvé, d'autres nœuds vérifient le résultat, récompensent le mineur et ajoutent le bloc à la blockchain. [22]

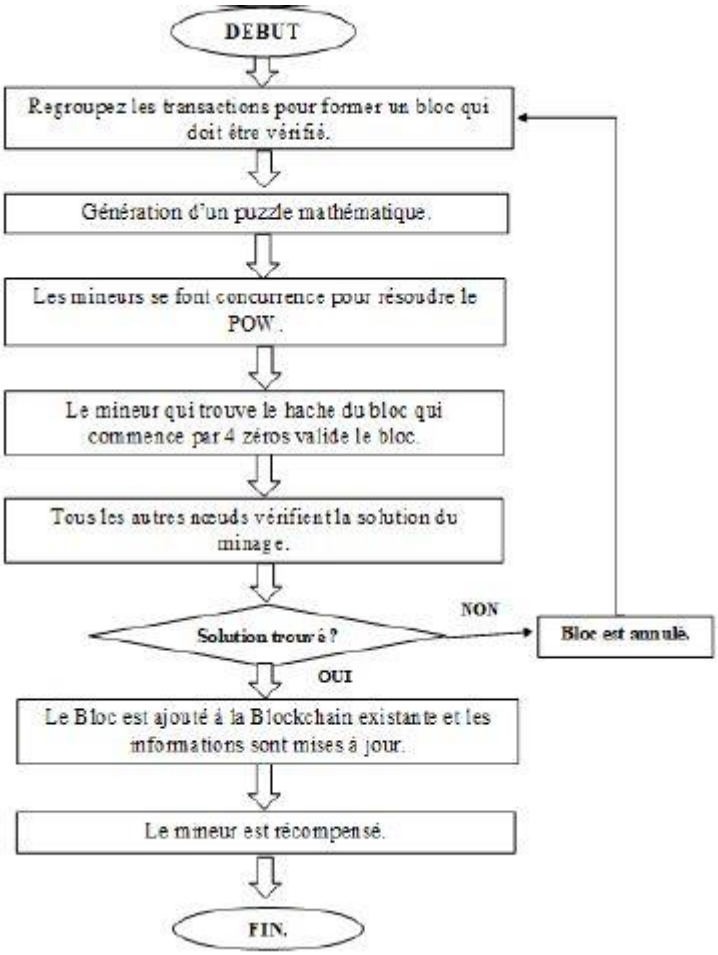

Figure 10: Structure de POW [19]

Les avantages

La preuve de travail permet de sécuriser le réseau contre un grand nombre d'attaques différentes. Une tentative de réussite nécessite une grande capacité de calcul.

Pour effectuer les calculs et donc ce sera inapproprié car le temps pour créer le bloc est beaucoup plus important. [22]

Les inconvénients

- Utilisez-le pour les machines minières qui consomment beaucoup d'électricité. [22]

- Couts élevé associé aux ressources matérielles. [22]

➢ Preuve d'enjeu (pos)

C'est l'un des protocoles de consensus les plus utilisés dans la technologie blockchain. Et utilisé par les crypto-monnaies pour valider les blocs. [23]

Fonctionnement de Pos

L'algorithme Pos est une alternative pour identifier qui est autorisé à ajouter de nouveaux blocs et à vérifier et vérifier l'état de la blockchain actuelle, où au lieu d'avoir deux mineurs en compétition pour trouver des solutions à un problème ou problème mathématique particulier, le produit de bloc suivant est attribué par un système aléatoire en fonction du nombre de crypto-monnaies dans le portefeuille ou de pièces stockée,

Ce système garantit que les plus grandes parties prenantes sont celles qui vérifient le bloc. [23]

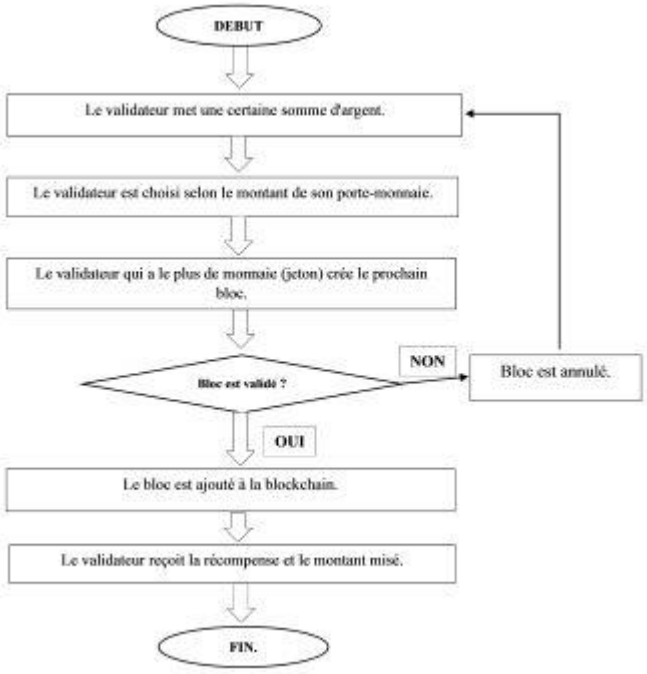

Figure 11: Structure de POS [19]

L'avantage

Consomme beaucoup moins d'énergie et est donc plus rentable. [23]

L'inconvénient

Le réseau a été piraté puisqu'il n'est plus nécessaire de dépenser de l'énergie pour miner un bloc, une personne malveillante peut facilement détourner le réseau et réécrire sa blockchain. [23]

c. Hash

Génère une chaîne de longueur fixe appelée empreinte digitale. À partir d'un ensemble de données de toute volume. Cet ensemble de données peut être un mot, une phrase, un texte plus long ou un fichier entier. [19]

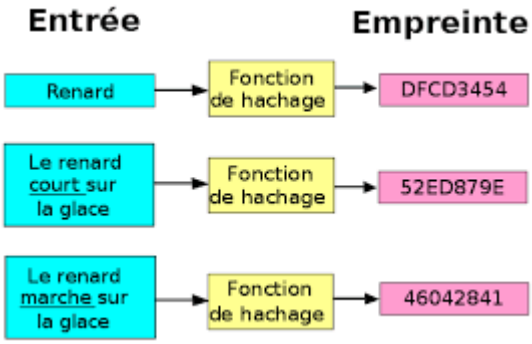

Figure 12: Exemple de Hash [24]

Les propriétés de Hash

- La fonction est déterministe, c'est-à-dire qu'une même donnée aura toujours la même valeur de hash. [19]
- Il est impossible de trouver deux messages différents ayant la même valeur de hachage. [19]

d. Méthodes de minage

- **Minage de CPU**

Bien que l'extraction de CPU était autrefois très populaire parmi les mineurs, beaucoup la considèrent maintenant comme trop lente et peu pratique en raison des dépenses élevées en énergie et en refroidissement. [25]

- **Minage de GPU**

Il augmente la puissance de calcul en combinant un tas de GPU sur une seule petite plate-forme.

Une RAM, un système de refroidissement et un châssis en forme de plate-forme sont nécessaires pour l'extraction du GPU, et cette méthode est beaucoup plus rapide que la méthode précédente. [25]

- **Méthode de ASIC**

Les mineurs ASIC créent plus d'unités de crypto-monnaie que les mineurs GPU puisqu'ils sont destinés exclusivement à l'extraction de crypto-monnaie. Cependant, ils sont plus chers, ce qui implique que si l'extraction devient plus difficile, ils deviendront rapidement obsolètes. [25]

- **La différence entre les méthodes**

Il s'avère que le rôle de chacune des méthodes de minage est très similaire, mais il existe une différence fondamentale entre elles.

- Le rôle du CPU, du GPU et de l'ASIC est très similaire et consiste à calculer et traiter les données.[25]
- Le CPU a la capacité d'exécuter des commandes beaucoup plus rapidement que le GPU .[25]
- Bien que le CPU soit plus puissant que le GPU, l'ASIC est plus puissant que les deux . [25]
- Le GPU est plus facile à acheter et plus disponible contrairement à ASIC, dans lequel chaque devise doit acheter une puce différente .[25]

2.6 Plateforme d'échange

Il organise et facilite la relation entre acheteurs et vendeurs, tout en apportant des liquidités substantielles pour accélérer au maximum le processus de négociation. Il peut suivre directement les transactions économiques entre eux. [26]

Il y a aussi un exemple : Binance, CoinBase. [27]

- **Binance :**

Binance est une plateforme de trading de crypto- monnaie fondée en janvier 2018 par le programmeur sino -canadien Changpeng Chao. Il s'agit de la plus grande plateforme de trading de crypto-monnaie au monde, avec plus d'un milliard et demi de dollars en monnaie numérique échangés chaque jour. Sa force vient du fait qu'il permet aux utilisateurs de choisir parmi des centaines de crypto-monnaies différentes. [27]

- **CoinBase :**

Coinbase est un échange de crypto - monnaie fondé en 2012 et basé à San Francisco, en Californie. Il est très simple d'investir dans des actifs cryptographiques majeurs tels que Bitcoin, Ethereum, XRP, Bitcoin Cash et Litecoin.

