RÉPUBLIQUE DU SÉNÉGAL

Un peuple - un but - une foi

¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATON

¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤

L'excellence ma référence

¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤

Mention : Management des systèmes d'information Automatisé

Département : Économie Gestion

UFR : Science Économique Sociale

¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤

THÈME :

La crypto-monnaie dans l'espace UEMOA : économie, technologies et gouvernance

¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤¤

Présenté par :

Mame Diarra MBENGUE

Sous la direction de ;

Dr Kéba Aly GOUDIABY

Dr Edouard Ngor SARR

Sous la supervision de :

Prof Serigne DIOP

Membres du jury :

Pr Serigne DIOP (**Président**)

Dr Abel DIATTA (**Examinateur 1**)

Dr Amon Anike Deh (**Examinateur 2**)

Année universitaire : 2023–2024

Soutenu publiquement le 03/08/2024

Dédicace

Je dédie ce mémoire à mon défunt papa, dont l'amour, le soutien indéfectible et les sacrifices ont été les piliers de mon parcours académique. Son encouragement constant et son foi en moi ont été ma source d'inspiration. Merci pour tout papa tu nous manques.

Remerciements

Je remercie d'abord le bon **Dieu**, Allah le tout puissant qui m'a donné le courage d'affronter toutes les difficultés rencontrées durant les recherches ;

Je tiens à présenter mes remerciements avec une profonde reconnaissance et gratitude à mes encadrants **Dr Kéba Aly GOUDIABY** et **Dr Edouard Ngor SARR** d'avoir accepté de superviser et diriger ce travail. En plus des conseils avisés, de leur volonté d'aider et de leur investissement sans failles ;

Nos vifs remerciements s'adressent à Tout le corps professoral de l'Université Assane Seck de Ziguinchor pour la qualité de leur enseignement ;

Je tiens à remercier également les membres du jury qui ont accepté d'évaluer ce modeste travail ;

J'adresse également mes remerciements à mes parents particulièrement mon père.

Je remercie Un merci spécial à mon frère et mes sœurs qui m'ont soutenu durant tout mon cursus scolaire ;

J'adresse ma profonde gratitude à mes camarades de classe qui sont devenus une seconde famille Awa Ndiaye, Bigue Samb, Aida Diouf, Bassine Ba, Fatou mamour Sy, Oumy Salymata Touré, Abdoulaye Niang Faye merci pour la bonne ambiance partagée durant ces années d'études ;

J'adresse également ma profonde gratitude aux personnes que j'ai eu l'honneur de côtoyer au sein de l'université Assane Seck de Ziguinchor et qui ont fini par occuper une place assez importante dans mon cœur.

Résumé

La cryptomonnaie représente une monnaie numérique totalement décentralisée, dont la sécurité est basée sur la technologie blockchain pour la validation de transactions, le contrôle de création de nouvelles unités et le transfert d'actifs. L'intégration de la cryptomonnaie dans l'espace UEMOA représente une évolution majeure dans les domaines de l'économie, de la technologie, et de la gouvernance. Cependant, il faut reconnaitre que c'est une monnaie qui est sujette de plusieurs controverses, d'arnaques et d'attaques spéculatives. L'objectif de ce mémoire est de lever l'équivoque sur cette monnaie, en expliquant la technologie qui la gouverne ainsi que les stratégies optimales de gestion de celle-ci dans un contexte de l'UEMOA. Cette étude facilitera la mise en place d'une réglementation appropriée nécessaire pour une collaboration des gouvernements de la région, les institutions financières afin d'établir des normes claires et de promouvoir l'éducation des utilisateurs pour maximiser les avantages de la cryptomonnaie dans l'espace.

Mot clés : Cryptomonnaie, blockchain, technologie, gouvernance, UEMOA

Abstract

Cryptocurrency represents a completely decentralized digital currency whose security is based on blockchain technology for the validation of transactions, control of the creation of new units and the transfer of assets. The integration of cryptocurrency in the UEMOA space represents a major development in the fields of economy, technology, and governance. However, it must be recognized that it is a currency that is subject to several controversies, scams and speculative attacks. The objective of this thesis is to remove the ambiguity about this currency, by explaining the latest technology as well as the optimal management strategies for it in a WAEMU context. This study will facilitate the establishment of appropriate regulations necessary for a collaboration of governments in the region, financial institutions to establish clear standards and promote user education to maximize the benefits of cryptocurrency in the space.

Keywords: Cryptocurrency, blockchain, technology, governance, UEMOA

Sommaire

Liste des figures

Sigles et abréviations

- UEMOA : Union Economique et Monétaire Ouest Africaine
- BTC : Bitcoin
- LTC : Litecoin
- PPC : Peercoin
- XRP : Ripple
- NMC : Namecoin
- Doge : Dogecoin
- CEMAC : Communauté Economique et Monétaire de l'Afrique Centrale
- BCAO : Banque Centrale des Etats de l'Afrique de l'Ouest
- BEAC : Banque des Etats de L'Afrique Centrale
- POS : Power Of Stake
- POW : Power Of Work
- FCFA : Franc de la Communauté Financière Africaine
- EBC : Electronic CodeBook
- CBC : Cipher Block Chaining
- CFB : Cipher FeedBack
- OFB : Output FeedBack
- RSA : Rivest Shamir Adleman
- DSA : Digital Signature Algorithm
- MD5 : Message Digest algorithm 5
- SHA1 : Secure Hash Algorithm 1
- DPoS : Delegated Proof of Stake
- LPoS : Liquid Proof of Stake
- POA : Proof of Authority
- PoSe : Proof of Service
- PoHold : Proof of Hold
- PoC : Proof of Capacity
- PoB : Proof of Burn
- PoWeight : Proof of Weight
- PoI : Proof of Importance
- DBFT : Delegated Byzantin Fault Tolerance

- PBFT : Pratical Byzantin Fault Tolerance
- ECDSA : Elliptic Curve Digital Signature Algorithm
- ICO : Initial Coin Offerings
- STO : Security Token Offerings
- NFT : Non-Fungible Token

Introduction Générale

La monnaie définit l'ensemble des moyens de paiement c'est à dire l'ensemble des actifs acceptés partout, par tous et en tout temps, et qui permet d'acquérir un bien ou un service. Elle a beaucoup évolué dans le temps, en passant de la monnaie marchandise à une monnaie dématérialisée avec l'explosion des nouvelles technologies. Nous assistons de nos jours à la création de plusieurs cryptomonnaies dans le monde qui sont souvent utilisées comme une monnaie de spéculation. L'intégration fulgurante des marchés financiers et des économies ont fait naitre une interconnexion des marchés au niveau mondiale. Ces monnaies deviennent répandues même dans les économies en développement. Ainsi, la prise en commun de ces dernières s'est généralisée et reste une solution plus que plausible aux problèmes liés à plusieurs crises (sanitaire COVID 19, crise géopolitique). Elles peuvent être définies comment étant des monnaies numériques émises de pair en pair, sans nécessité de banque centrale, utilisables au moyen d'un réseau informatique décentralisé. Les crypto-monnaies reposent sur la technologie blockchain qui permet de stocker les données numériques de manière décentralisée et sécurisée. Cette technologie fonctionne sans organe centrale de contrôle. Sa nature décentralisée crée le nouveau concept d'une économie symbolique dans laquelle les revenus de la communauté peuvent être alloués aux producteurs de contenu et utilisateurs de services réels qui créent de la valeur.

Notre étude s'intéresse aux pays de l'Union Economique Ouest Africain (UEMOA) qui n'est pas en rade dans cette nouvelle mouvance mondiale qui interpelle chaque pays. Cependant, il faut reconnaitre que cette zone utilise officiellement une monnaie appelée franc CFA. En effet, A l'instar de la plupart des zones monétaires, la zone Franc a fait son apparition au cours de la période coloniale. Le franc CFA est une monnaie créée en 1945 pour les colonies françaises d'Afrique. Ainsi, la zone du franc CFA est composée de 14 pays de l'Afrique subsaharienne. Toutefois, il faut noter que cette monnaie connait des manquements souvent liés à la gestion monétaire et aux relations économiques entre les pays membres de l'UEMOA et la France à savoir : La dépendance économique des pays membres à l'égard de la France, la parité fixe avec l'euro qui peut entraver la flexibilité pour s'adapter aux réalités économiques et aux chocs extérieurs, la limitation en matière de politique monétaire, les pays de l'UEMOA font face à des contraintes budgétaires en raison des conditions imposées par le Franc CFA telle que le respect de critères de convergence.

D'après plusieurs études, la zone du franc connait beaucoup de difficultés sur plusieurs domaines à savoir la faiblesse des échanges intracommunautaires. Les échanges commerciaux entre les pays de l'UEMOA représentent 14% (base CNUCED) du total du commerce de la zone alors que celui de la zone euro est de 47% (Goudiaby et al.2023). Ils concluent le système CFA ne permet pas de corriger les écarts débiteurs des pays de l'UEMOA sur la période de 2005 à 2018. D'autres remettent en cause la capacité de cette monnaie à booster la croissance économique des pays de l'UEMOA (Nubukpo, 2007). En effet le PIB des pays de l'UEMOA est compris entre 10% et 15% ce qui est structurellement faible.

L'obligation des pays de la Zone franc à déposer 50 % de leurs réserves de change auprès du Trésor français. Cela signifie que la BCEAO et la BEAC doivent négliger leur besoin de financement pour développer leurs économies en construction, afin de se conformer aux politiques monétaires de la Banque centrale européenne. En effet en cas d'insuffisance des réserves de change, les banques centrales de la zone CFA doivent racheter aux entreprises privées et aux organismes toutes les devises. C'est après ce ratissage que le trésor français met les euros à la disposition des banques centrales de la zone CFA.

Les pays de l'UEMOA souffrent d'un problème de compétitivité-prix à l'export : avec des économies aussi faibles, avoir une monnaie arrimée à l'euro qui est une monnaie forte entraine une perte sur les exportations et une subvention sur les importations. Le sous financement des économies de l'UEMOA : les entreprises et les ménages souffrent de rationnement de crédit, en effet les banques centrales prêtent peu et le taux d'intérêt peut aller au-delà de 10% en général.

Dans ce contexte la création d'une cryptomonnaie dans l'espace UEMOA est-elle envisageable ?

L'objectif général de notre étude est de faire connaitre les crypto-monnaies dans l'espace UEMOA et de maitriser les aspects techniques de sa mise en œuvre.

Pour atteindre cet objectif général, nous élaborons quelques objectifs spécifiques à savoir :

- Présenter les aspects économiques, commerciaux et financiers de cette monnaie ;
- Expliquer la technologie qui est derrière la cryptomonnaie ;
- Elaborer une bonne stratégie de gouvernance de celle-ci.

Cette étude sur la crypto-monnaie est intéressante dans la mesure où elle permettra aux acteurs économiques de mieux connaitre le fonctionnement de cette monnaie afin de faire face aux différentes fraudes et arnaques autour de celle-ci. En effet elle discutera des avantages des cryptomonnaies dans le financement et le développement de ces pays.

Pour atteindre les objectifs nous avons formuler quelques hypothèses :

- La crypto-monnaie faciliterait les transactions financières ;
- La crypto-monnaie permettrait de donner une impulsion à la dynamique de financement dans l'espace UEMOA ;
- La crypto-monnaie faciliterait le transfert d'argent entre UEMOA et l'international.

Pour bien mener ce travail, notre démarche méthodologique repose sur une approche qualitative qui consiste à étudier des comportements, des besoins et de la perception des individus. Nous allons expliquer comment et pourquoi devrons nous adopter la crypto-monnaie dans l'espace UEMOA.

Ce mémoire se subdivise en trois parties. Nous présenterons en première partie l'aspect économique et l'évolution de la cryptomonnaie. Pour ce faire nous allons étudier les avantages et les inconvénients de cette dernière. La deuxième partie s'intéressera à la technologie blockchain qui sous-tend la cryptomonnaie en passant par la cryptographie, la chaine de blocs et l'activité de minage afin de terminer avec la dernière partie qui parlera de la gouvernance et de la gestion de la cryptomonnaie dans l'espace UEMOA.

Chapitre1 : Cadre théorique, évolution aspect économique de la crypto-monnaie

1. Cadre théorique de la crypto-monnaie

L'informatique est un système de traitement automatique des données numériques. Dans un système informatique, la cryptographie est un outil incontournable pour la protection des données considérées comme confidentielles. Elle assure la sécurité d'un système informatique en respectant les principes d'authenticité, d'intégrité, de confidentialité et de non-répudiation des données. Les cryptomonnaies utilisent la cryptographie dans la transaction des données pour instaurer la confiance et la responsabilité sans autorité centralisée. Une cryptomonnaie est appelée aussi cryptodevise ou monnaie cryptographique.

Selon Erwan J Jonchères (2016), les cryptomonnaies sont des monnaies numériques, qui se sont développées hors de tout contrôle étatique de manière décentralisé.

Jacques Favier, dans son ouvrage bitcoin la monnaie acéphale, Edition CNRS, 2017 définit le bitcoin premier cryptomonnaie créée en 2009 comme une technologie sans autorité centrale

Delahaye (2013) définit la cryptomonnaie comme une monnaie purement électronique qui n'a pas d'autorité centrale et que le fonctionnement du système est garanti par le réseau pair à pair. Le bitcoin étant la première cryptomonnaie crée depuis 2008, repose sur des protocoles cryptographiques. Pour Jean-Paul Delahaye le système bitcoin présente des forces et des faiblesses :

- La monnaie bitcoin repose sur un réseau pair à pair sans autorité centrale et complétement transparente.
- Les transactions de bitcoins sont rapides et irréversibles après un délai d'une heure ou moins personne ne peut agir sur vos bitcoins sans votre consentement.
- Le bitcoin est déflationniste avec le nombre limité de bitcoin qui est de vingt et un millions.
- Le bitcoin favorise le blanchissement d'argent et permet la fraude fiscale.
- Le nature déflationniste du bitcoin constitue un frein à la circulation de l'argent.

Enee Bussac dans son ouvrage : Bitcoin, ether & Cie, Munich, 24 juillet 2018 montre que la cryptomonnaie remplie les trois fonctions de la monnaie à savoir :

- La fonction réserve de valeur : un bitcoin peut être échangé ou vendu ;
- La fonction unité de compte : permettant le calcul économique, avec la cryptomonnaie on peut acheter certains produits ou services ;

- La fonction d'intermédiaire : les cryptomonnaies sont faites pour être échangées sur des places de marché intermédiaires.

