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
Département : Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine : Mathématiqueset Informatique
Filière : Informatique
Option : Résaux et sécuirité informatique
Thème

Analyse de la sécurité De la crypto-monnaies

Présenté Par

Meriem Mesnadi

Devant le jury

Dr. Ben Djenna.H	*PR*	*Univérsité Larbi Tébessi*	*Président*
Dr. Sahraoui.A	*MCB*	*Univérsité Larbi Tébessi*	*Examinateur*
Dr. Mekhaznia Taher	*MCA*	*Univérsité Larbi Tébessi*	*Encadreur*

Date de soutenance : 11/07 /2021

REMERCîMENTS

J'adresse mes remerciements à Dieu puis à ma encadreur Dr Mekhaznia.T, je tiens à lui exprimer ma gratitude pour la confiance qu'il m'a accordée et j'espère que ce travail sera à la hauteur de ses attentes. Je le remercie également pour son encadrement exemplaire, son accessibilité et sa grande disponibilité.

Je tiens également à exprimer ma gratitude à Monsieur le Président du jury, bendjenna hakim, et à Monsieur examinateur Sahtaoui.A,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.

Je tiens également à remercier tous les professeurs du Département de mathématiques et d'informatique.

Je remercie également ma famille, mes amis et mes collègues.

DÉDICACE

Je dédie ce modeste travail

A Mon Cher père,

A ma chère mère,

A mes frères,

A mes enseignants,

A mes amis,

Et à mes collègues.

Résumé

Apparu crypto-monnaies en tant que système de transaction sur réseau pair à pair utilisant déchiffrement pour le créer et le distribuer et cela dépend de la blockchain.
Ce qui assure un niveau élevé de transparence et de vérification de toutes les transactions individuelles utilisation d'algorithmes de mineurs et consensus qui s'appuient sur les travailleurs pour vérifier les transactions et leur validité.
Le but de la présente étude est d'expliquer crypto-monnaies et les transactions de manières sécurisé et essayez d'implémenter blockchain en java.

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

الملخص

ظهرت العملات الرقمية كنظام تبادل من نظير لنظير باستخدام التشفير لانشائها وتوزيعها.ويعتمدون في ذلك على البلوكشين والذي يوفر مستوى عال من الشفافية والتحقق من جميع المعاملات الفردية باستخدام التعدين الذي يعتمد على المعدنين للتحقق من المعاملات وصحتها.

الهدف من هذه الدراسة هو شرح مفهوم العملات الرقمية وكيفية تبادلها بطريقة امنة ومحاولة تطبيق البلوكشين بلغة الجافا.

الكلمات المفتاحية: :العملات الرقمية،العملات المشفرة، البلوك تشين، البيت كوين ،المفتاح العمومي، المفتاح السري، المحفظة الالكترونية

Sommaire

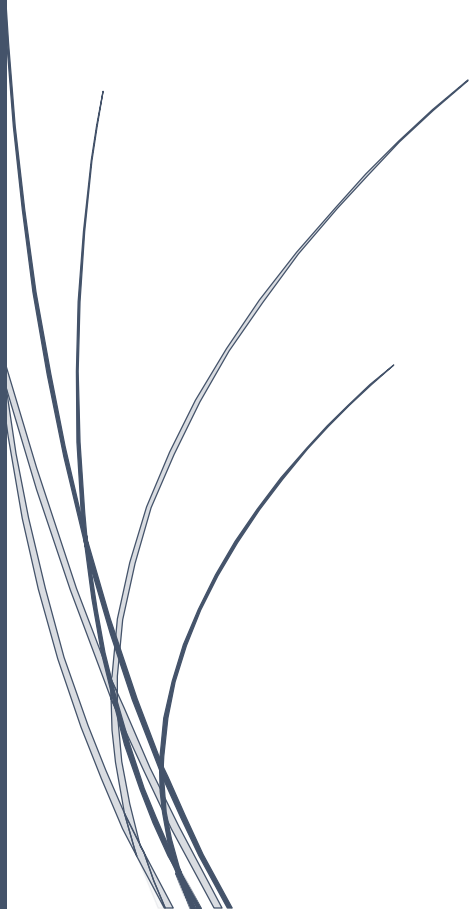
Sommaire

Chapitre 3 Blockchain

List des figures

Liste d’abréviations

POS	Proof Of Stake
POW	Proof Of Work
DLT	Distributed Ledger Technology
P2P	Peer-To-Peer.
AES	Advanced Encryption Standard
DDosDistributed	Denial Of Service attack



Introduction générale

Les crypto-monnaies sont un nouveau monde et peuvent être définis comme le terme universel pour décrire, tous les fonds électroniques, y compris les monnaies virtuelles et les crypto-monnaies sont disponible électroniquement et sous forme numérique, contrairement aux papier monnaies ou des pièces de monnaies, qui sont considérés comme intangibles.

En 2008, la première crypto-monnaie « Bitcoin » a été annoncée par le programmeur Satoshi Nakamoto.

En 2015 de nouvelles crypto-monnaies « Litecoin »et « Ethereum » ont émergé ont levé 75 millions de dollars.

En 2019, Facebook a annoncé Libra sa propre monnaie, qui a été lancée en 2020.

Notre objectif dans cette étude est d'analyser la sécurité des monnaies numériques en sachant comment crée des clés et leur rôle dans la confidentialité des transactions et des crypto-monnaies de données avec le rôle des algorithmes de consensus spécifiquement la preuve de travail et le preuve d'enjeu dans la protection des monnaies numérique.

Blockchain joue le rôle principal dans la création de crypto monnaies, qui distribue des informations numériques à toutes les parties du réseau au lieu de les copier. Cela signifie que chaque partiede données appartient à un seul propriétaire. Ainsi, en utilisant les fonctionnalités blockchain,on peut assurer que les crypto-monnaies sont transparentes. On a donc essayé d'implémentation blockchain, pow et pos en java pour avoir comment fonctionnent la sécurité de crypto-monnaies.

Les crypto-monnaies sont récemment devenues plus sécurisé en raison de son application de l'algorithme de preuve d'enjeu et de sa mise à jour fréquente pour vérifier de plus en plus de transaction et leur validité.

Et même dans les résultats d'implémentations des algorithmes POS et POW, on a trouvé que le preuve d'enjeu mieux que le preuve de travail coté à temps d'exécution.

Crypto-monnaies

1. Introduction

Dans ce chapitre, on parle d'abord de la définition de monnaie numérique, les types, des caractéristiques de la monnaie numérique, des réseaux de gestion, les transactions dans la monnaie numérique avec un exemple du classement de monnaie numérique. Dans la partie principale du chapitre, on parle la structure de données et les algorithmes le plus utilisé. Enfin, on parle le portefeuille de monnaie numérique, la définition avec ses types.

2. Qu'est-ce que monnaie numérique

La monnaie numérique est une nouvelle forme de monnaie qui n'existe que sous forme électronique ou numérique [1], c'est une monnaie qui stocké dans la blockchain et échange via des systèmes. [2]

3. Types monnaie numérique

Il y a deux types :

3.1 Centraliser

Les crypto monnaies centralisés ont un gérant c'est-à-dire un responsable(directeur), comme par exemple toute entreprise ou institution qui a un gestionnaire qui contrôle les employés. [3]

Les points faibles : [3]

- Concentration de puissance.
- Manipulation des prix.
- Risque crucial.

3.2 Décentraliser

Les crypto monnaies décentralisées c'est contraire de les crypto monnaies centralisés, n'ont pas gestionnaire non autorités que vous contrôlez et ont un système DLT situé dans blockchain qui gère leurs transactions et leurs échanges. [3]

Les Catégories :

- Politiquement décentralisé c'est-à-dire aucune entité peut contrôler le blockchain. [3]
- Architecturalement décentralisé il ne pas un point faible de défaillance central c'est-à-dire un système centralisé de fonctionner. [3]

4. Caractéristiques de la monnaie numériques :

Décentralisé. [4]

Ne change pas les données quelconque utilisateur(fixé). [4]

Il n'a pas besoin utilisateur pour l'identification personnel. [4]

5. Réseaux de gestion

Les crypto monnaies utilisant un réseau pair à pair(p2p) décentralisé. Ce réseau se compose de plusieurs ordinateurs et dans chaque ordinateur un blockchain, le blockchain contient un ou plusieurs blocs, chaque bloc peuvent assumer une variété de rôles différents par exemple sont assurent la sécurité de réseau en vérifiant les transactions par rapport aux règles d'algorithme de consensus. Lorsque des crypto monnaies sont envoyées au client, le bloc est le serveur et lorsque on reçoit des crypto monnaies, elles sont le client et chaque fois envoyées ou reçu, ces données sont stockées dans la blockchain. [5]

À être le réseau pair à pair qui transfère les crypto-monnaies d'un utilisateur à autre via blockchain. [5]

6. Transaction du la monnaie numérique :

La transaction commence par envoyer à un utilisateur A un bitcoin ou un autre crypto monnaies pour une différente personne B. par exemple