Coinbase permet à ses utilisateurs d'effectuer des transactions financières électroniques par son intermédiaire, leur permettant de vendre et d'acheter de manière transparente de la monnaie numérique, ainsi que de recevoir, d'envoyer et de stocker de la monnaie numérique, le tout en utilisant des transactions cryptées pour garantir la confidentialité et la sécurité des utilisateurs. [27]

2.7 Conclusion

Avec cela, nous avons vu un aperçu de la monnaie numérique, y compris sa définition, ses caractéristiques, ses transactions et sa gestion de réseau. Quelques exemples de monnaie numérique.

Chapitre 2
Processus de minage

1 Introduction

Dans ce chapitre, on parle d'abord l'aspect juridique des crypto-monnaies, les applications de minage d'algorithmes et de supports matériaux, et la sécurité des crypto-monnaies.

2 Enjeux et cadre juridique

La monnaie numérique Bitcoin reste l'objet de controverses et de confusion quant à la manière dont les pays la traitent. La vision de cette monnaie varie entre permettre qu'elle soit manipulée et l'interdire, ainsi qu'avertir son utilisation sans l'empêcher ou la juger illégale. [28]

Le bitcoin est une monnaie numérique, il n'y a pas de substitut physique, il ne peut être échangé qu'en ligne, il n'y a pas de régulateur central derrière lui, mais il peut être utilisé pour les achats en ligne comme n'importe quelle autre monnaie. [28]

Le statut juridique du Bitcoin varie d'un pays à l'autre et reste indéterminé ou variable dans de nombreux pays. Bien que la plupart des pays considèrent qu'il est illégal d'utiliser Bitcoin. [28]

Il s'agit notamment de la Chine, de l'Arabie saoudite, du Liban, de l'Islande, du Vietnam, du Bangladesh, de la Bolivie, de l'Équateur, de la Russie, du Maroc, de la Tunisie, de l'Algérie et de l'Égypte. Il existe des raisons similaires pour les risques de protection des consommateurs associés aux transactions Bitcoin, qui ne sont pas des devises régies par une banque centrale explicite qui régit ses politiques. Il a expliqué que la monnaie pouvait être un moyen de transférer des fonds illégalement, d'autant plus qu'elle n'est soumise à aucun régime fiscal. [28]

Contrairement à certains pays qui adoptent le Bitcoin comme moyen de paiement et d'échange, certains des pays les plus connus sont : l'Allemagne, le Canada, les États-Unis, le Mexique, l'Australie, les Philippines, les Émirats arabes unis, le Nigeria, le Japon, la Suisse, Malte.[28]

3 Etat de l'art

Les chercheurs ont mis en évidence sur la cryptomonnaie car il apparue comme un système de transaction réseau peer-to-peer, utilisant le décryptage pour le créer et le distribuer, il s'appuie sur la blockchain : d'une part, les mineurs de Bitcoin rejoignent de grandes bases minières afin de minimiser la variation de leurs revenus. (Böhme et al. 2015, 215–22) par contre, une « aristocratie » Bitcoin a été formée à la suite de l'architecture du code ; les membres de cette aristocratie sont ceux qui sont entrés tôt dans le jeu Bitcoin.[29]

Dans La vie sociale de Bitcoin, Nigel Dodd affirme que l'essence de l'idéologie de Bitcoin est de retirer l'argent du contrôle social, y compris du gouvernement, il y a même une déclaration d'indépendance Bitcoin. La déclaration inclut un message du crypto-anarchisme avec les mots : « Bitcoin est intrinsèquement anti-institution, antisystème et anti-état. Bitcoin sape les gouvernements et perturbe les institutions parce que le bitcoin est fondamentalement humanitaire ». [30]

David Golumbia déclare que les idées qui influencent les partisans du bitcoin proviennent des mouvements extrémistes de droite et de leur rhétorique anti-banque centrale, ou plus récemment du libertarisme de Ron Paul et Tea Party. [31]

Kroll et al. Soutiennent que l'écologie de Bitcoin aura besoin de structures de gouvernance pour survivre, (Kroll, Davey, and Felten 2013) montrant déjà des signes de structures de gouvernance émergentes. Ces modes de gouvernement peuvent être fondés sur le consensus et, si les dirigeants s'y opposent, la communauté peut choisir une autre voie. Au-delà de cela, les développements récents ont montré qu'un seul bassin minier pouvait tellement contribuer aux processus de calcul de Bitcoin, qu'il pouvait contrôler efficacement l'ensemble du système, mettant ainsi fin à sa structure décentralisée. [32]

Bauwens et Kostakis soutiennent que Bitcoin n'est pas un projet communautaire, mais une pièce représentant un nouveau type de capitalisme - un capitalisme « distribué », (Kostakis, Bauwens, and Niaros 2015) fondé sur l'idéologie politique libérale prônant l'élimination des états pour la souveraineté individuelle. En pratique, ce qui est réalisé est un capital concentré et une gouvernance centralisée. Vasilis Kostakis et Chris Giotitsas considèrent également que Bitcoin est un exemple d'un type dérivé du «capitalisme distribué» .[32]

bien qu'il faille plutôt le considérer comme une innovation technologique.

4 Application de minage

4.1 Minage

Le minage consiste à vérifier les transactions effectuées en monnaie virtuelle en cryptant les données et en les enregistrant dans la blockchain.[33]

4.2 Algorithmes

En utilise les algorithmes de hachage ou fonction de hach pour sécuriser les transactions de crypto-monnaie sur les blockchains.

Ceci est accompli en utilisant le hachage généré, dont la longueur varie en fonction de l'algorithme.

- **SHA 256**

En 1993, le premier protocole SHA est apparu, également connu sous le nom de SHA-0. Une version plus puissante et améliorée de SHA-1 est apparue deux ans plus tard. Quelques années plus tard, SHA-2 a été introduit, qui a quatre variantes basées sur le nombre de bits, telles que SHA-224, SHA-256, SHA-384 et SHA-512. [34]

Cet algorithme de cryptage a été développé par une agence de sécurité nationale (NSA) et le national des standards et de la technologie (NIST). Son objectif est de créer un hachage ou un jeton unique qui protège les documents ou les données informatiques contre tout agent extérieur souhaitant les modifie.[34]

- **Caractéristique de SHA 256**

- L'algorithme SHA-256 permet de générer un hachage fixe de 256 bits, qui est presque unitaire. [34]
- Il a une intention propre qui ne peut pas être décryptée de l'original. C'est l'une des fonctions de hachage les plus efficaces du marché. [34]

Fonctionnement de SHA 256

La fonction de hachage donne simplement un hachage identique des mêmes données saisies. Ceci est réalisé pour toutes les données et ne dépend pas de la façon dont l'algorithme est implémenté.[34]

Si des données sont saisies ou simplement si un caractère du texte est modifié, le hachage de la sortie est également modifié.[34]

Exemple :

b*itcoin.fr, site d'information et de nouvelles autour de Bitcoin.*
Hash SHA-256 =
9578c1ea7cd3b3129efea270c64e0d1637f6184f325b58e1d02e95829d03ba6c

B*itcoin.fr, site d'information et de nouvelles autour de Bitcoin.*
Hash SHA-256 =
ae7366010a2a5265344815b3ff98abd03283a1bf577f6f685fc31e74ff041d88

Dans cet exemple, le plus petit changement dans la chaîne d'entrée peut entraîner un grand changement dans la chaîne de sortie. [35]

Equihash

Le protocole ou l'algorithme minier Equihash est l'un des nombreux protocoles ou algorithmes miniers qui existent dans le monde du minage et de la blockchain. Mais Equihash a une place très particulière dans le monde de la cryptographie. Cela est dû au fait que la conception de l'algorithme qu'ils ont créé eux-mêmes fournit une énorme impédance à l'ASIC. Pas trop compliqué ou dangereux. [36]

Fonctionnement de Equihash

L'approche est basée sur une généralisation du problème des anniversaires qui trouve des valeurs de hachage qui se heurtent. Il a été conçu de manière à ce que les implémentations parallèles soient entravées par la mémoire bande passante, afin d'améliorer le compromis coût performance de l'implémentation ASIC personnalisée. L'ASIC est une organisation à but non lucratif qui promeut la résistance Equihash est basée sur l'hypothèse que le matériel

disponible dans le commerce possède déjà une mémoire à bande passante élevée et que les améliorations apportées par le matériel personnalisé ne valent peut - être pas le coût de développement. [37]

- **X11**

L'un des algorithmes de minage les plus puissants et les plus sûrs du monde des crypto-monnaies est X11, un algorithme qui se base sur un ensemble de fonctions de hachage différentes avec un seul objectif : fournir la meilleure sécurité pour le minage des crypto-monnaies. [38]

X11 collecte un total de 11 fonctions de hash qui sont utilisés dans un ordre spécifique pour aboutir au hachage final d'un bloc. [38]

4.3 Supports matériels

- **Cloud**

Cette nouvelle méthode permet aux utilisateurs de miner des crypto-monnaies même s'ils n'ont pas les ressources pour payer l'équipement de minage nécessaire. Alternativement, ils peuvent louer de la puissance de calcul auprès d'entreprises qui possèdent de tels équipements. Par conséquent, le processus d'extraction est effectué à partir d'un centre de données contrôlé à distance. [39]