Tiana Laurence dans ouvrage : La blockchain pour les nuls, Editions First, un département d'Edi8, 2018 propose une définition de la blockchain. Pour lui, la blockchain est « une structure de données qui permet de créer un livre numérique de données et de le partager dans un réseau d'individus indépendantes. » Ainsi pour l'auteur il existe différentes sortes de blockchain :

- Les blockchains publiques (permissionless blockchains) : « Les blockchains publiques, telles que Bitcoin, sont de grands réseaux distribués qui sont exécutés via un token ou jeton natif. Elles sont ouvertes à tous et à tous niveaux, et ont un code source ouvert que leur communauté maintient à jour »
- Les blockchains autorisées (permissioned blockchains) : » Les blockchains autorisées telles que Ripple, contrôlent les rôles que les individus peuvent jouer au sein du réseau. Elles sont toujours étendues et possèdent des systèmes distribués qui utilisent un token natif. Leur code source peut ou non être open source. »
- Les blockchains privées : « Les blockchains privées ont tendance à être plus petites et à ne pas utiliser de token. Leur accès est étroitement contrôlé. Ces types de blockchains sont favorisés par les consortiums qui ont des membres affiliés qui échangent des informations confidentielles. »

Jean Paul PONS et L'UTL34 dans leur ouvrage : Les cryptomonnaies impasse ou révolution ? déterminent les champs d'application de la blockchain à savoir :

- La blockchain comme support de base de données administratives ;
- La blockchain support d'un outil de gestion des droits d'auteur ;
- La blockchain pour authentifier des actes ;
- La blockchain pour faciliter le partage de biens et services ;
- La blockchain pour faciliter les transactions financières ;
- La blockchain pour la traçabilité des produits ;
- La blockchain pour faciliter l'exercice du droit de vote.

Jean Paul PONS détermine à travers son ouvrage les limitations de la cryptomonnaies dues à la technologie blockchain à savoir : la limitation du nombre de cryptomonnaies en circulation comme celui de bitcoin qui est de 21millions, des coûts croissants (bitcoin se comporte comme un système de paiement à couts marginaux : chaque unité coûte plus chère à produire et à

transférer que la précédente), des monnaies énergivores (une unique transaction de bitcoin consomme beaucoup d'énergie).

Gbémého Mathieu TRINNOU, dans son article Les cryptomonnaies : quels enjeux pour les banques centrales

L'auteur explique dans cet article l'influence des cryptomonnaies sur les banques centrales à adopter leurs propres cryptomonnaies.

1.1.Les différents types de cryptomonnaies

Les cryptomonnaies trouvent leurs origines dans les courants de pensée des libertariens et des cypherpunks qui cherchent à rétablir la séparation entre l'Etat et la monnaie et défendre le respect de la vie privée par la cryptographie. Nous assistons au développement de plusieurs cryptomonnaies :

1.1.1. Bitcoin (BTC)

Bitcoin est la première crypto-monnaie moderne crée en 2008 par Satoshi Nakamoto et mis en œuvre le 3 janvier 2009 où le début du minage a commencé. Toutefois il faut noter que bitcoin n'est pas la première monnaie numérique, avant sa création il existait plusieurs monnaies numériques comme B-Money et Bit Gold. En 2010 les premières transactions en bitcoin ont commencé avec l'achat de deux pizzas pour 10 000 bitcoins soient 600 millions de dollars. Bitcoin est souvent utilisé comme réserve de valeur et moyen d'échange [1]. En mars 2014, le marché des bitcoins a souffert de volatilité, limitant la capacité du bitcoin à constituer une réserve de valeur stable. Les commerçants acceptant le bitcoin utilisent d'autres devises comme unité de compte principale (HUSSAIN Ali,2022). Après la création du bitcoin des milliers de nouvelles crypto-monnaies ont vu le jour (le litecoin, Peercoin, le Ripple, Namecoin, le dogecoin Monero Nxt ou Ethereum). Ces crypto-monnaies sont appelées des alcoins. Ces dernières ont révolutionné le monde financier en créant une forme de monnaie stable qui n'est soutenue par aucun gouvernement et permet des transactions cryptées et anonymes. Les cryptomonnaies suppriment le recours à une banque centrale en autorisant des transactions directes entre pairs

Figure1 La cryptomonnaie bitcoin(BTC)

Source : https://www.phonandroid.com/ bitcoin-quest-ce-que-est-comment-marche-gagner-argent.html

1.1.2. Ethereum(ether)

Ethereum est la deuxième crypto-monnaie derrière le bitcoin utilisée pour trader sur des marchés et effectuer des transactions de NFT[1]. Elle est créée En 2015 par un chercheur en cryptomonnaie Vitalik Buterin, la blockchain Ethereum a été introduite par une équipe comprenant des contributeurs au projet Bitcoin. Ethereum a été présenté comme une plateforme open source permettant d'exécuter des applications décentralisées pour créer des contrats intelligents (smart contracts).

Figure2 La cryptomonnaie Ethereum(ether)

Source : https://www.wired.com/story/ ethereum-is-codings-new-wild-west/

1.1.3. Litecoin (LTC)

Le litecoin est un altcoin sous licence open source créée en 2011 par Charlie Lee. Il utilise le mécanisme proof of work et permet d'effectuer des paiements numériques décentralisés sans organe centrale. Il est basé sur le code source originelle du bitcoin permettant d'effectuer des paiements instantanés, avec des coûts proches de zéro à quiconque dans le monde. La crypto-monnaie litecoin offre beaucoup de liquidité que celle du bitcoin. En effet avec le litecoin, il est

[1] Un NFT (de l'anglais non-Fungible token) ou jeton non fongible (JNF) est un objet informatique (un jeton) suivi, stocké et authentifié grâce à un protocole de chaîne de blocs (blockchain), auquel est rattaché un identifiant numérique, ce qui le rend unique et non fongible.

plus facile d'acheter et de vendre sur le marché. Cela permet un retour sur investissement rapide pour les investisseurs. IL offre également une sécurité maximale grâce à un algorithme de hachage complexe, il n'est pas exposé au piratage. Selon la capitalisation boursière totale, le volume d'échange du Litecoin sur 24 heures est de 891,009,033 €, il est classé 16 parmi toutes les crypto-monnaies, avec une capitalisation boursière de 6,304,441,702 €. L'offre en circulation est de 72,177,696 Litecoin et l'offre maximale est de 84 millions de Litecoin [2].

Figure3 La cryptomonnaie Litecoin(LTC)

Source : https://www.cmcmarkets.com/fr-fr/ apprendre-a-trader-les-crypto-monnaies/qu'-est-ce-que-le-litecoin

1.1.4. Peercoin (PPC)

Le Peercoin est une crypto-monnaie peer to peer inspiré de bitcoin utilisant le système de preuve de travail(Proof-of-Work) et de preuve d'enjeu (Proof-of-Stake) pour la validation des blocs. La preuve de travail permet la distribution en renforçant la décentralisation du réseau alors que la preuve d'enjeu permet la sécurisation du réseau. La valeur de Peercoin n'a pas de limite stricte sur le nombre de pièces possibles comme celle de bitcoin et de litecoin, mais est conçu pour finalement contrôler la monnaie et autoréguler son taux d'inflation annuel de 1 % [3].

Figure4 La cryptographie Peercoin (PPC)

Source : *https://www.alamyimages.fr/* photo-image-peercoin-vecteur-de-piece-d-or-devise-crypto-realiste-de-l-argent-et-finances-signer-l-illustration-la-monnaie-numerique-peercoin-icone-compteur-fintech-blockchain-monde-celebre-la-cryptographie-146617333.html

1.1.5. Ripple ou XRP

Le Ripple ou XRP est une crypto-monnaie native du registre XRP (un registre distribué à code source ouvert, sans autorisation), qui a été développée en 2012, émise et partiellement gérée par la société américaine Ripple Labs. Le XRP est l'un des nombreux produits du bouquet de Ripple Labs, tous créés dans le but d'améliorer l'efficacité des paiements transfrontaliers, notamment dans le secteur bancaire. Le Ripple permet l'échange avec n'importe quelle monnaie et permet aussi de régler des transactions plus rapides et moins chères que les autres crypto-monnaies en 3 à 5 secondes. Le XRP permet de régler des transactions et d'améliorer les transactions transfrontalières dans le système bancaire.il joue un rôle de médiateur pour l'échange des devises. XRP utilise la technologie de registre de données distribuée, différente de la blockchain, qui assure le transfert de tokens (monnaie fiduciaire, crypto-monnaie, autres unités de valeur comme l'or). XRP utilise un protocole open source ce qui permet au système bancaire et non bancaire d'intégrer le protocole Ripple.

Figure5 La cryptomonnaie Ripple(XRP)

Source : https://autogo.tg/economie-finance/crypto-monnaie/ xrp-crypto-ne-manquez-pas-la-grosse-explosion-en-2023/5906/

1.1.6. Namecoin (NMC)

Namecoin est une crypto-monnaie créée en avril 2011 utilisant la technologie open source décentralisée qui améliore la sécurité, la résistance à la censure, la confidentialité et la vitesse de certains composants de l'infrastructure Internet, tels que le DNS et les identités. Namecoin partage certaines caractéristiques de base avec Bitcoin, son objectif principal est de fournir un système de nom de domaine décentralisé, cela le distingue nettement de Bitcoin qui est principalement axé sur les transactions financières décentralisées. Il utilise le consensus proof of work (preuve de travail) pour valider les transactions. Le nombre de tokens de Namecoin a été fixé à 21 millions comme bitcoin.

Figure6 La cryptomonnaie Namecoin(NMC)

Source : https://www.alamyimages.fr/ un-namecoin-cryptocurrency-physique-en-or-et-piece-en-argent-forme-sur-un-arriere-plan-sombre-studio-3d-render-image157384641.html

1.2.Blockchain

La blockchain ou chaine est un registre distribué de données qui permet de garder la trace des transactions de manière décentralisée, transparence et sécurisée [4]. La blockchain a été décrite pour la première fois par le cryptographe David chaum en 1982 dans sa thèse de doctorat. La technologie blockchain permet d'avoir une traçabilité des transactions, elle offre une sécurité et une transparence. Elle est caractérisée par sa nature décentralisée, son immutabilité et son consensus. Il existe plusieurs types de réseaux blockchain :

- La blockchain publique est la première technologie de blockchain. Elle supprime les problèmes liés à la centralisation, notamment une sécurité et une transparence moindres. Elle utilise la preuve de travail (PoW) et la preuve d'enjeu (PoS). Les Blockchains publiques pour échanger et miner des crypto-monnaies comme le Bitcoin, l'Ethereum et le Litecoin. La blockchain publique peut être utilisée par tout le monde. Les membres de la Blockchain ont des droits égaux pour lire, modifier et valider la Blockchain.
- Les blockchains privées sont décentralisées partiellement, L'autorité détermine qui peut être membre et quels droits ils ont dans le réseau. Leur accès est limité. Ripple, un réseau d'échange de devises numériques pour les entreprises, est un exemple de Blockchain privée.
- Blockchains hybrides regroupent les éléments des réseaux privés et publics. Les entreprises peuvent mettre en place des systèmes privés, basés sur les autorisations, parallèlement à un système public. De cette façon, elles contrôlent l'accès à des données spécifiques stockées dans la Blockchain tout en gardant le reste des données publiques. Ils utilisent des contrats intelligents pour permettre aux membres publics de vérifier si les transactions privées ont été effectuées. Par exemple, les Blockchains hybrides

peuvent accorder un accès public à la monnaie numérique tout en gardant la monnaie appartenant à la banque privée.

- Les blockchains de consortium sont gérées par des groupes d'organisations. Des organisations présélectionnées se partagent la responsabilité de la maintenance de la Blockchain et de la détermination des droits d'accès aux données. Les industries dans lesquelles de nombreuses organisations ont des objectifs communs et bénéficient d'une responsabilité partagée préfèrent souvent les réseaux Blockchain de consortium. Par exemple, le Global Shipping Business Network Consortium est un consortium Blockchain à but non lucratif qui vise à numériser le secteur du transport maritime et à accroître la collaboration entre les opérateurs de ce secteur.

2. Evolution de la crypto-monnaie

A l'échelle mondial, la capitalisation boursière totale des cryptomonnaies a atteint 1,2 milliard de dollars en 2023 [5]. Selon la capitalisation boursière totale des cryptomonnaies, il existe dans le monde 23823 cryptomonnaies avec une valeur marchande de 1.080.408.207.633 euro et une valeur marchande de 38.123.527.004 euro sur les 24h comme l'illustre le schéma 1. Dans le schéma 2 Avec ces 1.080.408.207.633 euro, environ 47% d'entre elles ne dominaient que par le bitcoin, suivis de l'éthereum, du Tether, du BNB de l'USD coin, de l'XRP, de Cardano, du Dogecoin, de Polygon, du Solona avec respectivement 19%, 7%, 4%, 2.53%, 2%, 1.16%, 0.94%, 0.77%, 0.76% environ. Les 14.92% restants de la capitalisation boursière sont dominés par le nombre restant de cryptomonnaies.

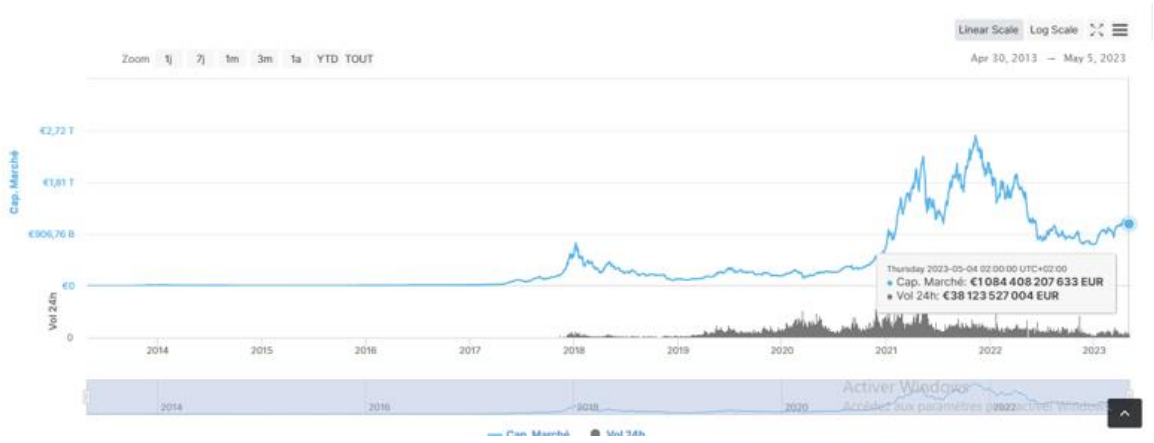
Le bitcoin est la cryptomonnaie la plus populaire, 29700 commerces accepteraient le bitcoin dans le monde ((HUSSAIN Ali,2022).). Lors de sa création en 2009, le prix du bitcoin était nul. La première transaction du bitcoin a eu lieu le 12 janvier 2009 lors que Nakamoto a envoyé 10bitcoins à Hal Finney. En Février 2011 le bitcoin a atteint pour la première fois la parité avec la principale devise internationale : 1bitcoin égale 1 Dollars. En 2013 il atteint un record de près de 1200 dollars [6]. Avec une forte spéculation, le fait de vouloir couvrir les baisses des marchés des actions, le risque inflationniste ainsi que le développement des actifs numériques ont attirés l'attention des économistes en 2020 sur les crypto-monnaies. [7]. En fin 2022 le bitcoin évolue aux alentours de 16500$[8].