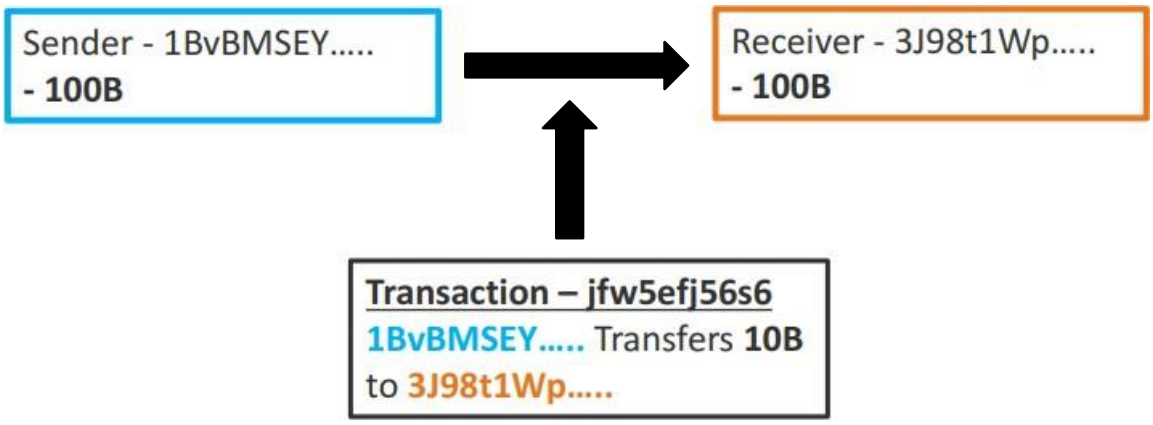


Figure1 :première transaction. [4]

Ensuite, envoie le crypto-monnaies du portefeuille de A au portefeuille de B sur le réseau, A signe et envoie des transactions comme ci-dessus :

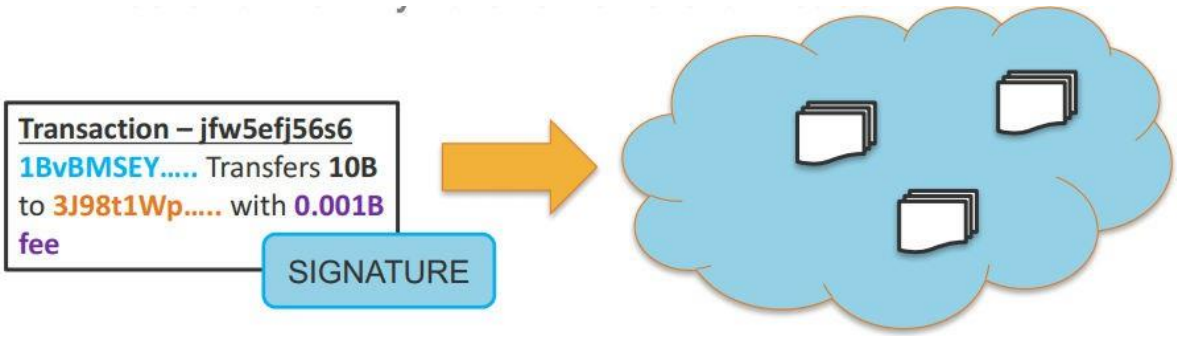


Figure2 : Signal transaction [4]

Un validateur vérifié la signature et la transaction sont valide, si valide il ajoute la transaction à son bloc pour obtenir une recompose et il résout un puzzle difficile.

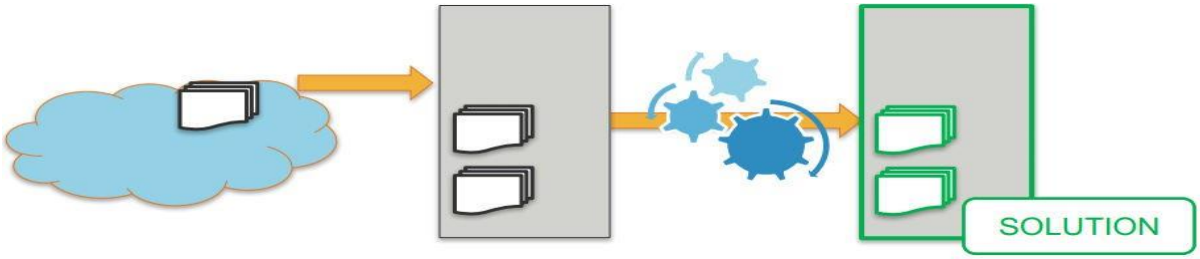


Figure 3 : Vérification de transaction [4]

Si le bloc est valide est diffusé sur le réseau en deux participant :

Le première participant vérifiant les transactions et signatures sont valides, deuxième participant sont vérifient la solution du puzzle est correcte.

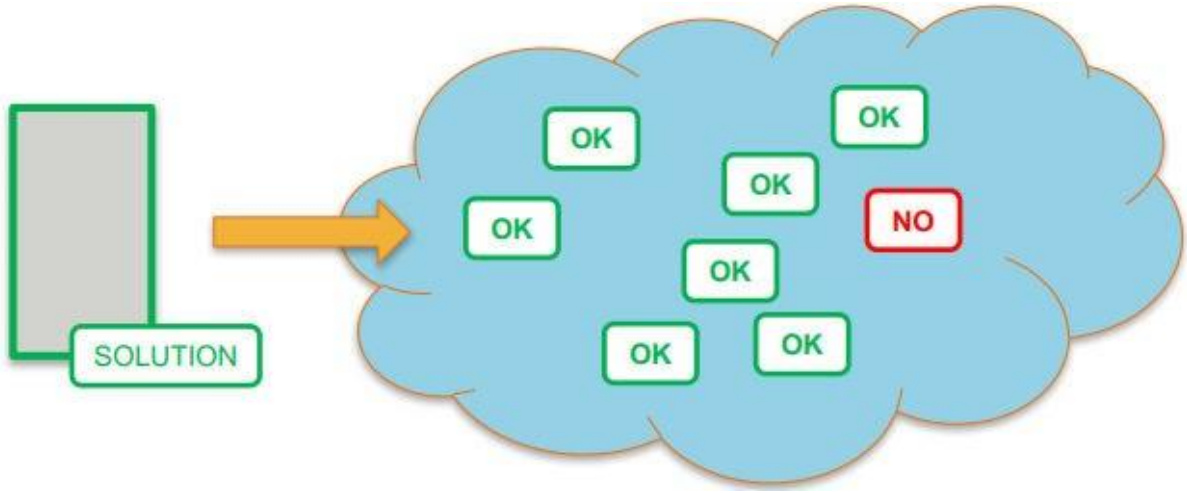


Figure4 : Transaction valide.[4]

Chaque récepteur peut trouver deux réponses valide ou non valide, comme ci-dessus

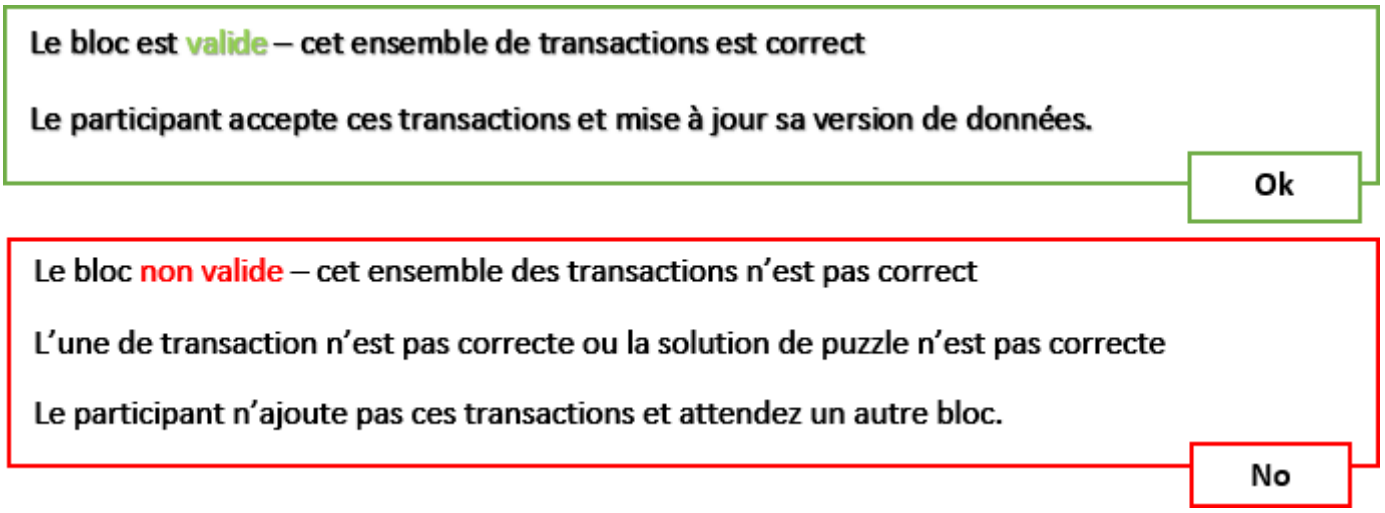


Figure5 : Notification de la transaction [4]

Après de quelques minutes, si la transaction est valide

Figure 6 : Accepte la transaction [4]

Découvrez le classement des 10 plus importantes monnaies virtuelles en tenant compte de leur capitalisation boursière : [6]

Liste de Crypto-monnaies	Date de création	Capitalisation boursière au 03 juin 2021	Variation des cours sur 1 an (USD)
Bitcoin (BTC)	2009.	731,945 milliards de dollars	+ 3,85 % environ.
Ethereum (ETH)	2015.	329,203 milliards de dollars	+ 4.50 % environ.
Binance coin (BNB)	2017.	65,499 milliards de dollars	+ 4.09 % environ.
Tether (USDT)	2015.	61,770 milliards de dollars.	– 0,30 % environ.
Cardano (ADA)	2015.	58,360 milliards de dollars.	+ 2,84 % environ.
Dogecoin (DOGE)	2021.	52,783 milliards de dollars	-3,82 % environ.
Ripple (XRP)	2012.	47,535 milliards de dollars.	+ 0,98 % environ.
Polkadot (DOT)	2016	27,074 milliards de dollars	+4,71 % environ.
USD Coin(USDC)	2018.	22,679 milliards de dollars.	0,00 % environ.
Uniswap (UNI)	2018.	14,680 milliards de dollars	+1,99 % environ.