Types de cloud

- **Serveur privé virtuel (VPS) :** cette méthode de minage nécessite la mise en place d'un serveur et l'installation d'un logiciel de minage, autrement dit, elle nécessite la location d'un ordinateur pouvant être connecté à distance via Internet. [40]
- **Location de puissance de calcul :** Acheter ou acquérir un contrat avec une entreprise pour louer une partie de sa puissance de calcul. En règle générale, les utilisateurs peuvent choisir la puissance de calcul à louer. [40]
- **Exploitation minière hébergée :** Dans ce modèle, l'entreprise paie les mineurs. En d'autres termes, ils sont responsables de la consommation et de l'entretien des équipements miniers appartenant au client. [40]

- **Réseaux cloud**

Genesis Mining : est l'une des plus grandes sociétés de cloud mining, exécutant son propre matériel de pointe avec différents algorithmes. Lancée en 2013, cette plate-forme légitime de cloud mining est l'une des plus anciennes aujourd'hui. [40]

Caractéristique

- Une grande variété d'options de crypto-monnaies et de forfaits. [40]
- L'un des meilleurs sites pour exploiter de l'Ethereum via le cloud. [40]
- Pas de frais d'entretien. [40]
- Vous pouvez choisir des fonctionnalités d'exécution de 12 ou 24 mois pour le cloud mining. [40]

Gminers : Gminers et une plate-forme émergente du Royaume-Uni qui propose aux crypto-investisseurs un aperçu facile du mécanisme de minage basé sur le cloud. Avec un abonnement d'un an (individuel pour chaque client), il est possible de réaliser des bénéfices substantiels sur les crypto-monnaies. [39]

Caractéristique

- Paiements quotidiens en crypto-monnaies. [40]
- Une grande variété de contrats de cloud mining. [40]

Shamining : Depuis 2018, il fournit des services fiables d'extraction de bitcoins dans le cloud à des clients du monde entier. Actuellement, il compte plus de 17 000 utilisateurs qui exploitent la crypto-monnaie sans équipement spécifique ni connaissances techniques. [40]

Caractéristique

- Un gestionnaire personnel pour chaque client. [40]
- Des paiements instantanés 24h/24 et 7j/7. [40]
- Disponible depuis n'importe quel appareil. [40]
- Le ticket d'entrée minimum pour le cloud mining n'est que de 250 $.[40]

- **ASIC**

Les ASIC sont devenus populaires dans Bitcoin en tant que collection ultime de processeurs spécifiques optimisés pour l'extraction de blocs. Le 17 septembre 2012, la société chinoise Avalon (maintenant connue sous le nom de Canaan) a développé le premier Bitcoin ASIC au monde. Plus récemment, les ASIC ont fait le saut vers d'autres protocoles de minage et d'autres crypto-monnaies. Parmi eux, on peut se concentrer sur Ethereum, Monero, Zcash, etc. [41]

Ces systèmes ont des caractéristiques uniques en fonction de la devise qu'ils utilisent. La plupart de ces systèmes sont compacts et offrent de puissantes capacités d'extraction. Les mineurs ASIC sont spécifiquement conçus pour fournir les meilleures performances pour la crypto-monnaie prévue. Ils sont purement conçus pour l'extraction de crypto-monnaie, mais au-delà de cela, leur fonctionnalité est de peu d'utilité. [41]

Parmi les modèles les plus utilisés, les meilleurs ASIC sont les suivants :

L'Antminer S7 : consommation de 1290 W pour un taux de hash de 4,73 TH/s. [42]

L'Antminer S9 : Il est légèrement plus cher et consomme 1320 W, mais il déploie 13,5 TH/s de puissance de hachage.[42]

L'Antminer t17 : Le modèle plus récent (1000€) a une puissance de hachage plus élevée, proche de 45 TH/s, et consomme 2200 W. Il est dédié à l'algorithme SHA256. [42]

L'Antminer Z11 : En tant que l'un des ASIC les plus efficaces fonctionnant sur l'algorithme Equihash, ce modèle a une puissance de 135 Ksol/s et consomme environ 1400 W. Le coût est d'environ 900 euros. [42]

Figure 13: Exemple de Antiminer s9 [43]

5 Sécurité

- **Transactions :** pour assurer la sûreté et la sécurité des transactions entre utilisateurs, la technologie blockchain assure l'échange sécurisé de monnaies numériques sans avoir besoin d'un tiers.
- **Incidents passés :**

PyBitmessage, un outil de messagerie peer-to-peer qui imite le système de transaction et de transfert de blocs bitcoin, a été touché par une attaque "day zero" en février 2018. PyBitmessage utilise la notion de preuve de travail, qui est liée aux blockchains, pour "payer" les transferts de messages et réduire le spam. Cet exploit a été utilisé par les cybercriminels pour exécuter du code sur l'équipement concerné en envoyant des messages soigneusement conçus. Ils ont ensuite pu exécuter des scripts automatisés pour rechercher des portefeuilles Ethereum tout en installant des codes shell inversés pour un accès plus détaillé. [44]

- **Gestion de l'anonymat**

Les portefeuilles de crypto-monnaie sont actuellement totalement anonymes et uniquement associés à des mots de passe complexes. Informations personnelles introuvables. [45]

Cependant, l'Union européenne semble avoir décidé de réduire l'anonymat des crypto-monnaies. L'objectif est surtout de prévenir le blanchiment d'argent et autres délits financiers. [45]

- **Echange et perte de clés**

- **Transfert de cryptomonnaies à la mauvaise adresse numérique :**

Afin de transférer la crypto-monnaie de l'utilisateur A à l'utilisateur B, l'utilisateur B doit fournir à l'utilisateur A une adresse numérique. Si l'utilisateur A saisi la mauvaise adresse, la crypto-monnaie sera malheureusement transférée sur le mauvais compte. Le seul moyen pour l'utilisateur A de racheter sa crypto-monnaie est que le titulaire du compte qui a commis l'erreur de transfert rembourse le montant. Cette tâche n'est pas aisée car ce marché repose sur l'anonymat des détenteurs de cryptomonnaies et n'est régulé par aucune autorité centrale.

Pour éviter de tels problèmes, les adresses doivent être vérifiées plusieurs fois avant d'accepter les transferts. [46]

- **Transfert du mauvais type de cryptomonnaie dans un électronique portefeuille :**

Les portefeuilles qui reçoivent des transferts doivent accepter les crypto-monnaies comme sujet. Si vous transférez une crypto-monnaie vers un portefeuille qui n'accepte pas le type de crypto-monnaie en question, le montant transféré sera débité du compte mais pas crédité sur d'autres comptes. De plus, même si le portefeuille vers lequel le transfert est reçu accepte la crypto-monnaie concernée, il faut s'assurer que le portefeuille utilise cette clé publique cryptée. [46]

Par exemple, les portefeuilles qui acceptent Bitcoin, Ethereum et Ripple. Il contient trois clés publiques, une pour chaque type de crypto-monnaie. Si, pour une raison quelconque, des bitcoins sont transférés vers la clé publique Ethereum correspondante, le montant du transfert sera débité du compte de la personne effectuant le transfert, mais pas crédité sur le compte de la personne qui devrait recevoir le transfert. Encore une fois, il n'y a aucun moyen de récupérer les actifs perdus. [46]

La solution consiste à vérifier auprès de la personne recevant les fonds que son portefeuille accepte bien le type de crypto-monnaie en question avant d'effectuer le transfert, et qu'il utilise un jeton à clé publique correspondant à ce type de variation de crypto-monnaie. [45]

- **Perte de clé privé**

Certains investisseurs conservent leurs clés privées sur leur téléphone, leur ordinateur portable ou un morceau de papier. À plusieurs reprises, des pirates informatiques ont volé les téléphones ou les ordinateurs portables des investisseurs et y ont conservé leurs clés privées. Ainsi, les pirates ont pu accéder aux actifs cryptographiques des investisseurs. Alternativement, si le titulaire du compte oublie son mot de passe, il ne pourra plus accéder à son compte. La clé privée permet d'accéder au compte sans saisir de mot de passe. [46]

6 Challenges

➢ Consommation électrique

La consommation d'électricité de Bitcoin a augmenté de 18 % depuis 2017 et équivaut désormais à 90% de celle des ménages français. [47]

Le bitcoin représente 0,65 % de la consommation énergétique mondiale totale. [47]

La consommation énergétique annuelle de Bitcoin équivaut à la quantité d'électricité consommée par dix pays de l'union européenne. [47]

Pour couvrir la consommation totale du minage de Bitcoin dans le monde, il faudrait 31.090.418 éoliennes ou 10 centrales nucléaires. [47]

➢ Blanchiment

Les blanchisseurs d'argent utilisent des programmes de transfert d'argent, des plateformes de crypto-monnaie et des monnaies numériques pour cacher et déplacer des fonds illicites.

Le bitcoin et d'autres crypto-monnaies contribuent à anonymiser les actifs financiers et à les rendre facilement transférables dans le monde entier, ce qui a fait passer le montant d'argent non comptabilisé dans le monde d'environ 1 milliard de dollars en 2018 à 2,8 milliards de dollars en 2019.

7 Conclusion

Dans ce chapitre, ont vu les aspects juridiques de Bitcoin, y compris les applications de minage d'algorithmes et de support matériel. De plus, ont discuté sécurité des crypto-monnaies et comment sécuriser les transactions. Finalement, ont montré les challenges de crypto-monnaies dans le secteur de minage.