En février 2021, il a atteint la barre des 50000$, puis il a augmenté avec un record de 67000$ le 19 octobre 2021.Après avoir été multipliée par quatre en 2020, la valeur d'un bitcoin a atteint

les 40 000 dollars en janvier 2021, et a poursuivi son ascension pour dépasser les 60 000 dollars en milieu d'année. Extrêmement volatile, son cours ne cesse cependant de fluctuer. En septembre 2021, la valeur de marché des crypto-monnaies a dépassé 20000milliards de dollars [9].

Dans le schéma 3 illustrant les informations générales sur les cryptomonnaies, nous constatons que le prix des crypto-monnaies a chuté à l'exception du Tether et de l'USD Coin. La chute de ces crypto-monnaies est dû à la loi de l'offre et de la demande. En effet avec 23823 cryptomonnaies dans le marché. Pour la plupart de ces crypto-monnaies, le prix est inférieur à 1 euro, tandis que pour celui du BNB Coin, il dépasse 100 euros, à l'exception du Bitcoin et de l'Ethereum qui est respectivement 26.182 et de 1.708 par crypto-monnaie. Cette baisse des prix de certaines de ces cryptomonnaies offre la possibilité aux investisseurs de réaliser des bénéfices de manière efficace, diversifier leur portefeuille de placements en s'investissant dans ces dernières. Avec cette baisse des prix, la demande sur le marché de bitcoin et l'Ethereum sera en baisse. La baisse des prix des cryptomonnaies est due à divers raison : la volatilité du cours des cryptomonnaies avec la fluctuation des prix, le système non autorisé et le comportement passif des investisseurs.

Figure7 La capitalisation boursière totale des cryptomonnaies de 2014 à 2023



Source : coinMarketcap, https://coinmarketcap.com/charts/ consulté le 05/05/2023

Figure8 Pourcentage de dominance totale de la capitalisation par des crypto-monnaies jusqu'au 30 avril 2023

Source : coinMarketcap, https://coinmarketcap.com/charts/ consulté le 05/05/2023

Figure9 Information sur les crypto-monnaies

#	Nom	Prix	1h %	% 24h	7d %	Cap. Marché	Volume (24 h)	Offre en Circulation	7 Derniers Jours
1	Bitcoin BTC	€26,182.17	-0.33%	+0.48%	-3.11%	€506,994,640,297	€17,260,580,718 659,545 BTC	19,364,118 BTC	
2	Ethereum ETH Acheter	€1,708.86	-0.20%	-0.43%	-2.70%	€205,705,107,370	€7,637,232,901 4,472,542 ETH	120,375,862 ETH	
3	Tether USDT	€0.9077	-0.19%	-0.69%	-1.55%	€74,417,200,869	€24,803,536,685 27,327,100,637 USDT	81,985,825,505 USDT	
4	BNB BNB Acheter	€294.60	-0.27%	-0.50%	-4.28%	€45,917,178,010	€509,574,983 1,730,896 BNB	155,861,985 BNB	
5	USD Coin USDC	€0.9073	-0.19%	-0.69%	-1.57%	€27,329,319,275	€3,347,549,155 3,689,870,089 USDC	30,120,340,501 USDC	
6	XRP XRP	€0.4159	+0.24%	+0.04%	-2.75%	€21,530,060,077	€794,688,130 1,911,162,021 XRP	51,768,283,547 XRP	
7	Cardano ADA	€0.3525	-0.43%	+0.56%	-7.75%	€12,274,940,419	€203,336,262 576,818,280 ADA	34,818,629,835 ADA	
8	Dogecoin DOGE	€0.07133	+0.05%	-0.03%	-3.66%	€9,929,219,208	€284,198,079 3,997,909,518 DOGE	139,207,936,384 DOGE	
9	Polygon MATIC	€0.8939	-0.19%	-1.43%	-4.71%	€8,267,929,925	€348,923,857 390,648,367 MATIC	9,249,469,069 MATIC	
10	Solana SOL	€19.75	-0.65%	+0.34%	-3.72%	€7,785,146,665	€341,797,612 17,310,567 SOL	394,124,769 SOL	

Source : coinMarketcap, https://coinmarketcap.com/charts/ consulté le 05/05/2023

2. Les avantages de la cryptomonnaie

Les crypto-monnaies sont d'une véritable révolution sur les marchés financiers avec l'utilisation de la technologie blockchain. En effet, investir dans les crypto-monnaies comporte de nombreux avantages pour ses millions d'utilisateurs. Comme avantages nous pouvons en citer cinq, à savoir :

2.1.Les crypto-monnaies et la plateforme Blockchain riment avec sécurité optimale

La technologie blockchain assure les transactions et les investissements. Etant un registre de stockage des données décentralisées qui suit chaque transaction entreprise par son moyen. La blockchain permet d'assurer :

- Le stockage des données décentralisées ;
- Le suivi des transactions et investissements réalisés ;
- L'assurance de visibilité (impossible d'effacer une opération une fois saisie) ;
- L'impossibilité de piratage avec le système de stockage décentralisé ;
- La sécurité des informations infaillible.

2.2.Un système financier avec plus de transparence :

Avec le système financier des banques traditionnelles, les transactions sont gérées par des intermédiaires tiers (lors d'une transaction il faut donner confiance à l'un de ces intermédiaires). Ainsi avec la technologie blockchain et les crypto-monnaies, les transactions et les investissements peuvent se faire sur les marchés financiers en toute sécurité sans l'intermédiaire des entremetteurs tiers (les institutions financières ou la banque centrale). Les transactions, le nom des comptes des utilisateurs, le montant des comptes sont accessibles au public car il n'y a pas l'intervention d'un organe central assurant la fiabilité. Cette transparence permet de suivre tous les flux monétaires du réseau.

2.3.La possibilité de faire des investissement 24h/24 et 7j/7 (disponibilité des crypto-monnaies) :

Les crypto-monnaies sont disponibles 24h/24, avec le minage des crypto-monnaies et l'enregistrement des transactions, le marché est toujours ouvert. On peut acheter, vendre ou échanger des crypto-monnaies sans l'ouverture des institutions et des places boursières. Avec cette disponibilité, elle permet aux investisseurs de générer des revenus hors des heures normales de travail.

2.4.La crypto-monnaie, un moyen pour palier l'inflation :

Les crypto-monnaies ne sont pas spécifiquement attachées à une seule devise ou à une seule économie. Le prix des crypto-monnaies est le reflet de la demande mondiale plutôt que de l'inflation nationale. Le nombre d'actifs des crypto-monnaies est plafonné (la plateforme Bitcoin possède un plafond global et celle de l'Ethereum un plafond annuel) donc la quantité disponible ne peut pas devenir incontrôlable, pas de risque d'inflation. Certains crypto-monnaies comme le bitcoin sont déflationnistes. Elles prennent petit à petit de la valeur. En effet, avec le bitcoin on peut échapper qu'un acteur dominant décide de faire fonctionner la planche à billets et prendre l'argent par l'inflation créée, aucune émission en dehors de celle inscrite dans le protocole (et qui est de plus en plus faible, au cours du temps) n'est possible. Le nombre de bitcoins émis est fixé et ne dépassera jamais 21 millions.

2.5.La diminution des frais lors d'un échange ou d'un achat d'actifs :

A la différence du système bancaire traditionnelle ou les frais de transaction sont élevés. Contrairement aux crypto-monnaies ou les transactions se font de pair en pair et ne nécessitent aucun intermédiaire comme les banques, les frais de transactions sont minimes voir nuls. Cette baisse des couts permet aux commerçants de développer leur commerce et leur entreprise en réduisant une partie des frais liés à ce développement. Ainsi la baisse des couts de transactions offerte par le système du bitcoin permet aux immigrants d'envoyer régulièrement de l'argent à leur famille. En effet les marges prises par les plateformes d'échange dans la zone UEMOA vont de 8% à 12% de la somme envoyée en moyenne ce qui est un lourd prix pour ses pays. Le système bitcoin propose des frais moins élevés oscillant entre 1% et 3% que les plateformes traditionnelles [10].

3. Les inconvénients et les risques de la crypto-monnaie :

3.1.La volatilité :

La volatilité qui est le principal risque des crypto-monnaies. En effet, les crypto-monnaies ne sont pas adossées à aucune devise physique. Le prix des crypto-monnaies est déterminé par la loi de l'offre et de la demande ce qui les rend volatiles. En effet, Le prix d'une crypto-monnaie peut connaitre soudainement une hausse avec des bénéfices associés pour les investisseurs puis retomber aussi à des taux très bas. Le marché des crypto-monnaies se développe sur la spéculation et sa petite taille, ce qui le rend vulnérable aux fluctuations de prix ce qui aura des répercussions sur la valeur des actifs. Par exemple le prix du bitcoin est passé de 19161dollars le 24 novembre 2020 à 17156 dollars le 27 novembre 2020. Trois jours après il a connu une

augmentation de 19860 dollars. En septembre 2020 il était environ 10000 dollars. Et il a chuté en dessous de 5000 dollars en mars 2020[11]. Cette volatilité entraine le risque de pertes plus élevées.

3.2.L'absence de contrôle centralisé :

Les crypto-monnaies échappent au contrôle des Etats et des établissements financiers. Elles ne possèdent ni cours officiel ni valeur nominale. En cas de perte d'unités de crypto-monnaie suite à une défaillance technique, de vol ou erreur humaine il y'aura aucune garantie légale de remboursement pour les investisseurs du fait de l'absence de régulation. Le fait qu'aucun contrôle centralisé ne soit opéré par une autorité centrale a pour conséquence que le cours de certains crypto-monnaies comme le Bitcoin est soumis à de fortes variations spéculatives.

3.3.Les arnaques et Le piratage informatique :

Une autre menace des crypto-monnaies est le manque de protection des utilisateurs en cas de vol ou de perte. Les crypto-monnaies sont stockées dans des fichiers puis échangées à l'aide de clés électroniques. En cas de perte de ses clés électroniques ou de suppressions de crypto-monnaies, il est impossible pour l'utilisateur de récupérer les crypto-monnaies mais aussi pour l'ensemble du réseau. Après une transaction il est impossible de l'annuler car les transactions sont irréversibles quel que soit les circonstances de son exécution. L'effondrement de la plateforme d'échange de bitcoins le plus important en volume, Mt. Gox qui a été piraté en février 2014 à hauteur de 750 000 bitcoins ce qui représentait 350 millions de dollars. Les retraits et les transactions ont été stoppés par le site évoquant un bug informatique en début févier. Par la suite la disparition du contenu du site a entrainé des pertes plus ou moins importantes aux utilisateurs [12].

Chapitre2 : Cadre pratique et technologies de la blockchain

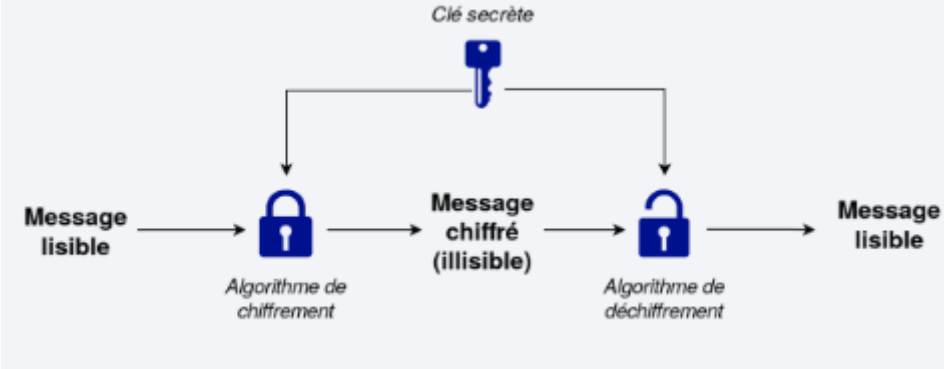
1.1. La cryptographie

La cryptographie a été créée depuis l'antiquité avec le chiffrement de césar. En effet La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Elle est la pratique des informations par l'utilisation d'algorithmes codés, de hachages et de signatures. Elle a quatre principes : la confidentialité, l'intégrité, l'authentification et la non-répudiation [13]. Ainsi il existe deux types de cryptographie : la cryptographie asymétrique (cryptographie à [2]clés publique) et la cryptographie symétrique (cryptographie à clé secrète[3]).

1.1.1. La cryptographie symétrique

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique) est la plus ancienne forme de chiffrement. Elle utilise les mêmes clés cryptographiques pour le chiffrement du texte en clair et le déchiffrement du texte chiffré [14]. Elle permet donc de chiffrer et de déchiffrer un contenu avec la même clé. En effet elle consiste à prendre un texte(message) et à le chiffrer à l'aide d'un algorithme mathématique (clé secrète). Ainsi le texte crypté est décrypté par la même clé secrète.

Figure10 La cryptographie symétrique



Source : https://stph.librecours.net /#show-home

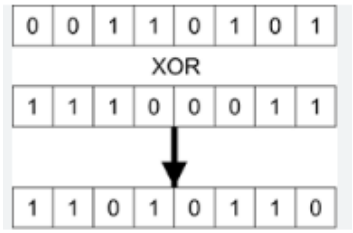
La cryptographie symétrique utilise deux types d'algorithme de chiffrement : le chiffrement de flux et le chiffrement par bloc.

[2] Une clé publique est un encodage rendu public dans le cadre d'un échange d'informations utilisant le principe de la cryptographie asymétrique.
[3] Une clés secrète est un encodage non-publié dans le cadre d'un échanges d'informations utilisant le principe de la cryptographie asymétrique. Elle est associée à une clés publique pour déclencher des algorithmes de chiffrement et déchiffrement de texte.

1.1.1.1. La cryptographie symétrique à chiffrement de flux

Le chiffrement de flux ou chiffrement par « fot » permet de chiffrer des données en longueur sans besoin de les découper, il agit en continu sur les données. Il fonctionne avec un générateur speudo-aleatoire avec lequel on opère un XOR un bit à la sortie du générateur et un bit provenant des données.

Figure11 Le chiffrement de flux



Source : https://www.di.ens.fr/~ferradi/ coursOTP.pdf

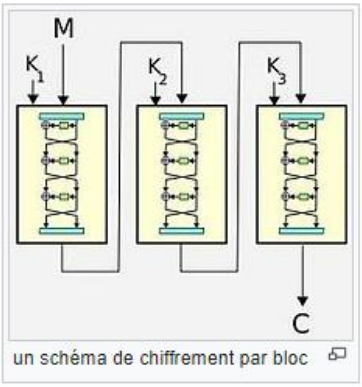
Les algorithmes utilisés sont :

- RC4(Cryptographe Rivest 4) : Le RC4 est un algorithme de chiffrement en continu conçu en 1987 par Ronald Rivest.
- RC5 (chiffre Rivest 5) et RC6(chiffre Rivest 6) : Le RC5 est un chiffrement par bloc, fonctionnant grâce à une clé dont la longueur varie entre de 40 à 2040 bits et RC6 est un algorithme de chiffrement de bloc dérivé de RC5.