Tableaux des exemples de liste crypto-monnaies [7]

7. Structure de données

7.1. Qu'est-ce que DLT (Distributed Ledger Technology) ?

Il s'agit à l'origine d'un système de base de données décentralisé, contenant toutes sorte de technologies responsable de l'échange entre les utilisateurs sur la plate-forme. [8]

Blockchain est un type de DLT. [8]

7.2.La structure de données dans DLT

- Etape01 : utilisateur de réseaux crypto monnaies ont une copie du grand livre DLT toute les données du transaction accepté, DLT est stocké dans la structure de Blockchain. [8]
- Etape02 : Les informations numériques sont collectées sous forme du bloc dans la blockchain. [8]
- Etape03 : Les utilisateurs créent des blocs de données contenant des informations sur leurs transactions. [8]
- Etape04 : ces données sont enregistrées sous la forme d'un réseau p2p à internet à l'aide d'un ordinateur confiance et crypté. [8]
- Etape05 : lier chaque nouveaux blocs données autre blocs précèdent par hach de bloc précèdent pour former ce qu'on appelle la Blockchain. [8]

8. Les algorithmes

Pour sécuriser les crypto-monnaies, vous devez utiliser un algorithme de hachage ou fonction du hach, ci-dessus les plus utilisés :

- SHA-256 : cet Algorithme indépendamment la longueur et la forme de l'entré, elle est hachis en un hachage fixe sur 256 bits. [9]
- EtHash : cet algorithme de hachage utilisé dans Etherieum. Basé sur le blockchain, il repose sur une très grande mémoire. [9]

Tout d'abord, il crée une valeur de départ(seed) à partir de bloc avant que le minage de données ne commence son travail, puis utilise seed pour créer un faux mémoire de taille 16 Mo, qui utilise pour créer plus 4Go de données afin de mettre à jour tous les 300000 bloc, après quoi l'exploration de données dans un réseau.Enfin, ce processus est vérifié en recréant temporairement une partie des données dansla mémoire de stockage.

- X11 : cet algorithme est plus complexe que l'algorithme SHA-256 car utilise 11 hachages différents. Ce qui le rend plus sûr et plus avancés dans l'utilisation. [9]

Cette algorithme contient 11 parties qui sont dans l'ordre suivante :

1. BLAKE
2. BLEU MIDNIGHT WISH(BMW)
3. GrosH
4. JH
5. Keccak
6. Echeveau
7. Luffa
8. CubeHash
9. SHAvite-3
10. SIMO
11. ECH

D'un ordre à l'autre, le mineur commence a créé le premier bloc de Hash au détail BLAKE, dépend du cryptage qui fonctionne sur une matrice de 4*4 mots dans la sélection de hachage, après quoi le reste des parties sont applique a le première bloc et ainsi de suite jusqu'à ce que toutes les parties soient terminer.

- EquitHash :cet algorithme repose sur une grande mémoire, donc la quantité de minage dont ondispose est contrôlée par la quantité de RAM. [9]
- CryptoNight :cet algorithme utilise la méthode de hachage à accès aléatoire, dépend de la RAM pour ralentir le mémoire et augmenter le temps de latence. [9]

Cette algorithme utilise le cryptage AES pour crée la clé en entrant des données et en convertissant en 31 octets de hachages avec fonction Keccak, puis le reste des données qui passent par 10 cycles pendante cryptage, puis l'envoie a DLT ou son espace de stockage dans mémoire.

- Scrypt :cet algorithme est gourmand en mémoire en cas d'attaque ceux-ci créent des faux nombres aléatoires, ce qui fait un grand nombre de crypto-monnaies utiliser. [9]

L'algorithme du Scrypt dérive la clé principale pendant les fonctions de mémoire séquentielle. Il fait une fragmentation à l'aide de la clé et de série des points marquer avec des bruits, ce bruit est série de nombre aléatoire qui sont stocker en mémoire.

9. Portefeuille du crypto-monnaie

Portefeuille (wallet en anglais) c'est un programme et une base de données ou outil qu'une Blockchain utilise pour envoyer, recevoir et sécuriser des crypto-monnaies. [10]

9.1. Fonctionnement de portefeuille

Le portefeuille crée des propres informations d'utilisateur (clé publique, clé privé et adresse) pour envoyer et recevoir des crypto monnaies et contrôler les transactions. Premièrement vérifier que l'utilisateur a des crypto monnaies ou non, permet à l'utilisateur de connaitre la date de ses transactions, envoyer et recevoir des crypto monnaies a toute sécurité, après vous être assuré que la transaction est correcte, directement connecté au blockchain vous envoyez une copie de transaction de manière sécurité. [9]

9.2. Les Types de Portefeuille :

9.2.1. Portefeuille chauds (hot wallet) :

C'est un outil qui permet aux utilisateurs de crypto-monnaie d'envoyer et recevoir jetons. C'est connecté à Internet, c'est comme si le portefeuille dans votre poché est facile à utiliser mais il vulnérabilité. [10] il y a deux types :

- **Logiciel portefeuille :**

il est un programme qui installé l'utilisateur sur son ordinateur ou son appareil mobile pour contrôler entièrement les crypto-monnaies. [10]

Avantages de Logiciel portefeuille :

- Stocker les clés de sécurité dans l'ordinateur ou l'appareil mobile. [10]
- Plus contrôler les transactions de cryptomonnaies. [10]

Inconvénients de Logiciel portefeuille :

- Plus susceptibles d'être voles en raison du piratage de l'appareil. [10]
- Plus complexes dans leur utilisationpar rapport les autres portefeuilles.[10]

➢ **Portefeuille En ligne:**

Il est plus convivial parce qu'il ressemble à des applications web. L'utilisateur doit vérifier son niveau de sécurité avant de l'utiliser. [10]

Avantages d'En ligne portefeuille :

- Facile à utiliser. [10]
- Vous n'avez pas besoin d'être installé. [10]

Inconvénients d'En ligne portefeuille:

- On n'a pas le droit de contrôler votre portefeuille a 100% parce que le site est responsable de portefeuille pas l'utilisateur. [10]
- Si le site est compromis, votre portefeuille perdu parce que l'utilisateur n'a pas sa clé privée, le site possédé la clé. [10]

9.2.2. Portefeuille froids (cold wallet) :

C'est utiliser un appareil pour stocker les clés, les rendre hors ligne, ce qui les rend moins vulnérables aux attaques, contrairement aux portefeuilles chauds. [10] il y a deux types :

➢ **Portefeuille matériel :** c'est un USB utilise pour créer les clés, plus sûr que reste des portefeuilles, mais il y a un problème qui l'exposé à des risques d'attaque s'il n'est pas installé correcte. [10]

Figure7 : Exemple du portefeuille matériel(USB). [10]

Avantages de portefeuille matériel :

- Plus sécurisé pour les attaques. [10]

Inconvénients de portefeuille matériel :

- Le prix trop élève, donc ce n'est pas beaucoup utilisé.[10]

➢ **Portefeuille papier** :créer les clés de portefeuille par un programme, puis imprimés sur une feuille de papier avec le code QR utilisé lors de chaque transaction. [10]

Figure8 : Exemple de portefeuille papier du Bitcoin. [10]

Avantages de portefeuille papier :

- Plus sécurisé pour les attaques. [10]

Inconvénients de portefeuille papier :

- Faible d'utilisation parce que transfert régulier.[10]