Chapitre 3
Etude expérimental

1 Introduction

Dans ce chapitre, on parlera de l'implémentation de blockchain en java. et on parlera de l'expérimentation de POW.

Le but des tests est de vérifier la sécurité de la transaction basée sur la POW. Cette dernière est illustrée par une série de zéros (généralement 4), placés en début de la chaine à crypter. Ainsi trouver un hash commençant avec 4 zéros, s'avere difficile et demande enormément de temps qui dépasse en réalité le temps de la création d'un nouveau bloc. Ainsi, un hacker qui arrive à trouver ce hash, il l'aura un peu en retard et ne peut l'exploiter, étant donné que le bloc en question est périmé.

2 Hard environnement

Pour la réalisation de notre projet, nous avons utilisé un ordinateur HP caractérisé par :

- **Système d'exploitation :** Windows 10
- **RAM :** 4 GB
- **Processeur :** Intel R Core (TM) i3-3110M

3 Soft environnement

3.1 Les langages

- **Java :** est un langage de programmation orienté objet, développé par Sun Microsystems. Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris).[48]

3.2 Les outils

- **JDK :** désigne un ensemble de bibliothèques logicielles de base du langage de programmation Java, ainsi que les outils avec lesquels le code Java peut être compilé, transformé en bytecode destiné à la machine virtuelle Java.[49]

4 Implémentation de blockchain

Étape 01 : Création de premier bloc (Genisis bloc) dans la blockchain

➢ Structure de bloc

Les transactions sont enregistrées dans une structure appelée blocs. Les blocs sont lié les une aux autres pour créer le blockchain. Chaque bloc enregistre les transactions récentes,

Pour créer un bloc, une classe **bloc** est implémenté. Dans la classe bloc :

- **Hash :** contiendra le hash du bloc.
- **PreviousHash :** contiendra le hachage du bloc précédent.
- **Data :** utilisées pour stocker les données du bloc.
- **Timestemp :** est utilisé pour stocker l'horodatage du bloc. Ici, le type de données long est utilisé pour stocker le nombre de millisecondes.
- **CalculateHash () :** pour générer le hachage.

Blockchain.java | bloc.java | crypt.java

Source | History

```
1  package blockchain;
2  import java.util.Date;
3  import java.util.List;
4  public final class bloc {
5      public String hash;
6      private String data;
7      public String previousHash;
8      private long timestemp;
9      private int index;
10 public bloc (int index, long timestemp, String previousHash, String data) {
11     this.data=data;
12     this.previousHash=previousHash;
13     this.timestemp = new Date().getTime();
14     this.index=index;
15     this.hash = calculateHash(index, timestemp, previousHash, data);}
16 public String getpreviousHash() {return previousHash;}
17 public void setpreviousHash(String previousHash) {this.previousHash=previousHash;}
18 public String getHash() {return hash;}
19 public void setHash(String hash) {this.hash=hash;}
20 public String getdata() {return data;}
```

Figure 14: Structure de bloc

Le premier bloc d'une blockchain est appelé GenesisBlock, c'est le seul bloc de la chaîne à ne pas posséder de previousHash. Il sera créé avec le code suivant :

```java
import java.util.Date;
import java.util.ArrayList;
import java.util.List;

public class Blockchain {


public static void main(String[] args) {


    List<bloc> Blockchain=new ArrayList<>();

bloc genisis_bloc=new bloc(0, new Date().getTime(), null, "genisis_bloc");
Blockchain.add(genisis_bloc);

System.out.println(".....blockchain.....");
Blockchain.forEach(System.out::println);
System.out.println(".....................");
```

Figure 15: Création de genisis bloc

```
run:
.....blockchain.....
bloc 0:
    previousHash : null
    timestemp : Sun May 01 23:10:40 WAT 2022
    data : genisis_bloc
    hash : 846a29fb93c6646e883a71dcea9af5c4076abc696038373ldela324703d9eca5
.....................
BUILD SUCCESSFUL (total time: 2 seconds)
```

Figure 16: L'affichage de genisis bloc

Étape 02 : hash

Le hash d'un bloc est la partie la plus importante, il est calculé à partir de toutes les données contenues dans le bloc, utilise la fonction de hash SHA256 pour sécuriser les données de blockchain.

```java
public String calculateHash(int index, long timestemp, String previousHash, String data, int nonce) {
    String calculatedhash = crypt.applySha256(
                    Integer.toString(index)+previousHash +
                    Long.toString(timestemp) +Integer.toString(nonce)+
                     data
                    );
    return calculatedhash;
}
```

Figure 17: Fonction de hash

Étape 03 : Ajouter des blocs

Pour générer un nouveau bloc, il nous faut connaître le hash du bloc précédent.

```
public bloc nextbloc(String data, bloc dernierblock){
    bloc newblock = new bloc();
    newblock.settimestemp(System.currentTimeMillis());
    newblock.setdifficulty(difficulty);
    newblock.setindex(dernierblock.getindex()+1);
    newblock.setdata(data);
    newblock.setnonce(nonce);
    newblock.setpreviousHash(dernierblock.getHash());
    newblock.calculateHash(index,timestemp,previousHash,data, nonce);
    return newblock;

}
```

Figure 18: Ajouter de bloc

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Sat May 28 19:07:45 WAT 2022
     Data : genisis_bloc
     Nonce : 299292
     hash : 000018d62c236129e6abc67572b94e570f60807f93b547c21d30436388b9b833
Bloc 1:
     PreviousHash : 000018d62c236129e6abc67572b94e570f60807f93b547c21d30436388b9b833
     Timestemp : Sat May 28 19:07:58 WAT 2022
     Data : zeghdoudi receive 52 Bitcoin a donia
     Nonce : 199254
     hash : 00000b7027249315c2eb3840bd915d064d2117aceda627c5d9d2ab965cb63591
Bloc 2:
     PreviousHash : 00000b7027249315c2eb3840bd915d064d2117aceda627c5d9d2ab965cb63591
     Timestemp : Sat May 28 19:08:15 WAT 2022
     Data : utilisateur b receive 5 Bitcoin a utilisateur a
     Nonce : 179880
     hash : 000044ac48cca7c0b3baf0a7ff70eaf9f768b43fed0ac88eddf267f5fe49ccd0
.........................
BUILD SUCCESSFUL (total time: 34 seconds)
```

Figure 19: Exemple de résultat de blockchain

5 Partie expérimentale

5.1 Preuve de travail

Étape01 : création de premier bloc dans la blockchain

```java
package blockchain;
import java.util.Date;
import java.util.List;
public final class bloc {
    public String hash;
    private String data;
    public String previousHash;
    private long timestemp;
    private int index;
    private int nonce;
    private int difficulty;
public bloc (int index, long timestemp, String previousHash, String data) {
    this.data=data;
    this.previousHash=previousHash;
    this.timestemp = new Date().getTime();
    this.index=index;
    this.nonce=nonce;
    this.hash = calculateHash(index, timestemp, previousHash, data, nonce);}
public String getpreviousHash() {return previousHash;}
public void setpreviousHash(String previousHash) {this.previousHash=previousHash;}
public String getHash() {return hash;}
public void setHash(String hash) {this.hash=hash;}
public String getdata() {return data;}
public void setdata(String data) {this.data=data;}
public int getdifficulty() {return difficulty;}
public void setdifficulty(int difficulty) {this.difficulty=difficulty;}
public int getindex() {return index;}
public void setindex(int index) {this.index=index;}
public void settimestemp(long timestemp) {this.timestemp=timestemp;}
public void setnonce(int nonce) {this.nonce=nonce;}
public int getnonce(int nonce) {return nonce;}
```

Figure 20: Structure de bloc en java

```java
public bloc genisis_bloc(String data){
        this.previousHash=null;
        this.timestemp = new Date().getTime();
        this.data=data;
        this.difficulty=difficulty;
        this.nonce=nonce;
        this.index=1;

        this.hash=calculateHash(index,timestemp,previousHash,data, nonce);
         return this;
        }
```

Figure 21: Fonction de création du premier bloc

Étape 02 : création les blocs suivants

```
public bloc nextbloc(String data, bloc dernierblock){
    bloc newblock = new bloc();
    newblock.settimestemp(System.currentTimeMillis());
    newblock.setdifficulty(difficulty);
    newblock.setindex(dernierblock.getindex()+1);
    newblock.setdata(data);
    newblock.setnonce(nonce);
    newblock.setpreviousHash(dernierblock.getHash());
    newblock.calculateHash(index,timestemp,previousHash,data, nonce);
    return newblock;

}
```

Figure 22: Fonction d'ajout de bloc

Étape 03 : hach de bloc

```
public String calculateHash(int index, long timestemp, String previousHash, String data, int nonce) {
    String calculatedhash = crypt.applySha256(
                    Integer.toString(index)+previousHash +
                    Long.toString(timestemp) +Integer.toString(nonce)+
                     data
                    );
    return calculatedhash;
}
```

Figure 23: Fonction de hash de bloc

Étape finale : l'affichage de résultat