1.1.1.2. La cryptographie symétrique à chiffrement par bloc

Le chiffrement par bloc est un chiffrement ou la taille du bloc est comprise entre 32 et 512 bits. Il transforme des données de taille fixe en bloc de données chiffrées de la même taille.

Figure12 Le chiffrement par bloc



Source : https://fr.wikipedia.org/wiki/ Chiffrement_par_bloc

Le chiffrement par bloc est composé de quatre modes :

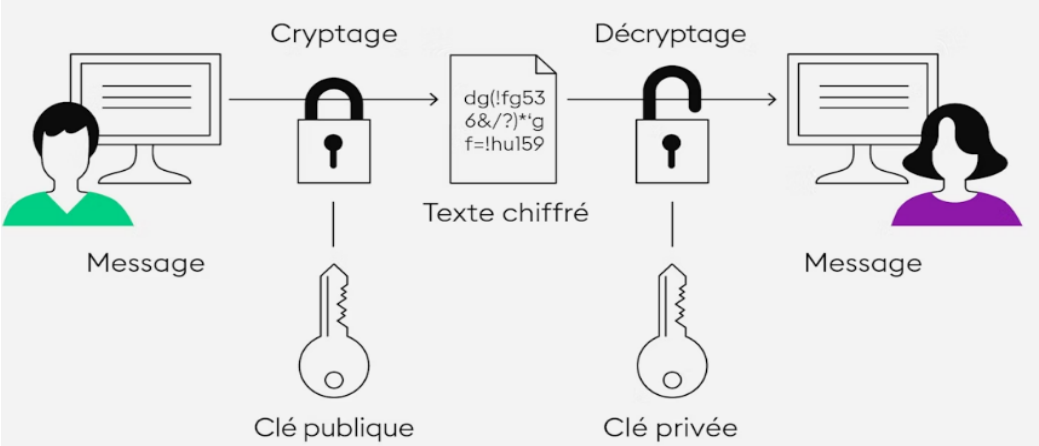
- Electronic CodeBook(EBC) : C'est un mode de fonctionnent simple avec un chiffrement par blocs qui est principalement utilisé avec le chiffrement à clé symétrique. Il s'agit d'un moyen simple de traiter une série de blocs de messages répertoriés séquentiellement [15].
- Cipher Block Chaining(CBC) : La chainage de blocs de chiffrement est un mode de fonctionnement pour un chiffrement par bloc, un mode dans lequel une séquence de bits est chiffrée à une seule unité, ou bloc, avec une clé de chiffrement appliquée à l'ensemble du bloc [16].
- Cipher FeedBack(CFB) : est un mode de chiffrement par bloc AES (Standard d'encryptage avancé) similaire au mode CBC en ce sens pour le chiffrement d'un bloc, Bi, le chiffrement du bloc précédent Ci-1 est requis [17].
- Output FeedBack(OFB) : Retour de sortie est un mode de chiffrement par bloc AES (Standard d'encryptage avancé) similaire au mode CFB. Ce qui diffère principalement de CFB, c'est que le mode OFB repose sur des blocs de texte en clair et de texte chiffré XOR avec des versions étendues du vecteur d'initialisation [18].

1.1.2. La cryptographie asymétrique (cryptographie à clé publique) :

La cryptographie à clé publique permet de transférer des données à l'aide de clé publique. En effet, une clé publique est un encodage rendu public dans le cadre d'un échange d'informations. Elle permet de convertir un message dans un format illisible. La clé publique est utilisée pour des opérations d'authentification, de chiffrement et de vérification de signature.

Une clé privée est un code sécurisé qui permet à son détenteur d'effectuer des transactions en cryptomonnaies et de prouver la propriété de ses avoirs [19]. Elle est un dispositif de sécurité qui utilise deux clés (clé publique et clé privée). C'est une amélioration de la cryptographie symétrique qui utilise une seule clé pour le chiffrement et le déchiffrement. La clé publique de la cryptographie asymétrique sert à chiffrer et la clé privée sert à déchiffrer.

Figure13 Cryptographie à clé asymétrique



Source : https://www.bitpanda.com/academy/fr/lecons/ qu'est-ce-que-le-chiffrement-asymétrique/

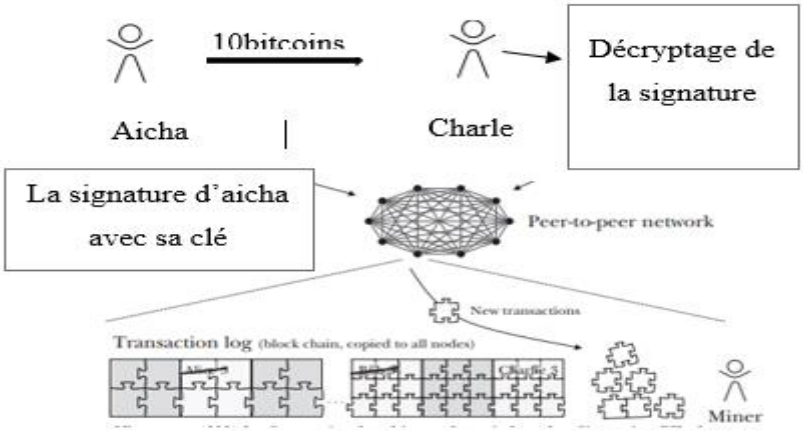
La cryptographie asymétrique utilise différents algorithmes

- RSA (chiffrement et signature) : Le RSA est une méthode de chiffrement souvent utilisée pour communiquer une clé de chiffrement symétrique, qui permet alors de poursuivre l'échange de façon confidentielle [20].
- DSA(signature) : L' algorithme de signature numérique (DSA) est un cryptosystème à clé publique et une norme fédérale de traitement de l'information pour les signatures numériques , basé sur le concept mathématique de l'exponentiation modulaire et le problème du logarithme discret [21].
- Protocole d'échange de clé Diffie-Hellman (échange de clé) : L'algorithme Diffie-Hellman est un algorithme d'échange de clés, utilisé notamment lors de l'ouverture d'une connexion à un site sécurisé via le protocole SSL/TLS (protocole pour serveur et navigateur) [22].
- Etc.

La technologie blockchain utilise la cryptographie asymétrique lors des transactions pour sécuriser l'identité des utilisateurs et assurer la non falsification des données. Elle est utilisée sur le réseau bitcoin et d'autres crypto-monnaies pour effectuer des transactions. Elle peut servir à chiffrer des informations et à signer des messages. En effet lors d'une transaction chaque participant du réseau génère une paire de clés (une clé publique et une clé privée), la clé publique est accessible à tous les participants de la transaction et la privée est connue que par son propriétaire.

Par exemple lors d'une transaction : aicha veut envoyer 10bitcoin à charle. Charle partage son adresse Bitcoin dérivée de sa clé publique. Pour cela Aicha crée une transaction indiquant qu'elle envoie 10 bitcoin à l'adresse de Charle. Elle signe cette transaction avec sa clé privée. Ainsi la transaction signée est diffusée sur le réseau Bitcoin. Les mineurs vérifient la validité de la signature et ajoutent la transaction à un bloc s'ils la considèrent comme valide. La transaction est confirmée, et les soldes des adresses d'Aicha et Charle sont mis à jour sur la blockchain. Il est important de souligner que la sécurité et la validité des transactions reposent sur l'utilisation de paires de clés cryptographiques (publique/privée) et de signatures numériques, assurant ainsi la propriété et l'authenticité des bitcoins transférés.

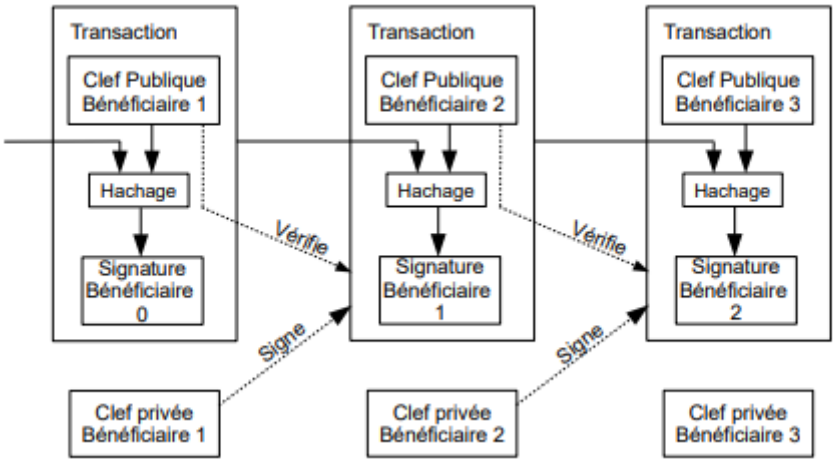
Figure14 Transaction de bitcoin



1.2. Les protocoles de transactions

Les protocoles sont des ensembles de règles de base qui définissent comment les transactions sont créées, vérifiées, validées et enregistrées dans la blockchain. Ils garantissent la sécurité, l'intégrité et la transparence des transactions.

Figure15 Protocole de transaction



Source : https://fr.wikipedia.org/wiki/ R%C3%A9seau_bitcoin

1.2.1. La signature électronique

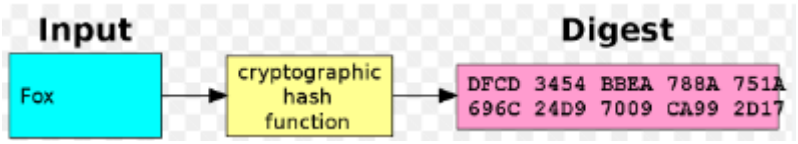
La signature par cryptographie à clé publique permet de chiffrer avec un mot de passe et de déchiffrer avec un autre différent. Elle permet d'assurer l'intégrité, l'authentification et la non répudiation. La signature numérique est effectuée avec la clé privée de l'expéditeur. La signature électronique garantit que la personne qui a initié la transaction possède la clé privée correspondante à la clé publique associée à l'adresse de départ. Cela sécurise la transaction contre la falsification, la garantissant ainsi dans un environnement décentralisé et transparent. La signature électronique utilise une fonction de hashing (hachage). En effet, les fonctions de hachage sont des fonctions mathématiques qui permettent de transformer une chaine de caractères de longueur indifférente à une autre de longueur fixe (256 bits, soit 64 caractères en notation hexadécimale complète pour SHA-256) [23]. Ce sont des fonctions à sens unique un même fichier donne toujours le même hash, il n'est pas possible d'obtenir le fichier de départ en utilisant le hash obtenu. Les fonctions de hachage sont utilisées dans la blockchain pour créer des adresses originales. Elles permettent de traiter et de condenser les données dans la blockchain. Les fonctions de hachages garantissent la sécurité des données en comparant les signatures. Elles sont importantes dans l'activité de minage pour la validation des transactions. Le hachage utilise différent algorithmes comme :

- Le Message-Digest algorithm 5 (MD5) : Le MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message) [24].

- Le Secure Hash Algorithm1(SHA1) : SHA-1 est un algorithme cryptographique qui prend une entrée et produit une valeur de hachage de 160 bits (20 octets). Cette valeur de hachage est connue sous le nom de résumé de message. Ce résumé de message est généralement rendu sous la forme d'un nombre hexadécimal de 40 chiffres. Il s'agit d'une norme fédérale américaine de traitement de l'information et a été conçue par la National Security Agency des États-Unis [25].
- Le Secure Hash Algorithm 256 (SHA-256) : Le SHA256 est l'une des fonctions de hachage qui succède le SHA-1 collectivement appelées SHA-2 et l'une des fonctions de hachage les plus puissantes disponibles. Il est utilisé par le système bitcoin.

Le hachage se caractérise par sa vitesse d'exécution, sa différenciation (deux entrées proches donnent deux empreintes différentes), son caractère unique et son imperméabilité face aux attaques.

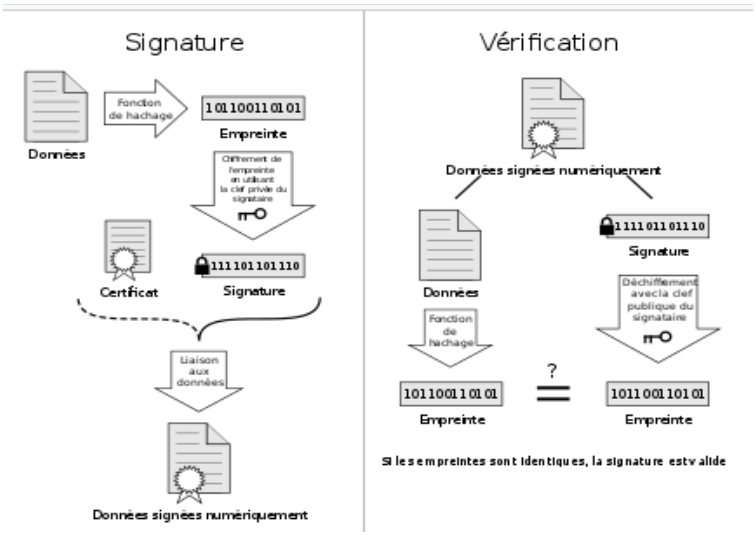
Figure16 Le hachage



Source : https://fr.wikipedia.org/wiki/ Fonction_de_hachage_cryptographique

Dans l'exemple précédent Aicha utilise la fonction de hachage (hashing) pour créer un résumé (digest) unique de la transaction. Ensuite, elle signe ce digest avec sa clé privée pour créer la signature numérique. Cela peut être fait à l'aide d'une fonction spécifique, souvent une fonction de signature numérique telle que ECDSA (Elliptic Curve Digital Signature Algorithm) dans le cas du Bitcoin. Aicha envoie la transaction signée (comprenant le digest et la signature) à Charle. IL reçoit la transaction signée et utilise la clé publique d'Aicha pour déchiffrer la signature numérique et obtenir un autre digest. Charle applique également la fonction de hachage à la transaction reçue pour générer un nouveau digest. Si le digest obtenu par le déchiffrement de la signature correspond au digest généré à partir de la transaction, cela signifie que la signature est authentique. Charle peut ainsi être sûr que la transaction provient bien d'Aicha, car seule la clé privée d'Aicha aurait pu produire une signature qui se déchiffre correctement avec sa clé publique.

Figure17 La signature électronique



Source : https://fr.wikipedia.org/wiki/ Signature_num%C3%A9rique

1.2.2. Les algorithmes de consensus blockchain

L'algorithme de consensus est le moyen par lequel la blockchain est susceptible de parvenir à un consensus. Cela s'applique notamment aux blockchains publiques puisqu'elles ne dépendent pas d'une autorité centrale pour la validation des transactions. Ce sont ce que l'on appelle des nœuds distribués qui sont régis par un algorithme de consensus qui vont devoir se mettre d'accord pour valider une transaction. L'algorithme de consensus a donc pour rôle de s'assurer que les règles ont bien été respectées [26].