dans cette figure structure de tous les types des portefeuilles

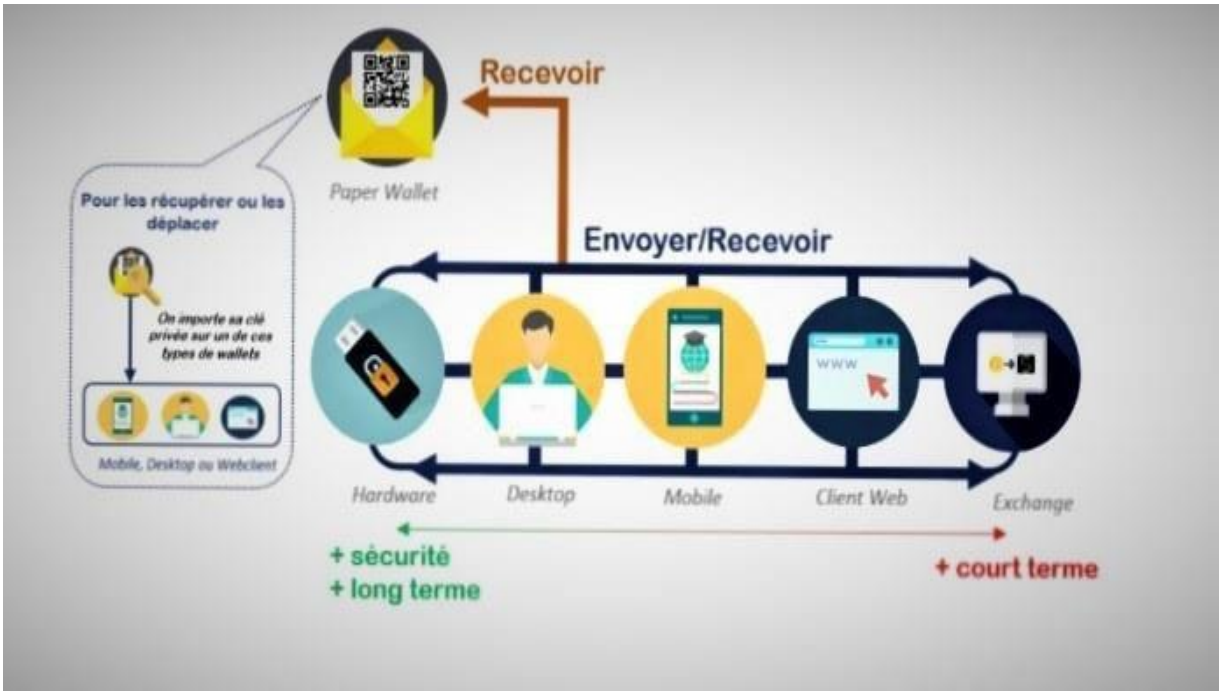
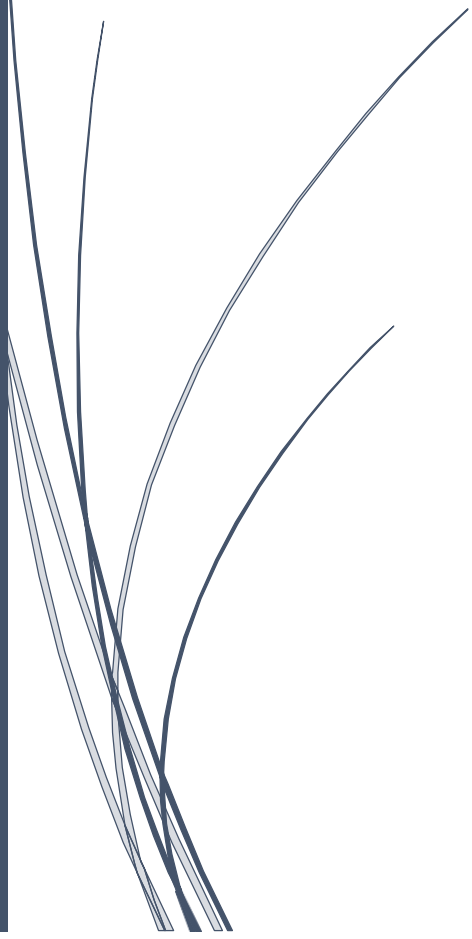


Figure09 : Structure des portefeuilles. [10]

10. Conclusion

Dans ce chapitre, nous avons vu un aperçu de la monnaie numérique comprenant la définition, ses caractéristiques, ses transactions et sa gestion de réseaux. Enfin, nous avons montré des exemples de monnaie numérique

sécurité de la cryptomonnaie



1. Introduction

Dans ce chapitre, nous verrons les clés de chiffrement de différents types et comment elles sont créées et travaillées. Ensuite preuve de travail et la preuve d'enjeu dans la protection des crypto monnaies et les différentes entre elle. Et enfin, nous allons parler des problèmes auxquels vous étés confortes.

2. Cryptographique asymétrique

Le chiffrement asymétrique est une méthode de chiffrer des messages ou des données,et déchiffré avec deux clés différentes (publique, privé) pour rendre l'attaque ou le vol difficile.[12]

2.1 Méthode de fonctionnement

La personne A envoie un message chiffré par la clé publique a la personne B, il est déchiffrant avec sa clé privée, comme l'exemple suivante :[12]

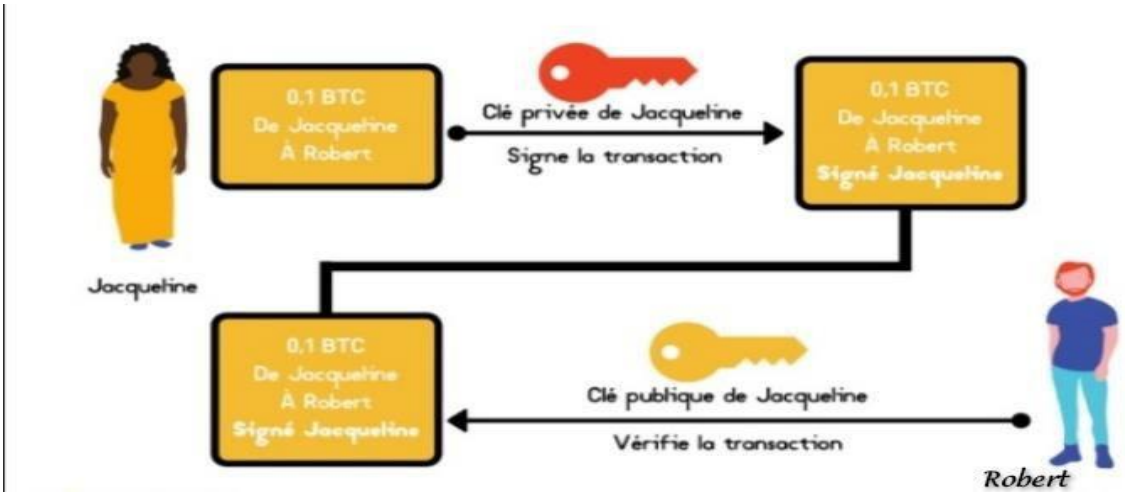


Figure10 Exemple d'utilisation les clés. [12]

2.2 Les Clés

2.2.1 Clé publique

Est une série aléatoire de chiffres qui peuvent être obtenus à partir de la clé à l'aide de processus de cryptage et de fragmentation, qui est également l'adresse à partir de laquelle les transactions de crypto-monnaie sont reçues. [13]

2.2.2 Clé privé

Est une grande série de nombres qui peuvent être un code binaire de 256 caractères, ou 64 code hexadécimale à 64 chiffres, qui est la clé qui ouvre votre crypto-monnaie et prouve qu'il vous appartient, pas à quelqu'un d'autre. [13]

2.2.3 Adresse

Pour créer une adresse du portefeuille en appliquent des algorithmes à la clé publique pour dériver l'adresse que l'utilisateur connait. [13]

2.2.4 Signature

Est une série de chiffre alphanumérique incompréhensibles, créé à partie de clé privé appliquer des algorithmes spéciaux entre utilisateur expéditeur et récepteur.

- Chiffrer la transaction avec une clé publique.
- La transaction est signée à l'aide de la clé privée en combinant avec les données envoyées.
- La transaction peut être validée à l'aide de la clé publique. [13]

Figure 11. Exemple de clés. [12]

3. Consensus algorithmes

Est une stratégie qu'un groupe d'ordinateurs utilise pour s'entendre entre eux sur ce qui est vrai. Il y a différente saveurs d'algorithme de consensus que les gens ont applique que chacun a des priorités ou des compromis différents en termes de sécurité d'accord et qui peut voter sur quoi. [14]

Le but de l'algorithme de consensus est juste de gérer quels participants au réseau arrivant à définir l'état de vérité que toute le monde est d'accord. [14]

Il y a beaucoup types d'algorithme de consensus qui ont été développés, parmi ces algorithmes preuve de travail et preuve d'enjeu. [14]

3.1 Preuve de travail(POW)

3.1.1 Définition

Preuve de travail (Proof Of Work) est l'algorithme utilisé par réseau blockchain afin de valider les transactions et créer de nouveaux blocs. Les mineurs utilisent cet algorithme pour confirmer les transactions. Le premier à terminer la validation obtient le droit créer le et reçoit une récompense. [15]

3.1.2 Comment fonctionne la preuve de travail ?

Preuve de travail dépend sur deux choses principales : puzzle mathématique complexe et possibilité résolution facile. Blockchain donner ce puzzle complexe aux mineurs pour transaction valide, et essayez de le résoudre avec les fonctions de hach, ceux qui ont obtenu la bonne solution partagent nouveau bloc, et ils vont vérifier si les comptes sont corrects, si c'est vrai il a créé un premier bloc. [16]

3.1.3 L'objectif de preuve de travail

Empêcher les utilisateurs de doubler les dépenses difficiles à résoudre sans administrateur ou l'impression de crypto-monnaie non gagné. [15]

3.1.4 Les avantages de preuve de travail

La preuve de travail est principalement utilisée pour prévenir les attaques DOS. DOS a besoin de beaucoup de temps, de calcul et de pouvoir informatique (power computing), il n'a y donc pas d'utilisation de telles attaques car le temps pour créer des blocs est trop, donc ce ne sera pas le moment de gâcher la transaction ou de faire de gros bénéfices de l'exploitation manière car un seul mineur crée le bloc à chaque fois. [15]

Contrôler l'exploitation manière en rendant difficile la résolution d'énigmes. [15]

3.1.5 Les problèmes de preuve de travail

Très cher en raison de son utilisation de machines minières qui consomment des très grandes électricités. [15]

Utilisez des appareils très couteux pour résoudre des puzzles. [15]

51% attaque, ce qui permet aux utilisateurs contrôler la puissance minière pour crée de nouveaux blocs et obtenir recomposés. [15]

3.2 Preuve d'enjeu(POS)

3.2.1 Définition

Il s'agit d'un algorithme de compatibilité qui examine la validité des transactions et des données dans la blockchain, c'est un algorithme d'économie d'énergie. Ils produisent plus de bloc et plus rapides par seconde que les preuve d'emploi et les travailleurs doivent prouver leur propriété. [17]

3.2.2 Fonctionnement

La transaction commence après quoi les données sont exécutées dans un bloc,d'une capacité 1Mégabits, il est répété sur de nombreux ordinateurs ou dans un contrat, ce contrat est l'organe directeur de Blockchain. [17]