```
minage de Genisis bloc ...
Block Miné!!! : 0000596be42687f7f27c695694f8425f6571272cf9908ce0bbd0602066f62bc3
Enterr nom destinateur
jihene
Entrer l'expediteur
dounia
entrer l'argent ?
6
dounia receive 6 Bitcoin a jihene
Confirm ? n/y
y
minage de block 1 ...
Block Miné!!! : 000699d676575cb4e5f7c2cb387f0b22f39934fb8a1c0cc484cf2472455fa151
it took 92.578932 seconds to mine the block
Paiement accepté
Voulez-vous effectuer un autre paiement ?
y
Enterr nom destinateur
xxxx
Entrer l'expediteur
yyyyy
entrer l'argent ?
30
yyyyy receive 30 Bitcoin a xxxx
Confirm ? n/y
y
minage de block 2 ...
Block Miné!!! : 00039a11c9d7ae6b85e2a07621571f9c42c4c8977cc09ba6af1b21ad6bb5eea2
it took 20.516696 seconds to mine the block
```

Figure 24: L'affichage de minage de blockchain

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Sat May 28 19:12:28 WAT 2022
     Data : genisis_bloc
     Nonce : 17939
     hash : 0000596be42687f7f27c695694f8425f6571272cf9908ce0bbd0602066f62bc3
Bloc 1:
     PreviousHash : 0000596be42687f7f27c695694f8425f6571272cf9908ce0bbd0602066f62bc3
     Timestemp : Sat May 28 19:12:44 WAT 2022
     Data : dounia receive 6 Bitcoin a jihene
     Nonce : 7478
     hash : 000699d676575cb4e5f7c2cb387f0b22f39934fb8a1c0cc484cf2472455fa151
Bloc 2:
     PreviousHash : 000699d676575cb4e5f7c2cb387f0b22f39934fb8a1c0cc484cf2472455fa151
     Timestemp : Sat May 28 19:13:00 WAT 2022
     Data : yyyyy receive 30 Bitcoin a xxxx
     Nonce : 3150
     hash : 00039a11c9d7ae6b85e2a07621571f9c42c4c8977cc09ba6af1b21ad6bb5eea2
.........................
BUILD SUCCESSFUL (total time: 35 seconds)
```

Figure 25: Résultat final de blockchain

6 Conclusion

Dans ce chapitre, on a parlé de la façon de créer une blockchain en java, on a vu les étapes et la fonction principale utilisée, la pow les étapes de son travail.

Chapitre 4
Test et résultats

1 Introduction

Après avoir expliqué comment créer une blockchain en Java au chapitre 3 avec les étapes. Dans ce chapitre on parle mis quelques tests sur la partie expérimentation (pow) pour voir comment le temps change à mesure que la difficulté de minage augmente.

2 Le test no1 : difficulté de minage

Difficulty : La difficulté de l'extraction est la valeur de hachage du bloc à travers lequel le bloc est sécurisé par le nombre de zéros spécifiés, plus cette valeur est élevée, plus le bloc est sécurisé.

- Pour une taille de bloc = 50 caractères

Pour difficulty=1

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:11:32 WAT 2022
     Data : genisis_bloc
     Nonce : 21
     hash : 0c171265b2f124868ec2f7cd17dc9710c6a99c5bed269a01fcd21b7d2b101026
Bloc 1:
     PreviousHash : 0c171265b2f124868ec2f7cd17dc9710c6a99c5bed269a01fcd21b7d2b101026
     Timestemp : Tue May 31 10:11:44 WAT 2022
     Data : zeghdoudi receive 75 Bitcoin a dounia
     Nonce : 16
     hash : 09d18729bb028b61e4515cf2998264cbf6442c4eaa8d8c8a94f9f464951b98dd
.........................
```

Figure 26: Test pour difficulty = 1

```
minage de block 1 ...
Block Miné!!! : 09d18729bb028b61e4515cf2998264cbf6442c4eaa8d8c8a94f9f464951b98dd
it took 0.009579903 seconds to mine the block
Paiement accepté
```

Figure 27: Le temp de création de block pou diff = 1

Pour difficulty = 2

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:15:03 WAT 2022
     Data : genisis_bloc
     Nonce : 60
     hash : 003a4fc75a7274081577b66e415c6b11b8e5f06b1cceaabd0ddbf3ebd057e274
Bloc 1:
     PreviousHash : 003a4fc75a7274081577b66e415c6b11b8e5f06b1cceaabd0ddbf3ebd057e274
     Timestemp : Tue May 31 10:15:17 WAT 2022
     Data : utilisateur b receive 21 Bitcoin a utilisateur a
     Nonce : 255
     hash : 001a6aaccf35ee7aa1b5e78986b24e5dbea7e6409df89f11bf29c13816led2e1
.........................
```

Figure 28: Test pour difficulty = 2

```
minage de block 1 ...
Block Miné!!! : 001a6aaccf35ee7aa1b5e78986b24e5dbea7e6409df89f11bf29c13816led2e1
it took 0.033560023 seconds to mine the block
Paiement accepté
```

Figure 29: Le temp de création de block pou diff = 2

Pou difficulty = 3

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:16:23 WAT 2022
     Data : genisis_bloc
     Nonce : 15643
     hash : 0009fd189178622267e18cecbf5258090b06d3da58b2b4a2d2c3be9693831cad
Bloc 1:
     PreviousHash : 0009fd189178622267e18cecbf5258090b06d3da58b2b4a2d2c3be9693831cad
     Timestemp : Tue May 31 10:16:34 WAT 2022
     Data : block 2 receive 6 Bitcoin a block 1
     Nonce : 2292
     hash : 000e3e0992820b2a9d6f6b60b56eaadfb27749d85ffd5086af9e7079dbb9381e
.........................
```

Figure 30: Test pour difficulty = 3

```
minage de block 1 ...
Block Miné!!! : 000e3e0992820b2a9d6f6b60b56eaadfb27749d85ffd5086af9e7079dbb9381e
it took 0.049223477 seconds to mine the block
Paiement accepté
```

Figure 31: Le temp de création de block pour diff = 3

Pour difficulty = 4

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:17:57 WAT 2022
     Data : genisis_bloc
     Nonce : 49651
     hash : 0000edf4eee405d46b1b2cfd9dde4689bed2adb4c5240d25a820db287f3b6ffb
Bloc 1:
     PreviousHash : 0000edf4eee405d46b1b2cfd9dde4689bed2adb4c5240d25a820db287f3b6ffb
     Timestemp : Tue May 31 10:18:10 WAT 2022
     Data : lakehal jihen receive 5 Bitcoin a zeghdoudi donia
     Nonce : 28512
     hash : 0000fe7fd43712c19bbb6a9ea3dd346dec646a700101160529cf8c7ffea7c9f4
.........................
```

Figure 32: Test pour difficulty = 4

```
minage de block 1 ...
Block Miné!!! : 0000fe7fd43712c19bbb6a9ea3dd346dec646a700101160529cf8c7ffea7c9f4
it took 0.197322827 seconds to mine the block
Paiement accepté
```

Figure 33: Le temp de création de block pou diff = 4

Pour difficulty = 5

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:19:43 WAT 2022
     Data : genisis_bloc
     Nonce : 249313
     hash : 0000019fd6797e7937ae6a7aeeb750452e360a3199c7e26b296c59f86665e932
Bloc 1:
     PreviousHash : 0000019fd6797e7937ae6a7aeeb750452e360a3199c7e26b296c59f86665e932
     Timestemp : Tue May 31 10:20:00 WAT 2022
     Data : yyyyy receive 98 Bitcoin a xxxxx
     Nonce : 1041592
     hash : 00000e9b00f456c0e1ab7148b88f6262f560a09c6d7bd4ce77971b543d9907d6
.........................
```

Figure 34: Test pour difficulty = 5

```
minage de block 1 ...
Block Miné!!! : 00000e9b00f456c0e1ab7148b88f6262f560a09c6d7bd4ce77971b543d9907d6
it took 3.754290579 seconds to mine the block
Paiement accepté
```

Figure 35: Le temp de création de block pour diff = 5

Pour difficulty = 6

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:21:03 WAT 2022
     Data : genisis_bloc
     Nonce : 14163929
     hash : 0000007fba696a941cb7b6f2da1cfee6b078b4c1fd8cd0fda6b65f895debc772
Bloc 1:
     PreviousHash : 0000007fba696a941cb7b6f2da1cfee6b078b4c1fd8cd0fda6b65f895debc772
     Timestemp : Tue May 31 10:21:59 WAT 2022
     Data : lakehal receive 6 Bitcoin a zeghdoudi
     Nonce : 11557824
     hash : 00000064080c961a49dbc689e22d5535c52fc59125a0c5afba7767120a30a79b
.........................
```

Figure 36: Test pour difficulty = 6

```
minage de block 1 ...
Block Miné!!! : 00000064080c961a49dbc689e22d5535c52fc59125a0c5afba7767120a30a79b
it took 39.405570046 seconds to mine the block
Paiement accepté
```

Figure 37: Le temp de création de block pour diff = 6

- Pour une taille de bloc = 70 caractères

Pour difficulty = 1

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:31:48 WAT 2022
     Data : genisis_bloc
     Nonce : 11
     hash : 008f3d133197c4e816c51e1cc8668da3b94590c31f5179e70f56c927640cae43
Bloc 1:
     PreviousHash : 008f3d133197c4e816c51e1cc8668da3b94590c31f5179e70f56c927640cae43
     Timestemp : Tue May 31 10:32:00 WAT 2022
     Data : utilisateur yyy receive 59 Bitcoin a utilisateur xxx
     Nonce : 5
     hash : 0575f1c1475c6535d58acb192628f91e40c8e7434efcfb8faf36f0ca7b096c9f
.........................
```

Figure 38: Test pour dif = 1