Les algorithmes de consensus permettent aux nœuds du réseau de trouver un accord sur la validité et l'authenticité des blocs de transactions ou des données. Ils permettent d'assurer l'intégrité et la sécurité des systèmes. Il existe deux types algorithmes de consensus :

- Les algorithmes de consensus par vote : Les algorithmes de consensus basés sur le vote parviennent à un consensus sur les transactions (et parfois sur les décisions du réseau) en comptabilisant le nombre de votes exprimés par les nœuds sur un réseau de grand livre distribué [27].
- Les algorithmes de consensus par preuve : dans l'algorithme de consensus de preuve il y'a l'exigence des nœuds de rejoindre le réseau de vérification pour montrer qu'ils sont plus qualifiés que les autres pour effectuer le travail d'ajout.

1.2.2.1. Les algorithmes de consensus par preuve

Les algorithmes de consensus par preuve permettent de sélectionner les validateurs, ce sont des mécanismes de résistance aux attaques des 51 pourcents (attaque de double dépense par réorganisation de chaine).

1.2.2.1.1. La preuve de travail ou Proof of work(POW)

La preuve de travail est la plus célèbre des mécanismes de consensus présentée par Nakamoto en 2008 qui est à la base du bitcoin. Les preuves de travail (proof of work) : participent au tirage au sort pour l'ajout du cahier de compte et du gagnant des 25 bitcoins dans le système bitcoin, avec les preuves de travail les mineurs sont en concurrences les uns avec les autres. Les mineurs utilisent les preuves de travail pour confirmer les transactions et produire de nouveaux blocs sur la chaine. La probabilité d'être sélectionné pour créer un bloc dépend de la puissance de calcul. La preuve de travail consomme beaucoup d'énergie et nécessite une grande puissance de calcul, car elle repose sur une fonction de hachage. Bitcoin et Dogecoin utilisent La POW.

1.2.2.1.2. La preuve d'enjeu ou Proof of Stake(PoS)

La preuve d'enjeu (proof of Stake) est un mécanisme de consensus qui a été introduite en 2011 pour répondre aux problèmes de la preuve de travail. Elle a été créée pour réduire considérablement les dépenses énergétiques. La preuve d'enjeu est une alternative du POW. Contrairement à la preuve de travail qui pour valider les transactions utilise de la puissance informatique avec le minage physique, la preuve d'enjeu opte le minage virtuel qui est moins énergivore et plus écologique, les validateurs doivent staker des fonds. En effet pour sélectionner les validateurs, la preuve d'enjeu utilise un processus speudo-aleatoire. Les validateurs sont sélectionnés en recherchant les nœuds avec la valeur de hachage la plus basse et le stake le plus grand. Pour devenir validateur il faut posséder des tokens. Les validateurs reçoivent des frais de transaction en récompense. La preuve d'enjeu est résistante aux attaques des 51%, mais possède une vulnérabilité importante : le problème du « rien en jeu » qui rend les algorithmes de POS complexes. Il faut noter que la preuve d'enjeu et la preuve de travail sont les deux mécanismes de consensus les plus couramment utilisés dans le domaine des cryptomonnaies et des blockchains.

1.2.2.1.3. La preuve d'enjeu déléguée ou Delegated Proof of Stake (DPoS)

La preuve d'enjeu déléguée a été créée en 2014 par Daniel Larimer. Dans ce mécanisme, les transactions sont validées par un petit nombre d'individus. Ces individus sont appelés des délégués qui sont élus par des détenteurs du token natif. Les délégués sont élus par vote par les participants du réseau pour assurer le bon fonctionnement du réseau. Ce mécanisme de consensus réduit le nombre de nœuds d'un réseau blockchain. Ce mécanisme offre la tolérance aux pannes byzantines(BFT). La preuve d'enjeu déléguée n'est pas entièrement décentralisée par rapport à la preuve d'enjeu. Le système décentralisé compte 20 à 21 délégués pour vérifier les transactions. Dans la preuve d'enjeu déléguée les transactions sont validées avec rapidité grâce au nombre limité de nœuds validateurs.

1.2.2.1.4. La preuve d'enjeu liquide ou Liquid Proof of Stake (LPoS)

La preuve d'enjeu liquide est une variante de la preuve d'enjeu déléguée, c'est un système décentralisé qui se fait par l'intermédiaire de la blockchain. Elle permet aux utilisateurs de déléguer des jetons afin de gagner une récompense proportionnelle mis en jeu. Cela contribue à une importante création monétaire sans que les délégataires subissent de perte de pouvoir d'achat.

1.2.2.1.5. La preuve d'autorité ou Proof of Authority (POA)

La preuve d'autorité est un algorithme de consensus utilisé le plus souvent pour des blockchains privées. Elle permet de désigner des nœuds du réseau comme validateurs, ces nœuds ayant pour rôle de déterminer l'état du registre pour l'ensemble du réseau. La preuve d'autorité est principalement utilisée comme une alternative à la preuve de travail ou à la preuve d'enjeu. Elle permet d'augmenter significativement la vitesse de validation des transactions, au détriment cependant de la décentralisation de la blockchain. Les blocs et les transactions sont validés par des comptes approuvés à l'avance. Ici c'est l'identité du validateur et sa réputation qui sont mises en jeu plutôt que la puissance de calcul pour devenir validateurs. La preuve d'autorité est entièrement utilisée pour le système centralisé. Elle est principalement utilisée dans les réseaux privés.

1.2.2.1.6. La preuve de service ou Proof of Service (PoSe)

La preuve de service est un modèle de preuve d'enjeu qui, outre la possession de tokens, demande au nœud du réseau intéressé de fournir un service défini par le protocole, comme le

mélange de tokens ou le maintien d'une infrastructure supplémentaire. Les nœuds chargés de ce service sont appelés les masternodes. Cette méthode est généralement couplée à une autre méthode de base : par exemple, Dash fonctionne grâce au minage (preuve de travail), mais les masternodes interviennent pour garantir les transactions instantanées et pour empêcher les attaques des 51% (ChainLocks) [28].

1.2.2.1.7. La preuve d'histoire ou Proof of History (PoH)

La preuve d'histoire est un algorithme de consensus utilisé par Solona. Elle repose sur un concept mathématique appelé Verifiable Delay Function. Le concept de Proof of History consiste à prouver qu'un message a eu lieu avant ou après un événement connu, plutôt que de s'appuyer sur un horodatage. Cela ressemble à la façon dont la photo d'un otage tenant la dernière édition d'un journal prouve que l'otage était vivant après la publication de ce journal particulier. Solana utilise l'algorithme minier SHA256 de Bitcoin auquel s'ajoute une fonction de retardement vérifiable pour créer un enregistrement historique des événements sur la blockchain [29].

1.2.2.1.8. La preuve de conservation ou Proof of Hold (PoHold)

L'algorithme de consensus Proof of Hold (PoH) ou preuve de conservation est très proche du Stake. La seule réelle différence entre ces deux consensus est que la probabilité pour un nœud d'être sélectionné dépend de l'âge de la cryptomonnaie. Pour parvenir à la sélection, le calcul est le suivant : multiplication entre valeur d'un UTXO et du temps durant lequel la cryptomonnaie n'a pas été déplacée. Le concept de Proof of Hold (PoH) est utilisé dans le projet Peercoin qui utilise également le Proof of Work [30].

1.2.2.1.9. La preuve de capacité ou Proof of Capacity(PoC)

L'algorithme de consensus Proof of Capacity / Proof of Space (PoC) ou preuve de capacité est une alternative au PoW. Ce mécanisme de consensus repose sur la capacité de stockage des participants. Les mineurs allouent de l'espace disque pour résoudre des énigmes complexes et gagner la possibilité de créer un bloc. Son but est également de réduire la consommation énergétique du cryptomonnaie. C'est en utilisant l'espace vide sur les disques durs des nœuds du réseau blockchain que le Proof of Capacity (PoC) fonctionne. En effet, cet espace vide va être utilisé pour stocker et donc miner de la cryptomonnaie.

1.2.2.1.10. La preuve de brulure ou Proof of Burn (PoB)

Le processus de Burn (destruction) de la cryptomonnaie consiste donc à envoyer de la cryptomonnaie à une adresse publique et vérifiable. Ces adresses dites d'ingurgitation, sont générées de manière totalement aléatoire et sans qu'aucune clé privée ne soit récupérable. Une fois les coins déposés sur ces adresses, ils seront perdus à tout jamais, ceci dans le but de réduire l'offre en circulation et d'augmenter la valeur des coins. De cette façon, plus un nœud brûlera de tokens, plus il aura de chance d'être sélectionné pour valider un bloc [31].

1.2.2.1.11. La preuve de poids ou Proof of Weight (PoWeight)

La preuve de poids (Proof of Weight) est une vaste classification d'algorithmes de consensus basés sur le modèle de consensus d'Algorand. L'idée générale est que, en PoS (Proof of Stake), votre pourcentage de jetons détenus sur le réseau représente votre probabilité de découvrir le bloc suivant, dans un système PoWeight, une autre valeur relativement pondérée est utilisée. Certaines de ses implémentations sont la Preuve de réputation (Proof of Reputation) et la Preuve d'espace (Proof of Space) [32]. La preuve de poids est un consensus hautement personnalisable et évolutif qui consomme peu d'énergie.

1.2.2.1.12. La preuve d'importance, ou Proof of Importance(PoI)

Le consensus de la preuve d'importance est une version lourdement modifiée de la preuve d'enjeu, avec des mécanismes différents qui prennent en compte une variété de critères. En effet, le principe est le même : la capacité de validation des blocs par un nœud dépend de la quantité de tokens possédée. Mais il y a une spécificité : au lieu de simplement compter ceux présents sur l'adresse, le mécanisme de la preuve d'importance ne prend en compte que les tokens qui ont été présents sur l'adresse un certain temps [33].

1.2.2.2. Les algorithmes de consensus par vote

Les algorithmes de consensus par vote sont utilisés dans les systèmes distribués pour parvenir à un accord sur une décision en faisant voter les différents nœuds participants. Ces algorithmes visent à synchroniser les états des nœuds en permettant à la majorité de prendre une décision qui est ensuite acceptée par tous les participants. Ils sont composés par le consensus byzantin basé sur la tolérance aux pannes et le consensus byzantin basé sur la tolérance aux pannes en cas de nœuds écrasés ou subvertis.

1.2.2.2.1. Le consensus byzantin basé sur la tolérance aux pannes

La tolérance aux pannes byzantine est la capacité d'un système informatique distribué à résister aux défauts byzantins. Ces défauts peuvent être : échec du consensus, échec de validation, échec de vérification des données, échec du protocole de réponse face aux situations du réseau. Cette tolérance est liée à la capacité que le réseau, dans son ensemble, peut créer un mécanisme de consentement [34].

1.2.2.2.2. La tolérance aux pannes byzantines déléguées ou byzantine Delegated byzantine Fault Tolerance (DBFT)

La tolérance de panne byzantine déléguée est un algorithme sophistiqué destiné à faciliter le consensus sur une blockchain. Bien qu'il ne soit pas encore couramment utilisé, il représente une alternative à une preuve d'enjeu, une preuve d'importance et des méthodes de travail plus simples. L'histoire de cet algorithme théorique est fascinante, il est censé aborder un problème particulier de la théorie des jeux de la vieille école appelé le problème des généraux byzantins. Dans ce scénario, plusieurs généraux élaborent un plan pour attaquer une ville. Un consensus doit être atteint, car rien de moins qu'un consensus conduit à des échecs de bataille significatifs. Cependant, il existe des difficultés de communication et une préoccupation supplémentaire : dans le problème des généraux byzantins, les planificateurs doivent rechercher des acteurs traîtres individuels des acteurs qui peuvent même ne pas rendre la même décision à toutes les parties concernées. Dans le monde de la blockchain, cela s'explique par le fait que, si certains opérateurs de nœuds sont des professionnels, d'autres sont des amateurs disposant d'une vision moins sophistiquée des marchés, de la théorie des jeux et de tout le reste. On ne peut pas compter sur eux. C'est donc le problème complexe que l'administration de la Tolérance aux pannes byzantines déléguées aborde. Afin de gérer cette incertitude, la Délégation de pannes byzantines déléguées utilise une règle des deux tiers et d'autres éléments pour s'assurer que le consensus est atteint même avec beaucoup d'inconnues [35].

1.2.2.2.3. La tolérance aux pannes byzantines pratiques ou Pratical Byzantin Fault Tolerance (PBFT)

La tolérance aux pannes byzantines pratique est utilisée pour désigner un protocole très populaire qui est utilisé sur une blockchain ayant un réseau distribué dans l'objectif d'atteindre un consensus suffisant malgré un dysfonctionnement sur le réseau. Ce protocole est utilisé lorsqu'un ou plusieurs nœuds d'ordinateurs au sein d'une blockchain peuvent subir un dysfonctionnement et ce protocole agit en réduisant l'utilité d'un de ces nœuds sur

la blockchain. C'est un protocole qui peut être utilisé sur de nombreuses blockchains et peut permettre d'effectuer des milliers de transactions par seconde, dans l'objectif d'assurer le fonctionnement d'une blockchain [36].

1.3. La chaine de blocs/ blockchain

La chaine de blocs est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. La chaîne de blocs est un registre numérique dans lequel sont inscrites les opérations effectuées entre diverses parties au sein d'un réseau. Il s'agit d'un registre distribué poste à poste basé sur Internet, qui contient l'ensemble des opérations effectuées depuis sa création [37]. Le premier bloc a été créé en 2009 par Satoshi Nakamoto.

1.3.1. Structure d'un bloc

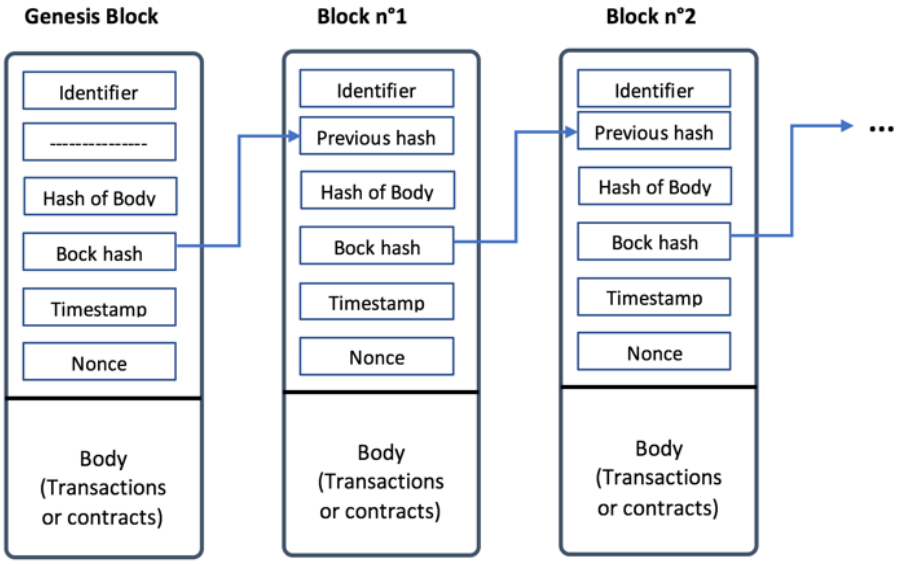
Un bloc est composé d'un entête et des données.