3.2.3 L'objectif

Si le réseau détecté une transaction non validée, ainsi le nœud inspecter une partie de sa part et non-participation à l'avenir, afin de pouvoir contrôler les transactions frauduleuses,

le nœud doit avoir une participation de attaques 51%. En le cas de crypto-monnaies pour contrôler le réseau, ondoit besoin d'acquérir 51% du nombre de coins dans on compte. [17]

3.2.4 LesAvantages

N'utilise pas beaucoup d'énergie électricité et plus sécurisé par rapport pow.[17]

Encourage les utilisateurs exécuté les blocs parce que c'est facile. [17]

3.3 Différence entre POW et POS

La première différence entre eux est que la preuve de travail est que la capacité de vérification dépend de la puissance de l'ordinateur, mais la preuve d'enjeu dépend de la vérification de validité de la transaction. [18]

Deuxièmes, en preuve le travail des récompenses des mineurs pour résoudre le puzzle de cryptage, quant à preuve,il n'y a pas de récompenses, mais collecte des frais de transaction. [18]

Troisièmes, la preuve de travail nécessite des appareils puissants pour ajouter de nouveaux blocs, conduisant à des attaques de 51%, quant à la preuve d'enjeu, elle a besoin de 51%de toutes les crypto-monnaies, ce qui rend les attaques impossibles et difficiles. [18]

4. Problématique

Selon les informations sur les crypto-monnaies, la plupart d'entre nous pensent qu'il est très sûr et confidentiel en raison de son utilisation de la blockchain et des algorithmes cryptés qui difficiles àrésoudre, mais les attaques chaque fois qui ils découvrent une entrée l'attaquant comme DDos qui suspend temporairement l'appareil afin qu'il leur permette de désactiver le service à tous égards.

Cela affecte négativement les utilisateurs l'échange de crypto-monnaies, ainsi que la violation de temps dans laquelle l'attaquant donne le mauvais moment pour un complexe ce qui rend

l'apparition de doubles dépenses de crypto monnaies. Ces hacks n'ont pas de solution, même s'ils sont trop dangereux.

5. Conclusion

Dans ce chapitre, nous avons vu le cryptographie symétrique, les clés de sécurité de crypto-monnaies , ensuite preuve de travail et preuve d'enjeu .Enfin, nous avons un problématique.

Chapitre 03

Blockchain

1. Introduction

Dans ce chapitre, on parle d'abord de définition de blockchain, des caractéristiques, des composant et des différents types. Dans la partie principale du chapitre, on parlera de la structure de données blockchain en commençant par le bloc de chaine et le réseau. Après cela, on parlera de l'implémentation de blockchain en java. Enfin on arlera de l'expérimentation de POW et POS.

2. Qu'est un blockchain

Il s'agit d'un système de base de données qui permet de stocker des transactions.

La technologie décentralisée qui transmet des crypto-monnaies à l'aide de clés de chiffrement et d'algorithmes de minage. A été appliquée pour la première fois au bitcoin. [19]

3. Composant du Blockchain

Blockchain contient les composants suivants :

Nœud :chaque utilisateur connecté au réseau Blockchain.

Transaction : chaque opération entre les nœuds du réseau qui est enregistrée dans un bloc.

Bloc : une structure de données pour l'enregistrement des transactions qui est distribuée dans tout le réseau.

Chain : un groupe de blocs liés dans un ordre spécifique.

Miner : nœuds spécifiques du réseau qui sont chargés de vérifier les blocs.

Consensus : règles et dispositions prises pour exécuter les opérations Blockchain. [20]

4. Hach cryptographie

On entre une série alphanumérique, quelle que soit la longueur pendant laquelle elle se transforme en une longueur fixe (32bits, 64bits, 128bits ou 256bits). Parmi ses caractéristiques: non reproductible, calculant la valeur au détail dans un temps très court, il n'y a pas deux messages de la même valeur au détail. [21]

Blockchain utilise le cryptage de hachage pour chiffrer les données stockées dans une chaîne et connecter des blocs les uns aux autres. Il place son propre hachage et son code de hachage précédent dans un bloc, ce qui le rend immuable. [21]

5. Types de blockchain

5.1. Publique blockchain

Tout utilisateur peut y participer, toutes leurs transactions sur le réseau pour cette raison blockchain décentralisée. [22]

Toutes les données stockées dans la blockchain publique sont sécurisées et les données ne peuvent pas être modifiées ou altérées après validation. [22]

Un exemple bien connu appliqué à la blockchain publique est Bitcoin et Ethereum. [22]

5.2. Privé blockchain

Seules les personnes autorisées sont autorisées à vérifier les transactions, elles ont leurs propres restrictions pour les utilisateurs déterminés par l'autorité responsable. [23]

La blockchain privée est utilisée dans les entreprises, les banques et autres que les données ne doivent être disponibles que pour des personnes spécifiques. [23]

6. Architecture du Blockchain

6.1 Bloc

Liste de toute les données de transaction dans DLT sur une certaine période de temps. Ces données comme suivants :

- **Numéro de version de bloc** : numéro de bloc dans la blockchain.
- **PreviousHash:** la valeur de hachage du bloc précède.
- **Hash**: la valeur de hachage du bloc contenant.
- **Nonce:** nombrealéatoireajouter au bloc pour modifier le hachage.
- **Timestamp:** le temps de création de bloc.
- **Data**: les données de bloc.

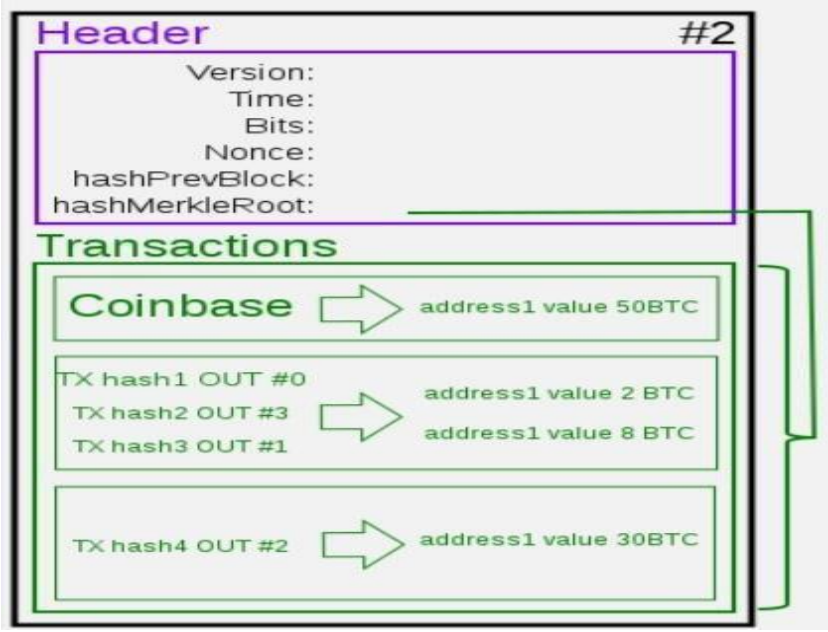


Figure12. Structure de bloc [24]

6.2 Chain

Fonction de hachage qui permet aux blocs d'être mathématiquement liés les uns aux autre. la forme correspondante montre comment les lier :

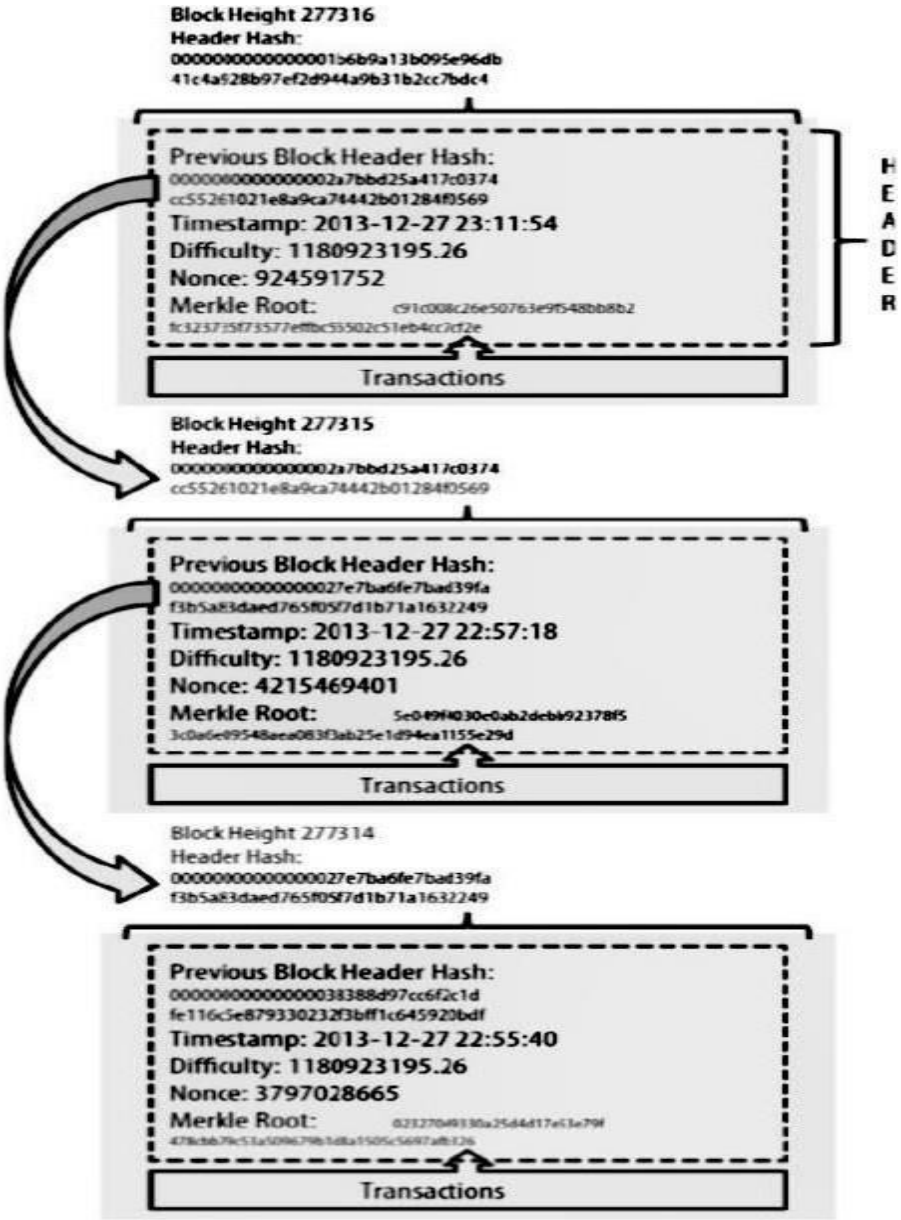


Figure 13 : Architecture de Blockchain. [25]

Le premier bloc est appelé Genesis bloc, car il n'a pas de données de transactions et pas de hach précèdent.