```
minage de block 1 ...
Block Miné!!! : 0575f1c1475c6535d58acb192628f91e40c8e7434efcfb8faf36f0ca7b096c9f
it took 0.01490269 seconds to mine the block
Paiement accepté
```

Figure 39: Le temp de création du block pou dif = 1

Pour difficulty = 2

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:38:21 WAT 2022
     Data : genisis_bloc
     Nonce : 154
     hash : 007740f19e16b11e5d7d24e5f73409238327e6cd00f7975adbff6619b40d7c23
Bloc 1:
     PreviousHash : 007740f19e16b11e5d7d24e5f73409238327e6cd00f7975adbff6619b40d7c23
     Timestemp : Tue May 31 10:38:32 WAT 2022
     Data : block bb receive 5 Bitcoin a  block aa
     Nonce : 643
     hash : 00d8b7fce580d0c248701f384a4631885cc9064f5c230f60943la9bf22f9a01d
.........................
```

Figure 40: Test pour dif = 2

```
minage de block 1 ...
Block Miné!!! : 00d8b7fce580d0c248701f384a4631885cc9064f5c230f60943la9bf22f9a01d
it took 0.050840796 seconds to mine the block
Paiement accepté
```

Figure 41: Le temp de création du block pour dif = 2

Pour difficulty = 3

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:42:50 WAT 2022
     Data : genisis_bloc
     Nonce : 247
     hash : 0002956581770d215a796a707920586614832dbcb28e8701b83f342019cd2fee
Bloc 1:
     PreviousHash : 0002956581770d215a796a707920586614832dbcb28e8701b83f342019cd2fee
     Timestemp : Tue May 31 10:43:05 WAT 2022
     Data : zeghdoudi donia receive 27 Bitcoin a lakehal jihen
     Nonce : 6174
     hash : 00096c6f6d5c2a3642078fbe833a9321261736cb00357385ea88e9e26d3bf85b
.........................
```

Figure 42: Test pour dif = 3

```
minage de block 1 ...
Block Miné!!! : 00096c6f6d5c2a3642078fbe833a9321261736cb00357385ea88e9e26d3bf85b
it took 0.210902838 seconds to mine the block
Paiement accepté
```

Figure 43: Le temp de création du block pour dif = 3

Pour difficulty = 4

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:45:11 WAT 2022
     Data : genisis_bloc
     Nonce : 7405
     hash : 0000625c20aaafb0e3bf51f2e7a71482cee9d75ecdc22dd5726a03dbf960e196
Bloc 1:
     PreviousHash : 0000625c20aaafb0e3bf51f2e7a71482cee9d75ecdc22dd5726a03dbf960e196
     Timestemp : Tue May 31 10:45:24 WAT 2022
     Data : agent yyyyy receive 56 Bitcoin a agent xxxx
     Nonce : 111744
     hash : 0000152ad12fa7ab0e4c17d607fe6ffb95d3d6580d510d20f3f90b489fa67ae7
.........................
```

Figure 44: Test pour dif = 4

```
minage de block 1 ...
Block Miné!!! : 0000152ad12fa7ab0e4c17d607fe6ffb95d3d6580d510d20f3f90b489fa67ae7
it took 0.655987312 seconds to mine the block
Paiement accepté
```

Figure 45: Le temp de création du block pour dif = 4

Pour difficulty = 5

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:48:44 WAT 2022
     Data : genisis_bloc
     Nonce : 2006168
     hash : 00000c54a66e322d291335c8fe2e65d8c410e378f6c39926ca59e1f001ee5914
Bloc 1:
     PreviousHash : 00000c54a66e322d291335c8fe2e65d8c410e378f6c39926ca59e1f001ee5914
     Timestemp : Tue May 31 10:49:10 WAT 2022
     Data : utilisateur yyy jihen receive 8 Bitcoin a utilisateur xxx donia
     Nonce : 586806
     hash : 0000040607a1ff031558ac7d45e4a2924d8750757223a1c5ae70b9926d77ed11
.........................
```

Figure 46: Test pour dif = 5

```
minage de block 1 ...
Block Miné!!! : 0000040607a1ff031558ac7d45e4a2924d8750757223a1c5ae70b9926d77ed11
it took 1.999885821 seconds to mine the block
Paiement accepté
```

Figure 47: Le temp de création du block pour dif = 5

Pour difficulty = 6

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Tue May 31 10:52:20 WAT 2022
     Data : genisis_bloc
     Nonce : 16334744
     hash : 00000060a7795b21bd4ff75cab2dd80aa4c40339caa6f8aaeee6bb436dd5bd95
Bloc 1:
     PreviousHash : 00000060a7795b21bd4ff75cab2dd80aa4c40339caa6f8aaeee6bb436dd5bd95
     Timestemp : Tue May 31 10:53:40 WAT 2022
     Data : ouvrier ddddddd zeghdoudi receive 61 Bitcoin a ouvrier aaaaa donia
     Nonce : 51243056
     hash : 000000897fc2dd07f806484652a10994dd99e2291618ff2f1c35e014910bea60
.........................
```

Figure 48: Test pour dif = 6

```
minage de block 1 ...
Block Miné!!! : 000000897fc2dd07f806484652a10994dd99e2291618ff2f1c35e014910bea60
it took 173.601630918 seconds to mine the block
Paiement accepté
```

Figure 49: Le temp de création du block pour dif = 6

- Pour une taille de bloc = 100 caractères

Pour difficulty = 1

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Fri Jun 03 23:10:16 WAT 2022
     Data : genisis_bloc
     Nonce : 33
     hash : 0c075933b6c5c5a4a822355b293aee250a9bc13746bda1459e26e2e5d7286038
Bloc 1:
     PreviousHash : 0c075933b6c5c5a4a822355b293aee250a9bc13746bda1459e26e2e5d7286038
     Timestemp : Fri Jun 03 23:10:44 WAT 2022
     Data : jjdhhutizhawleuh jvcbgzyuj vhdgdhhhfhg receive 67 Bitcoin a aajjfdhbbvjjhfhbnbjjj jjfihgjjf
     Nonce : 36
     hash : 0b66b3be6b842b89d2f3096426fd27edf813370f7a924023ba8fd22ddd229545
.........................
```

Figure 50: Test pour diff=1

```
minage de block 1 ...
Block Miné!!! : 0b66b3be6b842b89d2f3096426fd27edf813370f7a924023ba8fd22ddd229545
it took 0.0259356 seconds to mine the block
Paiement accepté
```

Figure 51: Le temp de bloc pour diff=1

Pour difficulty =2

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Fri Jun 03 23:18:04 WAT 2022
     Data : genisis_bloc
     Nonce : 106
     hash : 00e9e7bb89c71351cbfbcdce939906c4bf27d4d2b2a336b71af93c2d0bb072ae
Bloc 1:
     PreviousHash : 00e9e7bb89c71351cbfbcdce939906c4bf27d4d2b2a336b71af93c2d0bb072ae
     Timestemp : Fri Jun 03 23:18:48 WAT 2022
     Data : iyjugtrezaqswdxfcgvbhnjkpmljhqerwdxg receive 2 Bitcoin a iujhfdezrsdxgfcvhbjiuytrezsdfcgvhbj
     Nonce : 303
     hash : 0006f57728abebae65e70ad789053e5518f13609e248b898109258067lb0407e
.........................
```

Figure 52: Test pour diff=2

```
minage de block 1 ...
Block Miné!!! : 0006f57728abebae65e70ad789053e5518f13609e248b898109258067lb0407e
it took 0.062014688 seconds to mine the block
Paiement accepté
```

Figure 53:Le temp de block pour diff=2

Pour difficulty =3

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Sat Jun 04 11:16:47 WAT 2022
     Data : genisis_bloc
     Nonce : 706
     hash : 000a6624b4803aad8863fe7b47977f67606lcccfe5182108cb7a628f045406f3
Bloc 1:
     PreviousHash : 000a6624b4803aad8863fe7b47977f67606lcccfe5182108cb7a628f045406f3
     Timestemp : Sat Jun 04 11:17:04 WAT 2022
     Data : gfehsgdhc dfsgjfsdyhgfdhjsgdif receive 6 Bitcoin a iuytrfdvchiezgvhwxguygvgfsyugvxdx
     Nonce : 14760
     hash : 000d5592b7f286dbfafd3ebf5f19da29d43ede12b5ba13fc5e6213219a948956
.........................
```

Figure 54: Test pour diff=3

```
minage de block 1 ...
Block Miné!!! : 000d5592b7f286dbfafd3ebf5f19da29d43ede12b5ba13fc5e6213219a948956
it took 0.337400564 seconds to mine the block
Paiement accepté
```

Figure 55: Le temp de block pour diff=3

Pour difficulty = 4

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Fri Jun 03 23:29:54 WAT 2022
     Data : genisis_bloc
     Nonce : 105676
     hash : 0000c10e82b456200b74e4908a12afc51daaa8f8d6279bbe12ea508292e57a4b
Bloc 1:
     PreviousHash : 0000c10e82b456200b74e4908a12afc51daaa8f8d6279bbe12ea508292e57a4b
     Timestemp : Fri Jun 03 23:30:18 WAT 2022
     Data : zeghdoudidounia masterreseauxtrdgbfaqf receive 1 Bitcoin a zeghdoudidounia masterreseauxvdvdf
     Nonce : 222425
     hash : 0000fa076d13aba0b05505010e7b45ea8a6cefbca53325a19278d73add0efb68
.........................
```