- L'entête est composé du hachage du bloc précédent, de l'horodatage, du nonce, de la racine de l'arborescence de Merkle.
  - **Le hachage du bloc précédent :** Le hachage transforme un input de données aléatoires en une chaine d'octets de longueur et de structure fixe. Il facilite l'identification de la transaction sur la blockchain. Les données des blocs sont liées les uns des autres grâce au hachage et l'intégration des données d'un bloc au bloc suivant.
  - **L'horodatage :** L'horodatage est un petit élément de données stocké dans chaque bloc en tant que série unique et dont la fonction principale est de déterminer le moment exact où le bloc a été extrait et validé par le réseau blockchain. Il permet de construire un lien cryptographique entre l'empreinte numérique d'une donnée et un bloc de la blockchain qui est vérifiable en toute circonstance à posteriori [38].
  - **Nonce :** En cryptographie, un nonce est un nombre arbitraire destiné à être utilisé une seule fois. Il s'agit souvent d'un nombre aléatoire ou speudo-aleatoire conçu pour garantir la confidentialité des communications et se protéger contre les attaques par relecture [39].
  - **La racine de l'arborescence de Merkle :** Un arbre de Merkle est une structure de données utilisée dans la technologie blockchain pour vérifier et valider efficacement les données contenues dans les ensembles de données volumineux. Le principe d'un

arbre de hachage est de pouvoir vérifier l'intégrité d'un ensemble de données sans les avoir nécessairement toutes au moment de la vérification [40].

- Les données : ce sont les informations sur les transactions.

Figure18 Structure d'un bloc



Source : https://blog.eleven-labs.com/fr/ bases-blockchain/

1.3.2. Les nœuds

Dans la chaine de blocs, les participants qui utilisent la base de données partagée sont appelés des nœuds. Ce sont des appareils informatiques qui fournissent de la puissance de calcul. Un nœud permet de vérifier si les informations d'un bloc sont valides et correctes et de les stocker. Il existe trois catégories de nœuds :

- **Les nœuds de diffusion :** Ils n'envoient que des informations de transactions et stockent une petite quantité d'informations de la blockchain ;
- **Les nœuds complets :** Ils stockent l'intégralité des informations de la blockchain, vérifient la cohérence des données et émettent des transactions ;
- **Les nœuds de minages :** Ils sont encore appelés des mineurs qui diffusent les transactions. Les participants peuvent être des particuliers ou des entreprises.

Chaque participant conserve une copie identique du registre, dans lequel chaque écriture correspond à une opération (échange d'une valeur) entre les participants. En réalité, de nombreux types de chaînes de blocs différents sont développés et mis à l'essai, mais la plupart

suivent grosso modo ce cadre et ce mode de fonctionnement. Lorsqu'un participant veut envoyer une valeur à un autre participant, tous les autres nœuds du réseau les uns avec les autres selon un mécanisme prédéterminé afin de vérifier si la nouvelle opération est valide. Une fois l'opération acceptée par le réseau, toutes les copies du registre sont mises à jour. Habituellement, plusieurs opérations sont regroupées pour former un « bloc » qui est ajouté au registre. Chaque bloc contient des informations qui renvoient aux blocs précédents, et ainsi tous les blocs de la chaîne sont liés dans les copies identiques distribuées. Les nœuds participants peuvent ajouter de nouvelles opérations horodatées, mais il leur est impossible de supprimer ou de modifier les écritures une fois qu'elles ont été validées et acceptées par le réseau. Si un nœud modifiait un bloc précédent, son registre ne pourrait plus être mis à jour comme le reste du réseau et le nœud serait exclu de la chaîne de blocs. Une chaîne de blocs qui fonctionne comme il se doit est donc inaltérable, même s'il n'y a pas d'administrateur central. La chaine de blocs assure la rapidité des transactions et la sécurité du système. Elle réduit les couts de transactions [41].

1.4. L'activité de minage

L'activité de minage ou mining consiste à une résolution de formules mathématiques complexes pour la validation des transactions. Cette activité nécessite une forte utilisation du matériel informatique. Le minage consiste à trouver un bloc à partir d'un algorithme. Cet algorithme est exécuté plusieurs milliards de fois par seconde pendant plusieurs minutes avant de trouver un bloc. Lorsqu'on l'exécute, le SHA-256 produit une chaîne de caractères plus ou moins aléatoires que l'on appelle un hash. Trouver un bloc revient à trouver le hash qui commence par un certain nombre de zéros. Pour ce faire, les mineurs exécutent l'algorithme en y ajoutant un incrément, qu'ils augmentent à chaque tour, jusqu'à trouver le bon hash. Une nouvelle chaine de bloc est ajoutée lorsque tous les nœuds du réseau vérifient le hash trouvé.

Dans le système bitcoin les mineurs sont rémunérés de 25 bitcoins en participant à la création de la monnaie. Cette création de monnaie est transparente, puisque chacun peut savoir combien de nouveaux bitcoins ont été créés en fonction des blocs validés et assure le bon fonctionnement du réseau. Grâce à ce système, le réseau Bitcoin peut donc se passer d'une entité qui jouerait le rôle d'une Banque centrale. Un point essentiel à noter est que la récompense ou rémunération des mineurs n'est pas fixe. Plus le nombre de blocs validés augmente, plus la rémunération des activités de minage diminue. La rémunération est divisée par deux tous les 210 000 blocs trouvés, et cela pour une raison simple : la somme totale des bitcoins est limitée [42].

1.5. Les types de blockchain

Les techniques de vérifications diffèrent selon le type de blockchain. Ainsi nous avons :

- **La blockchain bitcoin :** Elle utilise l'algorithme de consensus proof of work (preuve de travail) pour résoudre des problèmes mathématiques. Ces problèmes sont résolus par un mineur. Ce principe fait que la blockchain valide les transactions en se passant comme autorité centrale. Après le bitcoin d'autres crypto-monnaies ont été créées avec l'Ethereum.
- **La blockchain Ethereum :** Elle est très similaire à celle de bitcoin. Ce blockchain est utilisée dans les smarts contracts (contract intelligent). Les smarts contracts sont des interfaces qui connectent un utilisateur à un fournisseur de service au travers d'un réseau peer to peer [43]. Dans la blockchain Ethereum les blocs sont traités environ un toutes les 14 secondes. Les mineurs sont récompensés à 4 unités. Ce nombre diminue de la valeur de la crypto-monnaie continue à augmenter. La blockchain Ethereum utilise les algorithmes de consensus proof of work et proof of stake pour la validation des transactions.
- **Le Ripple :** Elle n'utilise pas une blockchain comme bitcoin et Ethereum. Pour effectuer des transactions, le réseau Ripple utilise des serveurs de validations qui traitent les données à l'aide d'un registre commun. Ces serveurs de validations sont gérés soit par des banques, soit par des particuliers. Les serveurs de validations utilisent un mécanisme de consensus appelé HashTree[4]. Ce mécanisme est différent du proof of work de la blockchain du fait qu'il compare les données et les traite à l'aide d'un registre commun.
- **La blockchain Peercoin :** Elle est créée en 2012, c'est une cryptomonnaie peer to peer utilisant les algorithmes de consensus proof of work et proof of stake.
- **Hyperledger** : C'est une plateforme de développement de blockchain open source initiée en 2015 par la fondation linux.
- **Tendermint** : C'est une plateforme open source de Blockchain permettant l'exécution de smart-contract multi-langages dont l'algorithme de consensus PBFT résiste à la panne, même si 1/3 des acteurs sont malveillants ou déconnectés [44].

[4] Hash tree (arbre de hachage) est une structure de données persistante, une stratégie de mise en œuvre pour les ensembles et les cartes

- **Z-Cash :** C'est une Blockchain permettant les transactions anonymes grâce à la technologie cryptographique innovante [5]zk-SNARK. Sur le réseau Z-cash, il existe deux types d'adresse les transparentes « t-address » et les protégées « z-addresses ». Les transactions entre les premières sont similaires à celles de Bitcoin, celles qui se font sur la seconde en revanche sont inscrites dans le registre de manière chiffré. Un algorithme dit « de preuve à divulgation nulle de connaissance » (zero-knowledge proof) garantit l'intégrité de ces transactions [45].
- Tezos est une Blockchain qui permet le déploiement d'applications décentralisées dont le consensus repose sur la preuve d'enjeu (PoS : Proof of Stake) à « gouvernance intégrée », il permet d'exécuter des smarts contracts. En effet, toute proposition d'évolution du code source soumise à un vote réunissant 80% sur un Quorum de 80% des détenteurs de Tez donnera lieu à une mise à jour. De plus, le langage utilisé pour les smart contract est écrit en Ocaml et permet la vérification formelle de la cohérence entre le code compilé et le code source [46].

1.6. Utilisation des blockchains

Les blockchains peuvent être utilisées dans trois catégories : dans le transfert d'actif, dans les smarts contracts et dans l'ancrage.

1.6.1. Blockchains dans le transfert d'actif

Le bitcoin a été conçu pour permettre le transfert d'actif à travers une monnaie électronique entièrement décentralisée. En effet le transfert d'actif est une opération économique et financière, qui consiste à céder des actifs immobilisés ou circulants à une autre entreprise [47]. Selon la banque mondiale, le marché du transfert d'argent va représenter 636 milliards de dollars en 2017. Les opérateurs de transfert, comme Western Union, prennent quelque 10% de commission sur chaque transfert, et encore plus les transferts concernant l'Afrique qui sont près de deux milliards de dollars par an selon l'ONG Overseas Development Institute [48]. Blockchain ferait disparaitre les commissions des intermédiaires avec le transfert d'argent entre les particuliers. Avec la fondation Stellar qui est un organisme créé en 2014 par jed McCaled, effectue des paiements transfrontaliers à faible frais. La cryptomonnaie émise par cette dernière est convertie par des banques partenaires en monnaie fiduciaire locale.

[5] Zk-SNARK (Zero knowledge succinct Non-Interactive Argument of Knowledge) fait référence à une construction de preuve où l'on peut prouver la possession de certaines informations, par exemple, une clé sécrète, sans révéler ces informations et sans aucune interaction entre le prouveur et le vérificateur.

1.6.2. Blockchains dans les smarts contracts

Les blockchains sont utilisées dans les contrats intelligents pour automatiser les flux de travail. Ces contrats ont la capacité d'exécuter automatiquement des instructions préalablement définies. Le code informatique garantit la validité des transactions une fois que les obligations contractuelles sont remplies conformément aux termes établis en amont, et l'ensemble du processus numérique est automatisé. Grâce aux contrats intelligents, si l'une des obligations contractuelles n'est pas satisfaite, les transactions seront annulées, et le cas échéant, les sommes seront restituées sans nécessiter d'intervention de quiconque.

1.6.3. Blockchains dans l'ancrage

La technologie blockchain permet de protéger une création par l'encrage de la preuve dans la base de données en datant la création dans son œuvre et de répliquer la preuve dans la mémoire de l'intégralité des nœuds du réseau. L'ancrage blockchain permet de préserver l'intégrité et l'immuabilité d'un fichier contre toute modification ultérieure lors de son enregistrement. Il est aussi utilisé pour garantir l'intégrité des transactions ayant lieu dans le réseau blockchain.

1.7. La pratique de la blockchain dans les domaines d'activité

1.7.1. Les crypto-monnaies

La blockchain est une technologie de registres distribués qui forme la chaine de bloc. Les blocs différents des crypto-monnaies. Ces dernières sont des monnaies électroniques, des actifs numériques décentralisées qui n'existent que sur le réseau. Elles servent un moyen d'échange au sein d'un réseau d'utilisateur. Ces échanges sont sécurisés par la cryptographie asymétrique pour sécuriser les transactions financières. Bitcoin est la première cryptomonnaie la plus célèbre avec sa blockchain. La blockchain bitcoin permet de faire des transactions simultanées qui sont stockées dans un bloc. Un bloc contient toutes les transactions faites lors des 10 dernières minutes. Ces transactions sont vérifiées par des nœuds. Les nœuds sont des détenteurs du registre (chaque ordinateur qui possède une copie de la blockchain). Ces nœuds appelés mineurs vérifient le bloc. Tous les mineurs sont des nœuds, mais tous les nœuds ne sont pas forcément des mineurs. Après la création de la première cryptomonnaie, bitcoin qui se limite aux échanges des devises numériques, d'autres cryptomonnaies ont vu le jour comme l'Ethereum, le Litecoin, le Ripple etc. L'Ethereum est similaire à bitcoin à la différence que la blockchain Ethereum piste la propriété de la devise électronique et le fait de fonctionner le code de programmation de certain nombre d'applications décentralisées dapps (logiciels open source). Le Litecoin a été créé avec le même code source avec le bitcoin pour gérer un volume de transactions

beaucoup plus élevé grâce à sa génération de blocs rapides. Contrairement aux bitcoin, ether et le litecoin, le Ripple est un système de règlement proposant une alternative plus rapide, transparente et sécurisée aux systèmes utilisés par les banques comme le système SWIFT[6] [49]. La cryptomonnaie XRP est utilisée pour le transfert de paiement vers d'autres devises dans le réseau Ripple.

1.7.2. Les smarts contracts

Les smarts contracts sont des contrats stockés dans la blockchain, exécutés de façon automatique, et de pair à pair, lorsque les conditions précisées sont remplies [50]. Ces contrats sont écrits en langage de programmation et sont conçus pour automatiser, valider et exécuter automatiquement des termes contractuels lorsque les conditions spécifiées sont remplies. Les smart contracts fonctionnent sur la base de la technologie blockchain, ce qui garantit leur sécurité, leur transparence et leur immuabilité. Ils sont souvent utilisés pour automatiser divers processus et transactions, éliminant ainsi le besoin d'intermédiaires. Ils suppriment le besoin de recourir à une assurance dans le cadre d'un prêt avec la technologie blockchain. La blockchain la plus utilisée pour les contrats intelligents est l'Ethereum.

1.7.3. Les NFTs

Les NFTs (Non-Fungibles Tokens) encore appelés jetons non fongibles sont des objets numériques vendus sur la blockchain. Avec les NFTs l'information est encryptée sur la blockchain sous forme de jetons. Ils sont émis au même titre qu'une cryptomonnaie comme l'ether ou le bitcoin. Contrairement au bitcoin qui est fongible, Les NFTs ont un caractère unique pour chaque unité (token) et ne peut être dupliquer. Les NFTs sont utilisés dans les contenus numériques, les articles de jeu, les investissements et garanties (le decentralized finance utilise les NFTs pour garantir les prêts), dans les noms de domaine (comme le nom de domaine d'un site web en rendant l'adresse IP plus mémorable). Les NFTs permettent d'assurer l'authenticité et l'unicité d'un objet numérique et de le suivre dans le temps.