6.3 Réseaux

Cetteréseau se compose d'un nœud complet. Ce nœud en tant qu'ordinateur utilise l'algorithme pour sécuriser le réseau trouvé dans chaque nœud de données de transaction enregistrée dans blockchain. Ces nœuds sont situés partout dans le monde peut y participer, mais c'est couteux. [27]

7. Transaction du Blockchain

Un utilisateur de blockchain demande une transaction qui consiste à envoyées un cryptomonnaie ou des fichier …etc. cette transaction envoyée dans le réseau p2p via le nœud. Un réseauvalide la transaction à l'aide de ses algorithmes.

Si la transaction est correcte, elle est ajoutée au bloc dans le blockchain.

8. Implémentation du BlockChain

Étape 01 : Structure de blocs

Lestransactions sont enregistrerdans une structureappeléeblocs.Les blocs sont lié les uns aux autres pour créer le blockchain. Chaque bloc enregistre les transactions récentes, ainsi que d'autre élément tels que les temps de cette transaction et nombre de bloc, hash et le previous hash de bloc précèdent. Et il fait référence au bloc qui vient juste avant lui. Il contient la repose a un puzzle qui est le seul moyen de créer de nouveaux bloc.

BlockChain.java | SHA256.java | Block.java

```
package blockchain;
import java.util.Date;
public final class Block {
private String previousHash;
private String data;
private String Hash;
private final long Timetamp;
private final int index;
private int nonce;
public Block (int index, long Timetamp ,String previousHash, String data, int nonce){
    this.previousHash=previousHash;
    this.data=data;
    this.Timetamp=Timetamp;
    this.index=index;
    this.nonce=nonce;
    hashing();
}
    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;}
```

Figure14 : Structure de bloc en java

BlockChain.java | SHA256.java | Block.java

```
package blockchain;
import java.util.ArrayList;
import java.util.Date;

import java.util.List;
public class BlockChain {

    public static void main(String[] args) {
    List<Block> blockChainList=new ArrayList<>();

    //int difficulty=3;
    Block genisis_Block=new Block(0, new Date().getTime() ,null ,"Genisis Block");
    blockChainList.add(genisis_Block);

    System.out.println("-------------BlockChain----------------");
   blockChainList.forEach(System.out::println);
    }
}
```

Figure 15 :Création du Genisis bloc

Output - BlockChain (run)

```
run:
-------------BlockChain----------------
Block0 [
 Timetamp: Mon Jun 07 11:04:56 GMT+01:00 2021
 Hash: 6323e854ee9f8db5f50533046df1f87240b8a279d2d12012fe64611454f71b67
  previousHash: null
 data: Genisis Block ]
-----------------------------------
```

Figure16 : L'affichage de Genisis Bloc

Étape 02 : hash

Pour sécurité les données de blockchain,chaque bloc doit être haché. Utilise l'algorithme est la fonction de hachage SHA-256, cette fonction prend n'importe quelle taille de données et donne une chaine alphanumérique de taille fixe.

```
    public String hashing(){
  String dataToHash=Integer.toString(index)+previousHash+Long.toString(Timetamp)+data+Integer.toString(nonce);
  String valHash=SHA256.hashing(dataToHash);
 return this.Hash=valHash;

}
```

Figure17 : Fonction de hachage en java

Étape 03 : Ajouter des blocs

La première fois est crééele premier bloc,il est facile de créé un nouveau bloc à l'aide du premier hachage de bloc ou du hachage de bloc précèdent.

BlockChain.java | SHA256.java | Block.java

```
package blockchain;
import java.util.ArrayList;
import java.util.Date;

import java.util.List;
public class BlockChain {

    public static void main(String[] args) {
    List<Block> blockChainList=new ArrayList<>();

    //int difficulty=3;
    Block genisis_Block=new Block(0, new Date().getTime() ,null ,"Genisis Block", 895314);
    blockChainList.add(genisis_Block);
    Block Block1=new Block(1, new Date().getTime(), blockChainList.get(blockChainList.size()-1).getHash() ," Block1",
   blockChainList.add(Block1);

    Block Block2=new Block(2, new Date().getTime(), blockChainList.get(blockChainList.size()-1).getHash() ," Block2",
    blockChainList.add(Block2);

    Block Block3=new Block(3, new Date().getTime(), blockChainList.get(blockChainList.size()-1).getHash() ," Block3",
    blockChainList.add(Block3);
    System.out.println("---------------------------------");
    System.out.println("------------BlockChain----------------");
   blockChainList.forEach(System.out::println);
    System.out.println("---------------------------------");}}
```

Figure18 : Ajouter des blocs dans la blockchain

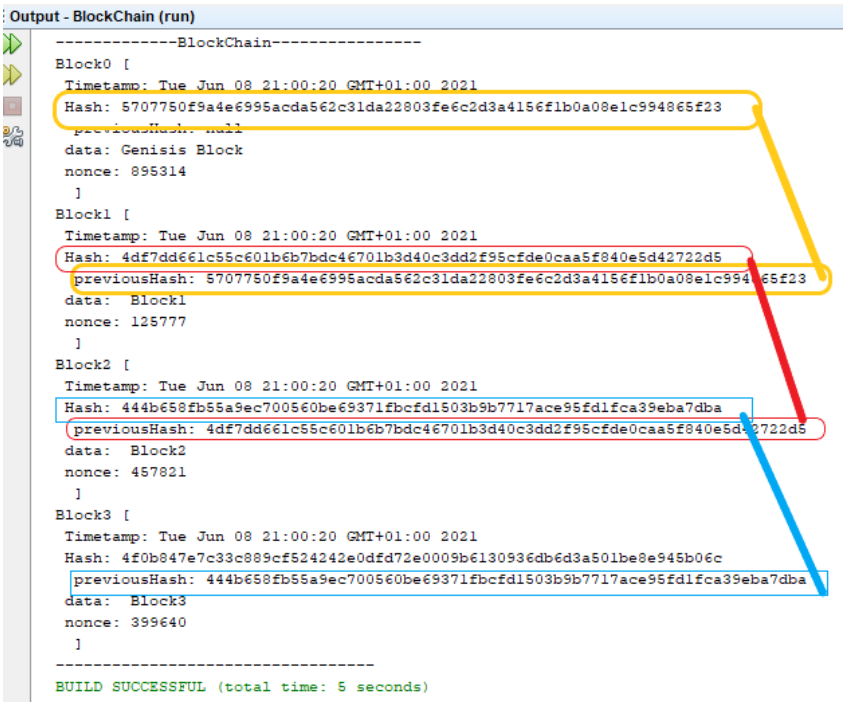


Figure 19 : Page du blockchain

9. La partie expérimentale

9.1 Preuve de travail

Dans cette partie, nous avons le première bloc (Genesis Block) dans le blockchain, puis ajouter le protocole de cryptage SHA-256 responsable du hachage de cryptage, puis nous avons ajouté la fonction d'ajout de bloc ou blocs à blockchain pour vérifier leur santé en ajoutant une fonction mineure qui vérifier à l'époque et hache chaque bloc et s'il le trouve correct l'ajoute à blockchain et si c'est faux le rejette.Comme ci-dessus :

Etape01 :création de première bloc dans la blockchain

Block.java | BlockChain.java

```
package blockchain;
import java.util.Date;
public final class Block {
private String previousHash;
private String data;
private String Hash;
private long Timetamp;
private int index;
private int nonce;
private int difficulty;

  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 int getNonce(){return nonce;}
public void setNonce(int nonce){this.nonce=nonce;}
public long getTimetamp(){return Timetamp;}
public void setTimetamp(long Timetamp){this.Timetamp=Timetamp;}
```

Block.java | BlockChain.java

```
    Block genesis_bloc(String data){
        this.previousHash=null;
        this.Timetamp=new Date().getTime();
        this.difficulty=4;
        this.data=data;
        this.index=1;
        this.nonce=14893;
        this.Hash=this.hashing();
        return this;
    }
```