Figure 56: Test pour diff=4

```
minage de block 1 ...
Block Miné!!! : 0000fa076d13aba0b05505010e7b45ea8a6cefbca53325a19278d73add0efb68
it took 0.877135071 seconds to mine the block
Paiement accepté
```

Figure 57: Le temp de block pour diff=4

Pour difficulty = 5

```
........blockchain.........
Bloc 0:
     PreviousHash : null
     Timestemp : Fri Jun 03 23:41:37 WAT 2022
     Data : genisis_bloc
     Nonce : 257451
     hash : 00000e5d828b496e93c6bb60a97893865e99dcf6d8777e2ad3fa11267a976da5
Bloc 1:
     PreviousHash : 00000e5d828b496e93c6bb60a97893865e99dcf6d8777e2ad3fa11267a976da5
     Timestemp : Fri Jun 03 23:41:57 WAT 2022
     Data : oikujyhtgrfsdxcfgvbhtrezaqwdxcfg receive 1 Bitcoin a ghkjvrytrctvtrvrvrtyxertcvnuioi
     Nonce : 1322859
     hash : 000004321 1d3bd09d6f6b7eff6aa126ca3a877b5f9f7f436556e92036adfc2a5
.........................
```

Figure 58: Test pour diff=5

```
minage de block 1 ...
Block Miné!!! : 00000432111d3bd09d6f6b7eff6aa126ca3a877b5f9f7f436556e92036adfc2a5
it took 4.422704651 seconds to mine the block
Paiement accepté
```

Figure 59: Le temp de block pour diff=5

3 Analyse

- Pour une taille de bloc = 50 caractères

Tableau 1: Pour une taille du block 50 caractères

Difficulty	Hash	Temps (seconds)
1	**0**9d18729bb028b61e4515cf2998264cbf6442c4eaa8d8c8a94f9f464951b98dd	0.0095
2	**00**1a6aaccf35ee7aa1b5e78986b24e5dbea7e6409df89f11bf29c138161ed2e1	0.033
3	**000**e3e0992820b2a9d6f6b60b56eaadfb27749d85ffd5086af9e7079dbb9381e	0.049
4	**0000**fe7fd43712c19bbb6a9ea3dd346dec646a700101160529cf8c7ffea7c9f4	0.19
5	**00000**e9b00f456c0e1ab7148b88f6262f560a09c6d7bd4ce77971b543d9907d6	3.75
6	**000000**64080c961a49dbc689e22dd5535c52fc59125a0c5afba7767120a30a79b	39.40

- Pour une taille de bloc = 70 caractères

Tableau 2: Pour une taille du block 70 caractères

Difficulty	Hash	Temps (seconds)
1	**0**575f1c1475c6535d58acb192628f91e40c8e7434efcfb8faf36f0ca7b096c9f	0.014
2	**00**d8b7fce580d0c248701f384a4631885cc9064f5c230f609431a9bf22f9a01d	0.050
3	**000**96c6f6d5c2a3642078fbe833a9321261736cb00357385ea88e9e26d3bf85b	0.21
4	**0000**152ad12fa7ab0e4c17d607fe6ffb95d3d6580d510d20f3f90b489fa67ae7	0.65
5	**00000**40607a1ff031558ac7d45e4a2924d8750757223a1c5ae70b9926d77ed11	1.99
6	**000000**897fc2dd07f806484652a10994dd99e2291618ff2f1c35e014910bea60	173.60

- Pour une taille de bloc = 100 caractères

Tableau 3: Pour une taille de block 100 caractères

Difficulty	Hash	Temps (seconds)
1	**0**b66b3be6b842b89d2f3096426fd27edf813370f7a924023ba8fd22ddd229545	0.025
2	**000**6f57728abebae65e70ad789053e5518f13609e248b8981092580671b0407e	0.06
3	**000**d5592b7f286dbfafd3ebf5f19da29d43ede12b5ba13fc5e6213219a948956	0.33
4	**0000**fa076d13aba0b05505010e7b45ea8a6cefbca53325a19278d73add0efb68	0.87
5	**00000**43211d3bd09d6f6b7eff6aa126ca3a877b5f9f7f436556e92036adfc2a5	4.42

Grâce à des expériences précédentes menées sur la blockchain, nous concluons que plus le minage est difficile, plus il est difficile de trouver le hachage, et cela nécessite un temps qui dépasse en réalité le temps de création d'un nouveau bloc.

Les résultats suivants montrent que le temps augmente à mesure que la difficulté de minage augmente.

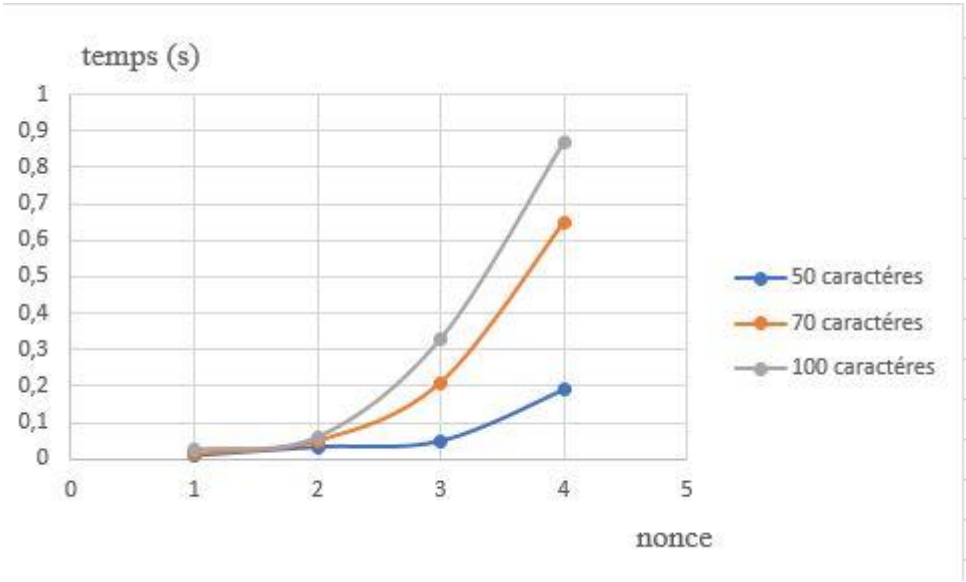

Figure 60: analyse le résultat

En effet, la Blockchain Bitcoin génère des blocs d'une taille maximale de 1 mégaoctet de données toutes les 10 minutes qui ne permettent finalement que de traiter 7 transactions par seconde, et la taille des données augmente d'environ 50 Mo, ce qui signifie qu'un bloc peut contenir plusieurs milliers de transactions. La Blockchain Bitcoin totalise désormais environ 160 Go.[50]

Ceci dit, nos tests ne peuvent conquérir le traitement réel du bitcoin vu la distinction concrète entre les deux environnements. Néanmoins, notre travail nous a permis de procéder à une simulation réelle de la transaction numérique qui sera bien entendu, facilement étendue avec des équipements adéquats.

4 Conclusion

Dans ce chapitre on a vu quelques tests sur la partie expérimentation (pow) pour voir comment augmente le temps change à mesure que la difficulté de minage augmente.

Par exemple pour un nonce de 3 zéros le temps est de 0.21 seconds, et pour un nonce de 4 zéros le temps est de 0.65 seconds.

Ce que nous remarquons, c'est une augmentation de la valeur de nonce, ce qui entraîne une augmentation du temps.

Conclusion Générale

1 Conclusion générale

Les crypto-monnaies sont ainsi nommées car elles utilisent la cryptographie pour vérifier les transactions. Cela signifie que le jeton est responsable du stockage et de la transmission de données de crypto-monnaie entre les portefeuilles et les registres publics.

Bien que les crypto-monnaies soient largement considérées comme sûres en utilisant la technologie blockchain, elles ont été piratées à maintes reprise.

Le travail réalisé nous a permis de mesurer le temps de réalisation d'une transaction monétaire en considérant la taille du nonce. Ce dernier qui, considéré comme l'élément essentiel de la sécurité du bloc a été utilisé avec une difficulté entre 1 et 5 et nous a permis d'enregistrer au moins une transaction par seconde et ce, en utilisant un matériel basique.

A noter que le traitement réel de ces transactions se fait à l'aide d'équipements puissants et réalise quelques transactions par secondes avec un nonce de difficulté 4. Donc, notre travail n'est guère de conquérir ce traitement mais de comprendre le mécanisme de transactions numériques et de manipuler les block chaines et de tester les divers niveaux de sécurité.