1.7.4. Les finances décentralisées

La finance décentralisée ou DeFi désigne une infrastructure innovante dont la particularité est de ne pas se reposer sur une banque centrale ou sur des agences gouvernementales pour fonctionner [51]. Les finances décentralisées s'appuient sur la technologie blockchain et les

[6] SWIFT (society for worldwide Interbank Financial telecommunication) est une composante du système financier international qui agit en tant qu'intermédiaire facilitant le transport des messages contenant des instructions de paiement entre les institutions financières impliquées dans une transaction.

contracts intelligents pour effectuer des transactions sans intermédiaires. La DeFi et les cryptomonnaies sont liées, La DeFi se sert de la cryptomonnaie pour exister en proposant des services financiers sans intermédiaires. Les utilisateurs de la DeFi utilisent des applications DApps qui permettent aux particuliers et aux entreprises d'effectuer des services d'obtention de prêt, de transfert d'argent, de placement d'épargne, etc.

1.7.5. Les registres de titres de propriétés

La blockchain améliore la tenue des registres et la vérification des titres en sécurisant les registres lors de l'enregistrement des transactions du registre foncier. En utilisant une base de données distribuées, les transactions et les enregistrements ne peuvent pas être corrompus ou manipulés. La blockchain étant un registre de données distribuées, cela empêche toute réclamation frauduleuse ou incorrecte des titres fonciers et de falsification des données car toute modification est visible pour tous les participants. Avec l'enregistrement des données liées à la propriété telle que les dossiers fiscaux et les informations sur les hypothèques dans la blockchain permet de vérifier l'authenticité des titres en éliminant tout litige potentiel [52]. Etant un réseau de transaction pair à pair, la blockchain rend le processus de transfert des titres fonciers plus rapides et plus sûrs. La blockchain élimine le besoin de vérification manuelle des titres fonciers qui peut être couteuse car c'est un réseau distribué et accessible à tous.

1.7.6. Le vote numérique

Le vote numérique est un système de vote dématérialisé, à un comptage automatisé, notamment des scrutins, à l'aide de systèmes informatiques [53]. Le système de vote numérique pose des problèmes de vérification des votes individuels, de piratage de bases de données électorales. L'application de la blockchain dans le vote numérique permet de donner des résultats anonymes. Le vote numérique sur une blockchain peut potentiellement améliorer l'accessibilité en permettant aux électeurs de participer depuis n'importe quel endroit avec une connexion Internet. Cela pourrait être particulièrement bénéfique pour les citoyens qui se trouvent à l'étranger ou dans des zones éloignées. Les votes pourraient être cryptés pour garantir la confidentialité tout en permettant aux parties autorisées de vérifier les résultats.

Chapitre 3 : Gouvernance et gestion de la crypto-monnaie dans l'espace UEMOA.

L'UEMOA est créée par le traité signé à Dakar le 10 janvier 1994 par les chefs d'Etat et de gouvernements des sept pays de l'Afrique de l'Ouest ayant en commun l'usage d'une monnaie commune, le Franc de la communauté Financière Africaine (FCFA), dont l'émission est confiée à la BCEAO. Le Franc CFA est une monnaie créée en 1945 par la France. Elle est basée sur quatre principes : libre convertibilité, libre transférabilité, parité fixe et la centralisation de 50% des réserves de changes vers la France. L'offre de cette monnaie est liée à plusieurs contraintes dont le niveau des avoirs en devises étrangères de la zone. Ainsi, beaucoup d'économistes pensent que la création de cette monnaie est insuffisante dans la mesure où une bonne partie de la population est exclue et n'ont pas accès aux financements. En plus, les échanges commerciaux entre les zones du Franc CFA sont très faibles environ 1% pour la CMAC et 15% pour l'UEMOA selon (la Cnuced, 2022). Ce qui remet en cause la quintessence de la création de cette union. Dans l'optique d'une création d'une cryptomonnaie dans l'UEMOA, sa création et sa gestion s'avéreront très complexe.

1. Création et offre de la cryptomonnaie

Avant de procéder à la création d'une monnaie numérique il faut faire le choix entre la création d'une cryptomonnaie et d'un jeton. Ces derniers présentent des différences. En effet un jeton est un actif numérique généré sur une blockchain existante pour développer des applications de finance décentralisée ou des jeux permettant de gagner des actifs numériques. Alors qu'une cryptomonnaie possède sa propre blockchain native, elle permet de faire des transactions et du staking[7] d'où le choix de cette dernière pour notre projet. Pour créer une cryptomonnaie il faut un certain nombre d'étapes :

La création d'un modèle économique, il faut d'abord définir l'offre totale d'actif numérique c'est-à-dire le nombre maximal d'actif numérique en circulation. Celui de bitcoin est limité à 21millions de pièces alors que pour Ethereum le nombre est illimité. Au moment de la création d'une cryptomonnaie, son cours initial est faible. La valorisation d'une cryptomonnaie dépend de son offre totale et de sa demande sur le marché. Si la demande est supérieure à l'offre, la cryptomonnaie aura une grande valorisation. La valeur d'une cryptomonnaie dépend aussi de l'intérêt des investisseurs.

[7] Le staking est une fonction similaire au minage : il s'agit d'un processus par lequel un participant au réseau est sélectionné pour ajouter le dernier de transaction à la blockchain et gagner des cryptomonnaies en contrepartie.

Lors de la création de la nouvelle cryptomonnaie, il est nécessaire de choisir l'architecture de la blockchain à adopter. Pour cela il faut faire le choix entre une blockchain publique (accessible à tous), une blockchain privée (accès personnalisé) et une blockchain avec autorisation. L'architecture de la blockchain permet ou non aux utilisateurs de valider les transactions ou de faire fonctionner les nœuds et d'avoir un contrôle sur la cryptomonnaie. Afin, de mieux cerner la création et la gestion de cette monnaie, notre réflexion sera axée sur la créance sur l'économie, sur les Etats et sur le reste du monde.

1.1. La création axée sur le crédit à l'économie

La création monétaire est de nos jours confiée aux banques commerciales qui à travers l'octroi des prêts à ses clients garantissent ce processus. Avec ce processus les banques commerciales créent de la monnaie scripturale par un simple jeu d'écriture. Par contre, la monnaie fiduciaire est créée par la banque centrale qui oriente le processus de création monétaire par les banques commerciales en fixant des taux directeurs par lesquels les banques commerciales se basent pour déterminer le taux d'intérêt des prêts accordés aux entreprises et aux particuliers. Avec la cryptomonnaie, les agents peuvent effectuer des crédits sans faire recours à des banques. Le prêt crypto, contrairement au système bancaire traditionnel, offre des modalités diverses et accessibles à tous. Il peut prendre la forme de prêts pairs à pairs basés sur la blockchain, où les utilisateurs prêtent directement des cryptomonnaies sans l'intermédiaire d'une entité centrale. Les plateformes spécialisées permettent également d'obtenir des prêts en déposant des cryptomonnaies en garantie, le montant étant bloqué en tant que collatéral. Sur des plateformes comme Binance, le prêt implique de bloquer une somme trois fois supérieure à celle empruntée. Ces prêts, basés sur des contrats intelligents, comportent des taux d'intérêt variables et les fonds sont restitués une fois le remboursement effectué. L'obtention de crédits en cryptomonnaie peut également se faire par le biais de participations à des projets de cryptomonnaies avec des Initial Coin Offerings (ICO) et des Security Token Offerings (STO). Les traders peuvent utiliser des marges de trading pour emprunter des cryptomonnaies sur certaines plateformes, moyennant des frais d'intérêts. Les emprunts institutionnels auprès d'institutions financières spécialisées dans la cryptomonnaie, avec des cryptomonnaies comme garantie, sont une option pour les entreprises et les investisseurs. De plus, l'échange de tokens contre des monnaies fiduciaires équivalentes est une possibilité. La finance décentralisée (DeFi) et le staking permettent aux détenteurs de cryptomonnaies d'utiliser le staking pour verrouiller leurs fonds dans un protocole, soutenant ainsi le réseau tout en ayant la possibilité d'emprunter des fonds en utilisant

le staking comme garantie. Les cryptomonnaies fonctionnent sur des principes décentralisés qui assurent le contrôle de la masse monétaire. La gestion de cette masse monétaire dans la création d'une cryptomonnaie axée sur le crédit à l'économie prend en compte plusieurs éléments pour assurer la viabilité et la stabilité de la cryptomonnaie. Pour cela il faut déterminer :

- Offre totale (fixe ou flexible) : Définir si la masse monétaire de la cryptomonnaie sera fixe comme celle de bitcoin ou le nombre de pièces à créer est plafonné ou flexible ou de nouvelles unités peuvent être créées en fonction des besoins de l'économie ce qui sera dans notre cas car certaines populations n'ont pas accès à des services financiers dans la région.
- Offre en circulation : déterminer le nombre de cryptomonnaies actuellement disponibles sur le marché. Ce nombre peut varier en fonctions des mécanismes de minage.
- La capitalisation boursière : Elle mesure la taille d'une cryptomonnaie sur le marché. Elle est calculée en multipliant le prix actuel de la cryptomonnaie par son offre en circulation.
- La création monétaire basée sur le crédit : notre cryptomonnaie sera axée sur le crédit permettant la création de nouvelles unités lorsqu'un acteur économique emprunte de l'argent à travers des contrats intelligents.
- Réserve fractionnaire : Mettre en œuvre un système de réserve fractionnaire où une partie des dépôts est conservée en réserve et le reste est prêtée. Ce qui peut augmenter la masse monétaire.
- La stabilité des prix : La gestion de la masse monétaire devrait viser la stabilité des prix pour éviter une volatilité excessive qui peut nuire à l'adoption et l'utilisation de la cryptomonnaie.
- Audibilité : Il faut assurer que la masse monétaire et les mécanismes de création sont transparente et vérifiable pour renforcer la confiance des utilisateurs dans la cryptomonnaie.
- Réaction aux fluctuations économiques : Pour cela, il faut prévoir des mécanismes qui permettent à la masse monétaire de s'ajuster en réponse aux fluctuations économiques.

La gestion de la masse monétaire de l'UEMOA est assurée par la BCEAO qui en tant qu'organe central de la politique monétaire, surveille les agrégats monétaires pour évaluer la quantité de monnaie en circulation. Elle met en œuvre des politiques visant à maintenir la stabilité des prix,

à stimuler la croissance économique et à garantir la stabilité financière dans la région. Selon les données de la BCEAO, Le volume des devises en circulation au sein des économies de l'UEMOA a continué de croître, atteignant 43 104,3 milliards FCFA en 2022, comparé à 38 359,3 milliards FCFA en 2021, enregistrant ainsi une hausse de 12,4% (+4 745 milliards FCFA)sur le rapport sur la politique monétaire de juin 2022, La situation monétaire de l'Union se caractérise par une augmentation de 12,7% de la masse monétaire à la fin de juin 2022, sur une base annuelle, par rapport à la croissance de 11,9% enregistrée à fin mars 2022. Cette progression de la masse monétaire est attribuable à l'augmentation des créances intérieures de 7 180,9 milliards (+18,4%), atténuée par la contraction des actifs extérieurs nets de 2 135,5 milliards (-24,5%). L'augmentation des créances intérieures provient de la hausse des créances nettes des institutions de dépôt envers les Administrations Publiques Centrales (+30,7% ou +4 154,8 milliards) et des créances sur l'économie (+11,9% ou +3 026,0 milliards). Les avoirs officiels de réserve ont enregistré une diminution de 79,9 milliards au cours du deuxième trimestre 2022, se fixant à 13 422,0 milliards à fin juin 2022, correspondant à un taux de couverture de l'émission monétaire de 77,8%, inférieur à son niveau du trimestre précédent (79,9%). Ces réserves officielles de change garantissent à l'Union une couverture de 5,1 mois d'importations de biens et services, tout comme au trimestre précédent. Il faut noter également que le taux de croissance du PIB de l'union a connu une hausse de 4.2 points par rapport à 2020 pour s'établir à 6,0% en 2021. La relance de l'activité économique après le COVID-19 est accompagnée par une hausse des prix à la consommation, le taux d'inflation annuel moyen est passé de 2,1% en 2020 à 3,6% en 2021. En 2022, il est à 7,1% en raison de la guerre en Ukraine sur les cours mondiaux Le taux de chômage des pays de l'UEMOA est passée de 44,6% au deuxième trimestre 2022 contre 43,5% le trimestre précédent. Il faut noter que la politique monétaire dans la Zone franc de l'UEMOA, dirigée par la BCEAO, présente deux lacunes majeures. D'abord, il y a un manque de réflexion interne sur le rôle d'une banque centrale dans des économies parmi les plus défavorisées, caractérisées par une faible monétarisation et bancarisation, avec une prédominance du secteur rural et informel. Ensuite, il y a une discordance entre les déterminants réels de son objectif de stabilité des prix et les moyens effectifs à sa disposition, notamment les instruments de gestion monétaire, dans un environnement avec des contraintes physiques, organisationnelles et institutionnelles significatives. Les données sur la politique monétaire de la BCEAO montrent qu'il n'y a pas suffisamment de monnaies pour soutenir l'activité économique au sein de l'UEMOA d'où notre

choix pour créer une cryptomonnaie avec une offre ajustable c'est-à-dire qui n'a pas d'offre fixe. Une offre ajustable permet d'injecter de nouvelles unités de cryptomonnaies dans le système, contrôler l'inflation. Pour le début de notre projet nous proposons une cryptomonnaie avec une offre initiale de 60 millions d'unités de cryptomonnaies. Ainsi, le prix de cette cryptomonnaie sera déterminer en fonction de la loi de la demande et de l'offre.

1.2. La création axée sur la créance sur les Etats

La création de la cryptomonnaie axée sur la créance sur les Etats implique l'utilisation des contrats intelligents. En effet la gestion de cette créance peut être adossée à des actifs souverains tels que des devises nationales pour garantir la valeur de la cryptomonnaie. Ces actifs peuvent être des titres d'Etats, des obligations et d'autres instruments financiers émis ou garantis par un gouvernement. Les smarts contracts ont la capacité d'exécuter automatiquement des instructions prédéfinies. Ils peuvent être programmés pour représenter les termes d'une créance sur un Etat en indiquant les conditions d'émission, de remboursement et de distribution de revenu de la cryptomonnaie. Les mécanismes de gestion des distributions des paiements associés à la créance sur les Etats pourraient être gérés par les smarts contracts en automatisant les intérêts et les remboursements provenant des actifs sous-jacents en fonction des conditions spécifiées dans les contrats intelligents. Avec la blockchain, les transactions des actifs sous-jacents seront enregistrées de manière transparente assurant ainsi la traçabilité et la vérifiabilité des réserves. Les contrats intelligents permettent de garantir l'adhésion des partenariats formels avec les gouvernements aux règlements et renforcer la confiance des utilisateurs en assurant la légitimité et la conformité réglementaire. Ces partenariats pourraient inclure des accords légaux, des audits réguliers, réglementaires, et des engagements de transparence pour garantir la conformité. Le fait d'adosser une cryptomonnaie à un actif émis par un gouvernement pourrait réduire la volatilité souvent associée à cette dernière. L'État exerce une influence significative sur la masse monétaire par le biais de ses politiques monétaires, fiscales et économiques. La gestion sur les créances sur les Etats impacte la quantité de monnaies en circulation. Selon les données de la BCEAO, la gestion des finances publiques dans les États membres de l'UEMOA serait marquée par une dégradation du déficit budgétaire, qui passerait de 5,5% du PIB en 2021 à 5,9% en 2022, en lien notamment avec la poursuite des mesures de relance et la mise en œuvre d'actions de lutte contre la vie chère. La consolidation budgétaire devrait toutefois reprendre à partir de 2023, avec un déficit prévu à 4,7% du PIB. Le taux de pression fiscale progresserait de 13,6% en 2022 à 14,2% en 2023. L'adoption de la

cryptomonnaie pourrait offrir des opportunités pour renforcer la stabilité financière, faciliter les transactions et potentiellement contribuer à la réduction du déficit budgétaire. En parallèle, une augmentation du taux de pression fiscale de 13,6% en 2022 à 14,2% en 2023 souligne la nécessité d'explorer des solutions novatrices pour optimiser les recettes publiques, et la cryptomonnaie pourrait jouer un rôle significatif dans cette transformation économique.