Figure20 : Création de première bloc

Etape 02 :création les blocs suivants

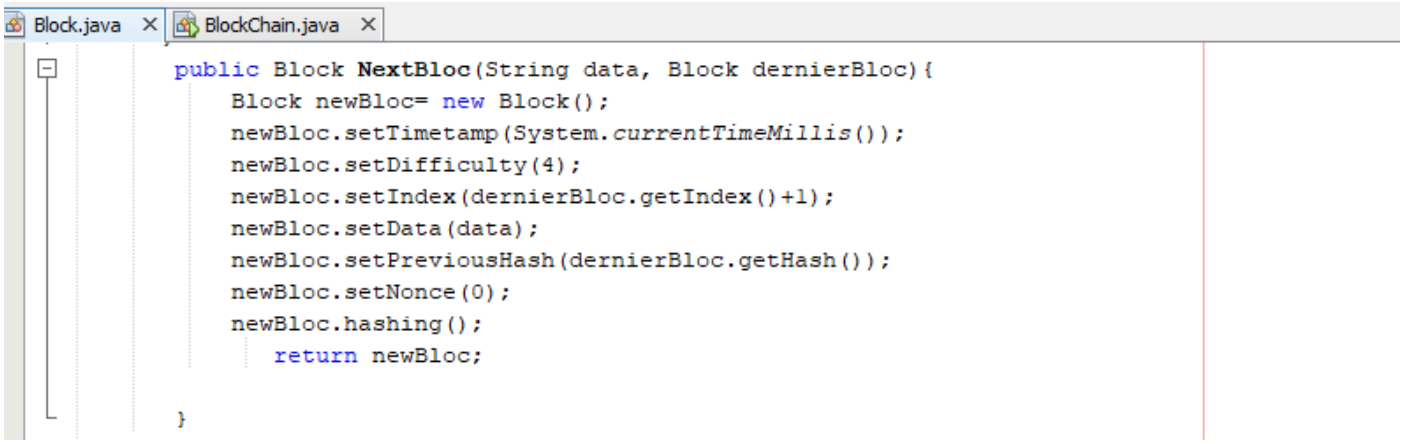


Figure21 : Création les blocs suivants

Etape 03 : hach de bloc

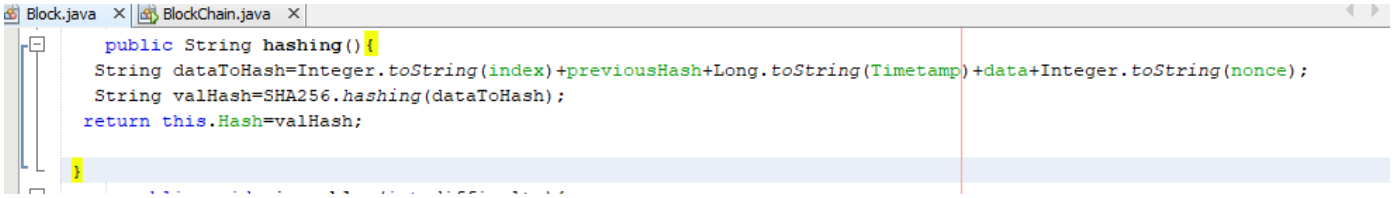


Figure22 : Fonction de hachage de bloc

Etape finale :l'affichage de résultat de test

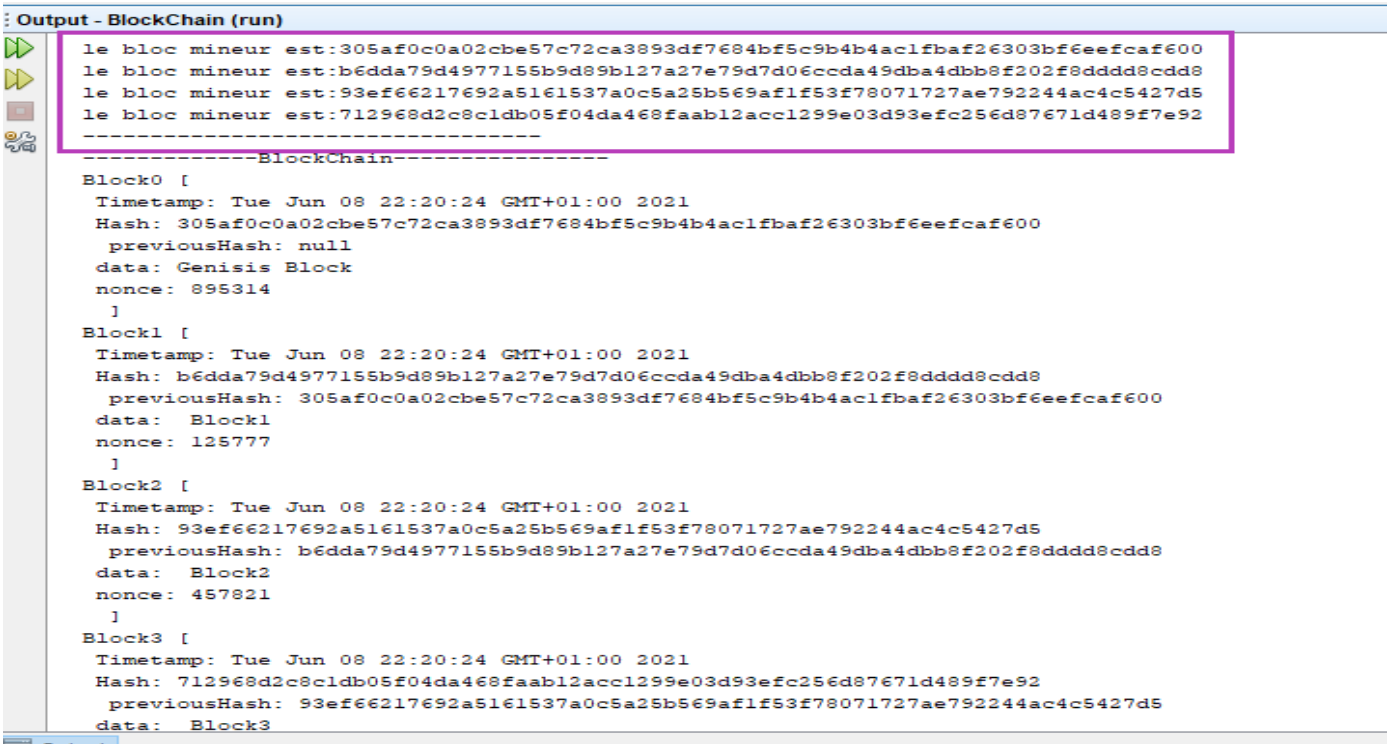


Figure23 : L'affichage de mineur de Blockchain

9.2 Preuve d'enjeu

Dans cette partie, on acréé la fonction d'ajout de bloc ou blocs à blockchain et ajouter le protocole de cryptage SHA-256 responsable du hachage de cryptage, puis ona ajouté une fonction validateur qui est tester asque previoushachégale le hach de bloc précédenteset s'il le trouve correct l'ajoute à blockchain et si c'est faux le rejette. Comme ci-dessus :

Etape01 : création des blocs

Bloc.java | Pos.java

```
package pos;
import java.io.UnsupportedEncodingException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Date;

public class Bloc {

private String previousHash;
private String data;
private String Hash;
private long Timetamp;
private int index;
private String validateur;
private String Signateure;

 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 getIndex(){return index;}
public void setIndex(int index){this.index=index;}
public long getTimetamp(){return Timetamp;}
public void setTimetamp(long Timetamp){this.Timetamp=Timetamp;}
```

Bloc.java | Pos.java

```
 Bloc genesis_bloc(String data){
    this.previousHash=null;
    this.Timetamp=new Date().getTime();
    this.data=data;
    this.index=1;
    this.Hash=this.hashing();
    this.validateur=validateur;
    return this;
}
public Bloc suivantBlocs(Bloc derniereBloc, String data){
    Bloc newBloc= new Bloc();
    newBloc.setTimetamp(System.currentTimeMillis());
    newBloc.index=derniereBloc.index+1;
    newBloc.previousHash=derniereBloc.Hash;
    newBloc.hashing();
    newBloc.validateur=validateur;
    return newBloc;

}
```

Figure24 : Création de blocs

Etape 02 : hach de blocs

Bloc.java | Pos.java

```
    public String hashing(){
  String dataToHash=Integer.toString(index)+previousHash+Long.toString(Timetamp)+data;
  String valHash=SHA256.hashing(dataToHash);
 return this.Hash=valHash;

}
```