Références Bibliographies

Références Bibliographies

[1]https://www.bibliotheque.assnat.qc.ca/fr/cinq-lectures-pour-comprendre/4870-cinqlectures-pour-comprendre-les-monnaies-numeriques

[2] Qu'est-ce que l'algorithme de minage Equihash? (s.d.). Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/qu%27est-ce-que-l%27algorithme-de-minage-equihash/

[3] caracteristique de la cryptomonnaie. (s.d.). https://www.lhommetendance.fr/caracteristiques-de-la-cryptomonnaie/. Consulté le 2022, à l'adresse https://www.lhommetendance.fr/caracteristiques-de-la-cryptomonnaie/

[4] Academy, B. (2022, 28 avril). Qu'est-ce que le Bitcoin ? Binance Academy. Consulté le 2022, à l'adresse https://academy.binance.com/fr/articles/what-is-bitcoin

[5] https://al-ain.com/article/cryptocurrency-prices-ukraine-war-fears-bitcoin

[6] Freepik. (2021, 2 avril). Ville intelligente futuriste avec technologie de réseau mondial 5g Photos gratuites. Consulté le 2022, à l'adresse https://fr.freepik.com/photos-vecteurs-libre/monnaie-numerique

[7] Academy, B. (2022a, mars 22). Qu'est-ce qu'Ethereum ? Binance Academy. Consulté le 2022, à l'adresse https://academy.binance.com/fr/articles/what-is-ethereum

[8] Academy, B. (2021, 18 novembre). Qu'est ce que Ripple? Binance Academy. Consulté le 13 février 2022, à l'adresse https://academy.binance.com/fr/articles/what-is-ripple

[9] dummies Learning Made Easy. (s. d.). Dummies. Consulté le 2022, à l'adresse https://www.dummies.com/article/business-careers-money/personal-finance/cryptocurrency/the-structure-of-blockchains/

[10] https://coin24.fr/wp-content/uploads/2020/06/Blockchain-sch%C3%A9ma1-1024x586-1.jpg

[11] Tshilonda, T. (2021, 17 septembre). Qu'est-ce qu'un portefeuille de crypto-monnaie (wallet crypto) et comment fonctionne-t-il ? IG. Consulté le 2022, à l'adresse https://www.ig.com/fr/strategies-de-trading/qu_est-ce-qu_un-portefeuille-de-crypto-monnaie--wallet-crypto--e-210917#information-banner-dismis

[12] Bit2Me, A. (2022, 23 mars). Bit2Me Academy - Formation Bitcoin et Crypto-monnaie. Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/

[13] http://dspace.univ-tebessa.dz:8080/jspui/bitstream/

[14] Qu'est-ce qu'un portefeuille ou un sac à main crypto-monnaie? (2022, 28 avril). Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/portefeuille-portefeuilles-de-crypto-monnaie/

[15] *Qu'est-ce qu'un portefeuille de cryptomonnaies ?* (s. d.). www.coinbase.com. Consulté le 2022, à l'adresse https://www.coinbase.com/fr/learn/crypto-basics/what-is-a-crypto-wallet

[16]https://encryptedtbn0.gstatic.com/images?q=tbn:ANd9GcQyeOujOrW4hrZLtc48Im1RXSuLXzG5WypC-w&usqp=CAU

[17] https://www.google.com/

[18] C., & Cryptonaute, V. T. L. A. (2022, 31 mars). Wallet Crypto | Liste des meilleurs portefeuilles Crypto 2022. Cryptonaute. Consulté le 2022, à l'adresse https://cryptonaute.fr/wallet/portefeuille-crypto-monnaie/

[19] http://dspace.univ-jijel.dz:8080/xmlui/handle/123456789/8575

[20] A. (2021, 6 mai). Comment fonctionne une transaction en bitcoin ? Voici nos explications. Pour une autre économie. Consulté le 2022, à l'adresse https://pouruneautreeconomie.fr/comment-fonctionne-transaction-bitcoin/

[21] B. (2020, 20 décembre). Les différents algorithmes de consensus blockchain. BriefCrypto. Consulté le 2022, à l'adresse https://www.briefcrypto.com/les-differents-algorithmes-de-consensus-blockchain/

[22] Lars, L. (2020, 30 juin). Qu'est-ce que la preuve de travail ou proof-of-work (PoW) ? Cryptoast. Consulté le 2022, à l'adresse https://cryptoast.fr/qu-est-ce-que-le-pow-proof-of-work/

[23] C. (2022, 12 avril). Qu'est-ce que le Proof of Stake (PoS) - preuve d'enjeu ? crypto-sous.fr. Consulté le 2022, à l'adresse https://www.crypto-sous.fr/blockchain-fonctionnement/proof-of-stake/

[24] https://www.technoscience.net/illustration/Definition/inconnu/h/Hash-function-fr.svg

[25] https://www.alroeya.com/207-0/2259563

[26] RÉ ; Daction, L. (2019a, février 12). *Plateforme d'échange de cryptomonnaies : ce qu'il faut savoir*. www.journaldunet.f. Consulté le 2022, à l'adresse https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1209386-plateforme-d-echange-de-cryptomonnaies/

[27] de Futura, L. R. (2020, 12 janvier). Quelles sont les meilleures applications pour transférer des cryptomonnaies ? Futura. Consulté le 2022, à l'adresse https://www.futura-sciences.com/tech/questions-reponses/informatique-sont-meilleures-applications-transferer-cryptomonnaies-12501/

[28] *Association Europe-Finances-Régulations | AEFR*. (s. d.). Association Europe-Finances-Régulations. Consulté le 2022, à l'adresse https://www.aef.asso.fr/l-146-analyse-juridique-du-bitcoin/

[29]https://www.researchgate.net/publication/333664700_Conception_et_modeles_de_blockchain_-_Bitcoin

[30] Hayek, Friedrich von. 1976. "Denationalization of Money: The Argument Refined." https://nakamotoinstitute.org/static/docs/denationalisation.pdf.

[31] The Economist. 2018. "Bitcoin and Other Cryptocurrencies Are Useless." The Economist, 2018. https://www.economist.com/leaders/2018/08/30/bitcoin-and-other-cryptocurrencies-are-useless.

[32] Kostakis, Vasilis, and Chris Giotitsas. 2014. "The (A)Political Economy of Bitcoin." ResearchGate. 2014. https://www.researchgate.net/publication/287241993_The_APolitical_Economy_of_Bitc oin.

[33] RÉ ; Daction, L. (2019, 6 mars). *Miner : définition du minage en cryptomonnaie*. minage en cryptomonnaie. Consulté le 2022, à l'adresse

https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1207718-miner/

[34] Crypto Stratégie. (2020, 22 octobre). SHA256 - Algorithme de hachage SHA256. Consulté le 2022, à l'adresse https://cryptostrategie.com/sha256-algorithme-bitcoin/

[35] Qu'est-ce qu'une fonction de hachage ? - bitcoin.fr

[36] Bit2Me, A. (2022b, mars 23). Qu'est-ce que l'algorithme de minage Equihash? Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/qu%27est-ce-que-l%27algorithme-de-minage-equihash/

[37] Community, B. (2021, 6 janvier). What is "Equihash"? Welcome to BITCOINZ. Consulté le 2022, à l'adresse https://getbtcz.com/what-is-equihash/

[38] Qu'est-ce que l'algorithme d'exploration de données X11 ? (2022, 23 mars). Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/qu%27est-ce-que-l%27algorithme-de-minage-x11/

[39] Qu'est-ce que le cloud mining ou le cloud mining ? (2022, 23 mars). Bit2Me Academy. Consulté le 23 mars 2022, à l'adresse https://academy.bit2me.com/fr/qu%27est-ce-que-le-cloud-mining-cloud-mining/

[40] Partenaire, A. (2021, 14 décembre). *Cloud mining : Les 5 meilleurs services en 2022*. cloud mining. Consulté le 2022, à l'adresse https://lepetitjournal.com/expat-pratique/patrimoine/cloud-mining-les-5-meilleurs-services-en-2022-327390

[41] Que sont les mineurs ASIC ? (2022, 23 mars). Bit2Me Academy. Consulté le 2022, à l'adresse https://academy.bit2me.com/fr/qui-sont-mineurs-asic/

[42] *Miner avec un ASIC (Tutoriel 2021)*. (s. d.). Miner-avec-asic. Consulté le 2022, à l'adresse https://greenbull-campus.fr/immobilier/guide/patrimoine/diversifier/miner-avec-asic

[43] https://www.google.com

[44] https://www.mcafee.com/enterprise/fr-fr/assets/reports/rp-blockchain-security-risks.pdf

[45] Lajeune, G. (2022, 26 février). Le Bitcoin (BTC) est-il anonyme ? Futura. Consulté le 2022, à l'adresse https://www.futura-sciences.com/tech/questions-reponses/cryptomonnaies-bitcoin-btc-il-anonyme-15960/

[46] Richter. (2021, août 3). PERTE de cryptomonnaies. Consulté le 2022, à l'adresse https://www.richter.ca/fr/nos-reflexions/perte-de-cryptomonnaies/

[47] Le Bitcoin consomme presque autant que tous les Français réunis. (2022, 17 février). Selectra. Consulté le 2022, à l'adresse https://selectra.info/energie/actualites/insolite/bitcoin-consommation-electricite

[48] Deluzarche, C. (s. d.). Java : qu'est-ce que c'est ? Futura. Consulté le 2022, à l'adresse https://www.futura-sciences.com/tech/definitions/informatique-java-485/

[49] Wikipedia contributors. (2022, 2 mars). *Java Development Kit*. Java_Development_Kit.Consulté le 2022, à l'adresse https://fr.wikipedia.org/wiki/Java_Development_Kit

[50] Blockchain Bitcoin : Découvrez comment ça marche ! (acheterbitcoin.info)