1.3. La création axée sur créance sur l'étranger

La création d'une cryptomonnaie axée sur la créance sur l'étranger implique de développer une cryptomonnaie adossée à des créances sur des actifs ou des obligations émis par des entités étrangères. Une cryptomonnaie adossée à une devise étrangère offre une représentation numérique de la valeur d'une monnaie étrangère et permet d'effectuer des paiements et des transferts internationaux tout en gardant la stabilité relative de la valeur. Avec les contrats intelligents, les transactions commerciales internationales peuvent être sécurisées et automatisées en définissant les conditions de paiement de manière transparente et immuable. La gestion des chaines d'approvisionnement internationale pourrait être facilitée par la blockchain en améliorant la traçabilité et la transparence afin de faciliter le suivi des créances et des paiements entre les parties prenantes. Les projets cryptomonnaies peuvent lever des fonds à l'échelle mondial en laçant des ICO internationales afin de créer une forme de financement décentralisée. Les implications économiques internationales d'une cryptomonnaie axée sur la créance sur l'étranger s'éclairent davantage. Cependant, en se recentrant sur la réalité des échanges extérieurs des États membres de l'UEMOA, on constate un solde global de la balance des paiements déficitaire de 508,8 milliards au deuxième trimestre 2022, en comparaison avec le déficit de 369,8 milliards enregistré à la même période de l'année précédente. Cette évolution résulte d'une aggravation du déficit courant que les entrées nettes de ressources n'ont pas pu couvrir. L'adoption d'une cryptomonnaie dans l'UEMOA pourrait offrir une solution potentielle à la réalité des échanges extérieurs des États membres, marquée par un solde global de la balance des paiements déficitaire de 508,8 milliards en facilitant les transactions internationales, améliorant la traçabilité en contribuant à la correction des déséquilibres dans la balance des paiements.

2. Gestion de la masse monétaire

La masse monétaire définit la quantité de monnaie en circulation dans une économie. Elle regroupe l'ensemble des liquidités (les dépôts bancaires, les actifs financiers et la monnaie fiduciaires). Il est géré par la banque centrale dans la zone euro de façon qu'elle soit adaptée

aux besoins des agents économiques. La masse monétaire mesurée des indicateurs appelés des agrégats monétaires c'est-à-dire des statistiques qui regroupent les moyens de paiement détenus par les agents d'un territoire donné. Les agrégats monétaires sont définis selon le degré de liquidité décroissante. La masse monétaire des cryptomonnaies fonctionne différemment par rapport aux monnaies traditionnelles émises par la banque centrale. Elle est analysée par différents éléments à savoir :

- La limitation de l'offre de certains cryptomonnaies : La plupart des cryptomonnaies ont une offre prédéterminée émise au fil du temps. Le bitcoin a une offre totale limitée à 21 millions. Il faut noter aussi que la confiance des utilisateurs, la sécurité du réseau et la réglementation ont une influence capitale sur la masse monétaire des cryptomonnaies.
- Le contrôle du réseau : les algorithmes de consensus tels que la preuve de travail et la preuve d'enjeu contrôlent la masse monétaire des cryptomonnaies en déterminant comment et quand de nouvelles unités de cryptomonnaie sont créées.
- L'émission de nouvelles unités en récompense par le processus de minage pour la validation des transactions peut influencer la masse monétaire
- La diversité des modèles : Les cryptomonnaies suivent différents modèles pour influencer la masse monétaire. Certains ont une offre limitée, d'autres se basent sur des mécanismes de consensus complexes pour créer de nouvelles unités. Ce qui peut différer la manière de gérer la masse monétaire. Cette diversité influence la perception des investisseurs et la valeur de la cryptomonnaie.
- L'impact sur la valeur : l'offre limitée ou illimitée de certain cryptomonnaie influence la valeur des cryptomonnaies.
- La volatilité des prix : L'offre limité de certain cryptomonnaie et l'émission de nouvelles unités influencent la volatilité des prix

Conclusion Générale

En somme la cryptomonnaie représente un domaine en constante évolution qui suscite un intérêt croissant dans le monde entier. Elle émerge comme une force motrice dans l'évolution financière mondiale, avec des implications profondes et diversifiées. Etant une monnaie numérique décentralisée, la cryptomonnaie repose sur la technologie blockchain. Cette dernière offre une solution transparente et sécurisée pour enregistrer et vérifier les transactions éliminant le besoin de confiance dans une entité centrale. La sécurité des cryptomonnaies pour garantir la confiance des utilisateurs et la stabilité du système est assurée par la cryptographie et les mécanismes de consensus. La cryptomonnaie offre des avantages potentiels tels que la décentralisation, la transparence, l'inclusion financière, la réduction des frais et l'autonomie financière. Cependant, Elle présente également des défis et des risques significatifs tels que la volatilité des prix, la réglementation incertaine, et les problèmes de sécurité qui nécessitent une gestion prudente.

L'intégration de la cryptomonnaie dans l'espace UEMOA offre un potentiel significatif pour façonner l'économie, stimuler l'innovation technologique en utilisant les applications décentralisées et les contrats intelligents, faciliter les paiements transfrontaliers, et de potentialiser de nouvelles formes d'inclusion financière. Pour garantir le succès de l'intégration des cryptomonnaies dans l'espace UEMOA, la gouvernance jouera un rôle central en exigeant une collaboration étroite entre les gouvernements pour créer un environnement favorable basé sur la compréhension des dynamiques spécifiques de la région pour maximiser les avantages des cryptomonnaies dans l'espace et une adaptation continue aux évolutions du marché mondial des cryptomonnaies. Cette trajectoire vers l'avenir financier doit être marquée par une adaptation continue aux évolutions du marché mondial des cryptomonnaies. Cela nécessitera une vigilance constante et une réponse agile aux changements pour garantir le succès et la durabilité de l'intégration des cryptomonnaies dans l'économie de l'espace UEMOA.

Bibliographie

Ouvrages :

- Jacques Favier. Bitcoin : La monnaie acéphale. 2017
- Tiana Laurence : La blockchain pour les nuls, Editions First, un département d'Edi8, 2018
- Enee Bussac : Bitcoin, ether & Cie, Munich, 24 juillet 2018
- Jean Paul PONS et L'UTL34 : Les cryptomonnaies impasse ou révolution ?
- L'internet de l'argent, d'Andrea M. Antonopoulos, 2019
- Blockchain et cryptomonnaies, de Primavera de Filipi, 2018
- Bitcoin-métamorphoses : de l'or des fous à l'or numérique ? de Jacques Favier, Benoit Huguet, et Aldi Takkal Bataille, 2018
- Bitcoin, monnaie libre, de Pierre Noizat, 2013
- J'achète du bitcoin : Guide pratique pour miser sur les nouveaux placements-Bitcoin, Ethereum, Token, Ico, de Philippe Herlin, 2018
- Mastering Bitcoin : programming the open blockchain, d'Andreas M. Antonopoulos, 2017
- Digital gold : Bitcoin and the inside story of the misfits and millionaires trying to reinvent money, de Nathaniel Popper, 2016

Articles :

- Delahaye, J. P., (2014). Le Bitcoin, première cryptomonnaie. Bulletin de la Société Informatique.
- Goudiaby, al, (2023) Le rôle du régime de change dans la correction des déséquilibres extérieurs de l'UEMOA : une analyse sur la position extérieure globale.
- Nubukpo, (2007) Dépenses publiques et croissance des pays de l'Union Economique et Monétaire Ouest Africaine (UEMOA).
- Delahaye, J.P., (2013). Bitcoin, la cryptomonnaie. Pour la science.
- Erwan J Jonchères (2016), les cryptomonnaies sont des monnaies numériques, qui se sont développées hors de tout contrôle étatique de manière décentralisé.
- HUSSAIN Ali. L'économie dans l'ère de la Crypto-Monnaies.2022

1. https://journalducoin.combitcoin/ définition-histoire-fonctionnement/
2. https://kriptomat.io/f/ cryptomonnaie/litecoin/qu'est-ce-que-le-litecoin
3. https://cryptoactu.com/ quest-ce-que-peercoin-pcc/
4. https://www.economie.gouv.fr/ entreprises/blockchain-definition-avantage-utilisation-application#
5. https://fr.investing.com/analysis/ la-valeur-du-marche-crypto-est-en-hausse-de-55-en-2023-facteurs-a-lorigine-du-rallye-200445133#
6. https://cryptoast.fr/ hal-finney-premiere-transaction-bitcoin-btc/
7. https://www.gsam.com/content/gsam/fra/fr/advisors/ market-insights/gsam-connect/2021/Keeping_up_with_the_Cryptocurrencies.html
8. https://lempreintedigitale.com/podcast/ cryptomonnaies-folle-evolution-bitcoin-depuis-10-ans/
9. https://www.lafinancepourtous.com/2023/11/30/ la-speculation-pousse-les-cours-du-bitcoin-a-la-hausse/
10. https://www.cairn.info/ revue-economie-et-prevision-2012 consulté le 12/04/2023
11. https://bitcoin.fr/le-cours-du-bitcoin/ consulté le 16/01/2023
12. https://www.memoireonline.com /04/22/12941/ régulation-des-marches-financiers-face-à-la-crypto-monnaie -en-droit-positif/ consulté le 16/01/2023
13. https://aws.amazon.com/fr/what-is/ cryptography/ consulté le 15/02/2024
14. https://aws.amazon.com/fr/what-is/ cryptography/ consulté le 15/02/2024
15. https://www.techtarget.com/searchsecurity/definition/ Cipher-block-Chaining consulté le 27/07/203
16. https://www.techtarget.com/searchsecurity/definition/ Cipher-FeedBack consulté le 27/07/203
17. https://www.techtarget.com/searchsecurity/definition/ output-FeedBack consulté le 27/07/203
18. https://n26.com/fr-fr/blog/ clé-privée consulté le 27/07/203
19. https://fr.wikipedia.org/wiki/chiffrement_RSA consulté le 27/07/203
20. https://en.wikipedia.org/wiki/ Digital-Signature-Algorithm consulté le 27/07/203
21. https://medium.com/antoine.ansel/ l-algorithme-d-échange-de-clés-Diffie-Hellman consulté le 27/07/203
22. https://www.movable-type.co.uk/scripts/ Sha256.htlm consulté le 27/07/203
23. https://fr.wikipediia.org/wiki/ MD5 consulté le 27/07/203

24. https://www.geeksforgeeks.org/ sha1-hash-in-java consulté le 27/07/203
25. https://www.archipels.io/fad/ quels-sont-les-différents-algorithmes-de consensus consulté le 27/07/203
26. https://hedera.com/learning/ consensus-algorithm consulté le 27/07/203
27. https://cryptoast.fr/ liste-différents-consensus-crypto-monnaies-blockchain consulté le 20/02/2023
28. https://kriptomat.io/fr/crypto-monnaies/solano/ qu'-est-ce-que-Solana consulté le 22/02/2023
29. https://www.briefcrypto.com/ les-différents-algorithmes-de-consensus consulté le 22/02/2023
30. https://www.briefcrypto.com/ les-différents-algorithmes-de-consensus consulté le 22/02/2023
31. https://www.briefcrypto.com/ les-différents-algorithmes-de-consensus consulté le 22/02/2023
32. https://cryptogains.fr/ 6401-les-algorihmes-de-consensus-la-preuve-de-poids-de-reputation consulté le 23/02/2022
33. https://cryptoast.fr/ liste-différents-consensus-crypto-monnaies-blockchain consulté le 23/02/2023
34. https://academy.bit2me.com/fr/ que-es-tolerancia-fallas-bizantinas-bft consulté le 23/02/2023
35. https://f.theastrologypage.com/ Delegated-byzantine-Fault-tolerance consulté le 23/02/2023
36. https://coinacademy.fr/lexique/ Pratical-byzantine-Fault-tolerance consulté le 23/02/2023
37. https://www.bdc.cu/fr/articles-outils/blogue/ que-sont-cchaines-blocs-quel-interet-presentent-elles-pour-votre-entreprise consulté le 14/02/2023
38. https://academy.bit2me.com/fr/ timestam-blockchain consulté le 14/02/2023
39. https://www.okta.com/fr/identity-101/nonce/ consulté le 15/02/2024
40. https://journalducoin.com/lexique/arbre-de-merkle/ consulté le 15/02/2024
41. https://fr.statista.com/statistiques/574479/ cours-mensuel-du-bitcoin/
42. https://bitcoin.fr/le-cours-du-bitcoin/ consulté le 16/01/2023

43. https://www.memoireonline.com /04/22/12941/ régulation-des-marches-financiers-face-à-la-crypto-monnaie -en-droit-positif/ consulté le 16/01/2023
44. https://www2.deloitte.com/fr/fr/pages/ blockchain consulté le 16/01/2023
45. https://academy.youngplatform.com consulté le 16/01/2023
46. https://cryptoast.fr/ fiche-Tezos consulté le 16/01/2023
47. https://www.l-expert-comptable.com/a/ 534108-la-cession-d'-actifs-par-une-entreprise consulté le 16/01/2023
48. Https : //www.blokchainforgoogle.fr/index.php/2017/12/26/694
49. https://www.forbes.fr/finance/ bitcoin-et-Ripple-quelles-différence consulté le 07/11/2023
50. https://www.coinhouse.com/fr/academie/ définition-smart-contract consulté le 07/11/2023
51. https://www.coinhouse.com/fr/academie/ définition-finance-décentralisé consulté le 07/11/2023
52. https://ts2.space/fr/ blockchain-pour-le-registre-foncier-comment-cela-aide-à-améliorer-la-tenue-des-registres-la-verification-des-titres consulté le 07/11/2023
53. https://www.lesecho.fr/2016/io/ sécurisons-les-votes-électroniques-grâce-à-la-blockchain consulté le 07/11/2023

Table des matières