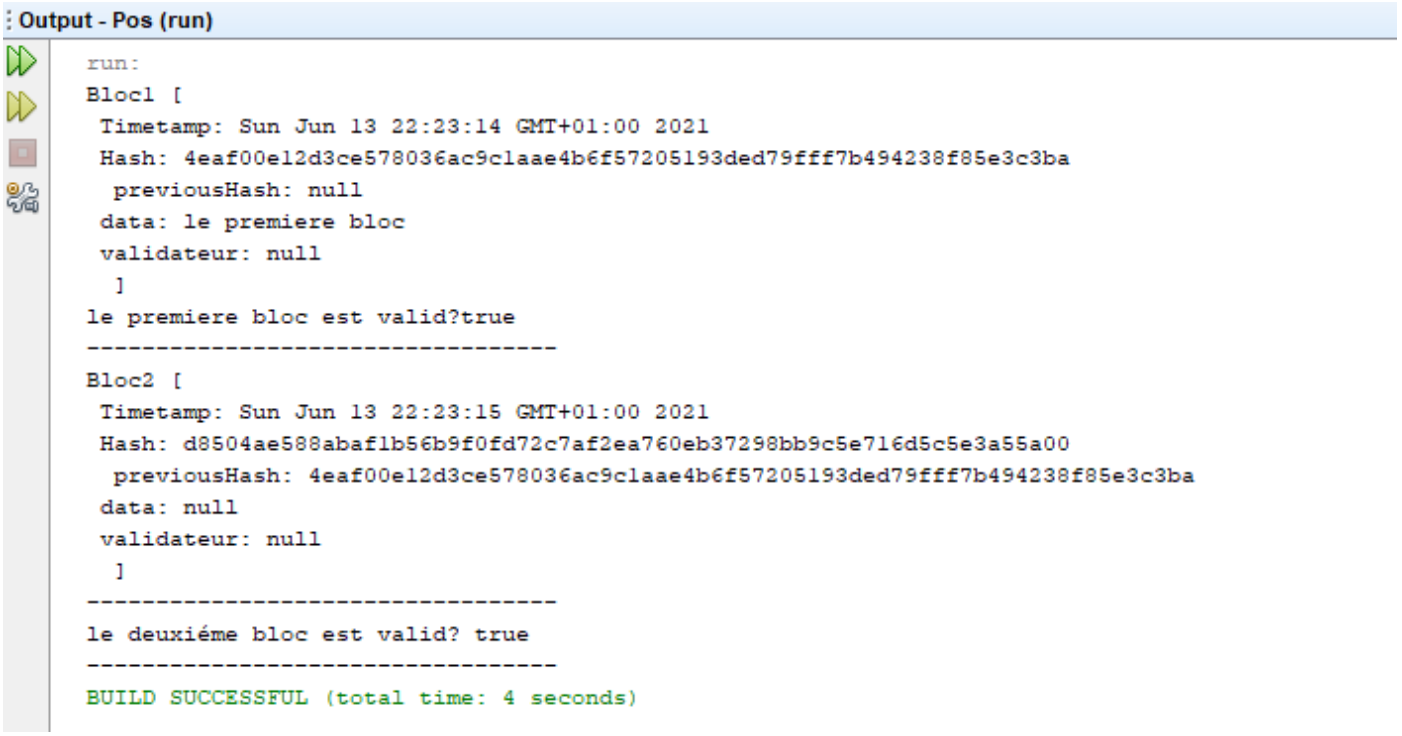
Figure25 : Hachage de blocs

Etape03 : Fonction de validation des blocs dans la class main

```
Bloc.java  Pos.java
    }

public static boolean validateur(List<Bloc> blockChainList) {
    boolean resultat=true;
     //dernier bloc est vide
    Bloc derBloc=null;
     for(int i=blockChainList.size()-1;i>=0;i--){
         if(derBloc==null){
            derBloc=blockChainList.get(i);

         }
         else{
            Bloc actBloc=blockChainList.get(i);
            if(derBloc.getPreviousHash() == null ? actBloc.getHash() != null : !derBloc.getPreviousHash().equals(actBloc.getHash())){
               resultat=false;
                 break;
             }
             //le dernier bloc c'est l'actuel bloc
             derBloc=actBloc;
         }
     }


    return resultat;
}
```

Figure26: Validation de bloc

Etape finale : affichage de test de POS



```
Output - Pos (run)
run:
Bloc1 [
 Timetamp: Sun Jun 13 22:23:14 GMT+01:00 2021
 Hash: 4eaf00e12d3ce578036ac9claae4b6f57205193ded79fff7b494238f85e3c3ba
  previousHash: null
 data: le premiere bloc
 validateur: null
  ]
le premiere bloc est valid?true
-----------------------------------
Bloc2 [
 Timetamp: Sun Jun 13 22:23:15 GMT+01:00 2021
 Hash: d8504ae588abaf1b56b9f0fd72c7af2ea760eb37298bb9c5e716d5c5e3a55a00
  previousHash: 4eaf00e12d3ce578036ac9claae4b6f57205193ded79fff7b494238f85e3c3ba
 data: null
 validateur: null
  ]
-----------------------------------
le deuxiéme bloc est valid? true
-----------------------------------
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figure27: L'affichage de test de POS

Bien que la façon dont cela fonctionne soit facile, elle est très difficile à implémenter. J'ai essayé autant que possible les algorithmes de consensus utilisés d'une manière simple qui ressemblait un peu à leur travail en fait.

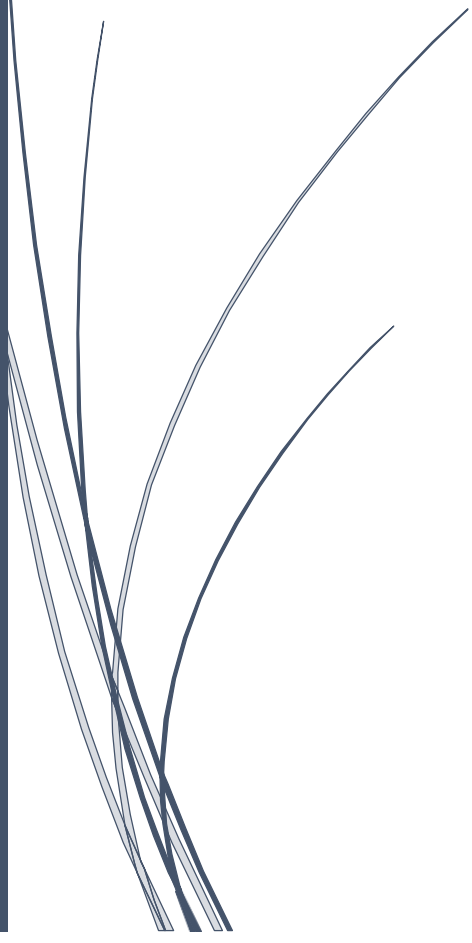
En expérimentant l'application d'algorithmes de Bitcoin et Ethereum en java en utilisant l'algorithmes de preuve de travail pour les deux et en appliquant l'algorithme SHA256 pour le Bitcoin , en l'algorithme SHA3 pour l'Ethereum tout cela appliquant dans la Blockchain publique, on consiste que l'Ethereum est plus rapide que Bitcoin en voir le temps d'exécution.

10. Conclusion

Dans ce chapitre, ona vu un aperçu de blockchain y compris la définition, ses caractéristiques, ses composants, différents types. Duplus, onadiscuté de la structure de données de blockchain, de son fonctionnement et de la manière dont elle sécurisé les transactions.

Ona parlé de la façon de créer une blockchain, ona vu les étapes et la fonction principale utilisée, la pow et la pos les étapes de son travail

Conclusion générale



La crypto-monnaies est ainsi nommée en raison de son utilisation de la cryptographie pour vérifier les transactions. Cela signifie que le jeton est responsable du stockage et de la transmission
des données de crypto-monnaies entre les portefeuilles et les registres publiques.

Bien que les crypto-monnaies utilisent la technologie blockchain pour être considérées comme largement sures, elles sont piratées.

Mêmes après avoir ajouté l'avantage de l'exploitation minière et preuve de travail, ce qui est considéré comme une grande raison de sa sécurité, mais en raison de certaines pénuries et de son utilisation de l'énergies de manières significative, ila été pénétré mais moins qu'auparavant.

.

REFERENCES BIBLIOGRAPHIES

[1] .https://www.bibliotheque.assnat.qc.ca/fr/cinq-lectures-pour-comprendre/4870-cinq-lectures-pour-comprendre-les-monnaies-numeriques
[2] .https://www.cafedelabourse.com/archive/article/bitcoins-monnaie-virtuelle-investir-crypto-monnaie
[3] .https://masterthecrypto.com/centralized-cryptocurrencies-coin-centralized
[4].cryptocurrencies_dbhtechnovation unite.un.org/techevents
[5] .https://academy.binance.com/en/articles/peer-to-peer-networks-explained
[6] .cryptocurrencies_dbhtechnovation unite.un.org/techevents
[7] .https://fr.advnfn.com/cryptomonnaies
[9] .https://tradeix.com/distributed-ledger-technology/
[10] .https://cryptorival.com/google-amp/algorithms
[11] . https://academy.bit2me.com/en/wallet-cryptcurrency-wallets/
[12] .https://academy.binance.com/fr/articles/crypto-wallet-types-explained
[13]. What Are Public Keys and Private Keys? https://www.ledger.com/academy/ blockchain/what-are-public-keys-and-private-keys/.
[14] .what is consensus algorithm? - Definition from WhatIS.com https://whatis.techarget.com/definition/cnsensus-algorithm
[15] . Andrew Tar. Proof-of-Work, Explained. https://cointelegraph.com/explained/ proof-of-work-explained/, January 2018. proof of work
[16] .https://www.coindesk.com/what-is-proof-of-work
[17] .https://www.bitpanda.com/academy/fr/lecons/algorithmes-de-consensus-la-proof-of-stake/
[18] . https://www.cityam.com/ethereum-2-0-staking-a-worthwhile-investment/
[19] .La Blockchain, qu'est-ce que c'est? Guide débutant https://cryptonaute.fr/blockchain/
[20] .https://www.researcharge.net/publication/33514496_CHAPITRE_3_Etat_de_l'art_de_la_Blockchain
[21] . Private, Public, and Consortium Blockchains - What's the Difference? https://www.binance.vision/blockchain/ private-public-and-consortium-blockchains-whats-the-difference/.
[22].https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparaison/
[23] .Tiana Laurence. The structure of blockchains. https://www.dummies.com/ personal-finance/the-structure-of-blockchains/. accessed February 7, 2020.
[24] .] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha. Analysis of Blockchain technology: pros, cons and SWOT. Cluster Comput, 22(S6):14743–14757, November 2019.
[25]. Bitcoin block structure.svg-Wikimedia Commons https://commons.wikimedia.org/wiki/File: Bitcoin_block_structure.svg
[26] .https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture