RAPPORT
DE STAGE DE FIN D'ETUDE

Développement d'une plateforme décentralisée
de paiement en ligne via la monnaie digitale
pour les sites E-Commerce

Présenté et soutenu par

Maarouf Hamza

Le : ../../2022

Encadré par

Mr. Zohir CHIBA

Mr. Brahim RAOUYANE

Mr. Youssef Boussofa

Composition du jury

Mr. Zohir CHIBA	Professeur à la Faculté des Sciences Ain-chock
Mr. Brahim RAOUYANE	Professeur à la Faculté des Sciences Ain-chock
Mr.	Professeur à la Faculté des Sciences Ain-chock
Mr.	Professeur à la Faculté des Sciences Ain-chock

Remerciements

Au terme de ce travail, Je tiens à exprimer mes sincères remerciements à ceux qui m'ont beaucoup appris au cours de ce stage, et même à ceux qui ont eu la gentillesse de faire de ce stage un moment très profitable.

Aussi, je remercie **Pr. Zouhair CHIBA** et **Pr. Brahim RAOUYANE**, mes maîtres de stage qui m'ont formé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie. Enfin, je tiens à remercier l'ensemble des collaborateurs de **MATIOUS Digital** et en particulier **M. Youssef Boussafa** pour les conseils qu'ils m'ont prodigués durant ces six mois.

Résumé

Le mécanisme des transactions blockchain est intrinsèquement peer-to-peer et décentralisé. Néanmoins, la plupart des solutions de paiement cryptographiques établies aujourd'hui gèrent les portefeuilles de leurs clients, en intégrant une technologie décentralisée dans des structures centralisées. En conséquence, les acheteurs paient des intermédiaires qui créditent le compte du commerçant.

Donc le but de résoudre ce problème, la société **Matious Digital** a proposé la réalisation d'une solution de paiement de portefeuille à portefeuille (P2P).

Les paiements Web3 multichaînes de **Abierto** déverrouillera la possibilité pour les commerçants de recevoir tous les jetons préférés avec la conversion d'actifs basée sur la blockchain des paiements entrants en temps réel.

Abstract

The mechanism of blockchain transactions is inherently peer-to-peer and decentralized. Nevertheless, most of today's established Crypto Payment solutions manage wallets for their customers, embedding a decentralized technology into centralized structures. As a result, the buyers pay middlemen who credit the merchant's account.

In order to solve this problem, the company **Matious Digital** has proposed the realization of a wallet-to-wallet (P2P) payment solution.

Abierto’s multichain Web3 payments will unlock the ability for merchants to receive any preferred tokens with blockchain-based asset conversion of incoming payments in real-time.

Introduction générale

Le volume de recherche pour “ **Web3** ” a considérablement augmenté au second semestre 2021. Le terme était en discussion depuis des années, nous sommes maintenant plus proches que jamais que la blockchain et cryptocurrencies deviennent plus largement embrassés. Par conséquent, le secteur de l’e-commerce subira des changements cruciaux, ce qui pourrait mener à de nouvelles formes et à de nouveaux environnements.

La première version d’Internet, Web1, consistait principalement en des liens et des pages d’accueil qui permettaient peu ou pas d’interactions pour les utilisateurs. Web2 a pris l’expérience des utilisateurs à une nouvelle hauteur. Les utilisateurs peuvent non seulement lire et écrire, mais aussi publier leur contenu pour les autres à consommer. L’émergence des médias sociaux a accru le partage de contenu des utilisateurs. Web2 fournit une abondance de services, beaucoup même gratuitement, mais les atteintes aux données personnelles ont amplifié l’inquiétude du public concernant leurs traces en ligne.

Alors que Web2 peut être compris comme lecture-écriture, Web3 sera lecture-écriture-propre. La troisième itération d’Internet permet aux utilisateurs de gérer leurs données et leur protocole à travers des applications décentralisées (dApps), construites sur des réseaux P2P comme Ethereum. Web3 résout le problème de confiance que nous avons au cours de la phase actuelle d’Internet en vérifiant continuellement l’identité et l’intention des utilisateurs. La nouvelle forme d’Internet aura un impact significatif sur le secteur du commerce électronique.

- ➔ **Le premier chapitre** présente le contexte général du projet comportant une présentation de l’organisme d’accueil, le cadre du projet, ses objectifs.
- ➔ **Le deuxième chapitre** décrit état de l'art de la Blockchain
- ➔ **Le troisième chapitre** décrit le contexte global du projet, ainsi que la description des besoins fonctionnels, et aussi l’analyse et la conception.
- ➔ **Le quatrième chapitre** est consacrée à la présentation des outils et les technologies utilisées dans la réalisation ainsi que la présentation des interfaces de l’application développée.

Chapitre I: Cadre général du projet

Introduction

Dans ce chapitre, nous présentons notre organisme d'accueil du stage, par la suite, nous faisons une étude de l'existant afin de relever les insuffisances et de proposer une solution efficace.

1. Présentation de l'organisme d'accueil

1.1. Présentation de l'entreprise

Matious Digital est une agence digitale spécialisée dans l'accompagnement technologique et marketing pour des entreprises en Europe et en Amérique du nord.

Depuis la création de **Matious Digital** l'objectif principale qui vise principalement à le réaliser est d'utiliser des technologies de pointe pour développer des solutions futuristes.

La mission de **Matious Digital** concerne plusieurs axes tels que :

- Développement web.
- Développement mobile.
- Data Science & ML.
- Marketing Digital.
- Applications décentralisées
- Développement de contrat intelligent

2. Contexte du projet

2.1. Problématique

Le mécanisme des transactions blockchain est intrinsèquement peer-to-peer et décentralisé. Néanmoins, la plupart des solutions de paiement cryptographiques établies aujourd'hui gèrent les portefeuilles de leurs clients, en intégrant une technologie décentralisée dans des structures centralisées. En conséquence, les acheteurs paient des intermédiaires qui créditent le compte du commerçant.

2.2. Solution proposée

Pour résoudre ce problème on a développé une passerelle de paiement peer-to-peer qui utilise les smart contracts pour la conversion à la volée.

Ce projet a pour objectif :

- Flux de trésorerie instantané : les paiements reçus sont réglés et disponibles pour les commerçants en temps réel.
- Conversion automatique : les jetons sont automatiquement convertis (par exemple en stablecoins) dans le cadre de la transaction de paiement.
- Acceptation de jetons inégalée

Abierto fusionne les idées fondamentales de décentralisation et d'interopérabilité avec les technologies Web3 de pointe en favorisant l'adoption massive des paiements basés sur la blockchain.

4. Outil de collaboration

4.1 Git

Git est un logiciel de gestion de versions décentralisé. C'est un logiciel libre créé par Linus Torvalds, auteur du noyau Linux, et distribué selon les termes de la licence publique générale GNU version 2. En 2016, il s'agit du logiciel de gestion de versions le plus populaire qui est utilisé par plus de douze millions de personnes.

4.2 Slack

Slack « Searchable Log of All Conversation and Knowledge » fonctionne à la manière d'un chat IRC organisé en canaux correspondant à autant de sujets de discussion. La plateforme permet également de conserver une trace de tous les échanges, permet le partage des fichiers au sein des conversations et intègre en leur sein des services externes comme GitHub, Dropbox, Google Drive ou encore Heroku pour centraliser le suivi et la gestion d'un projet. Un robot peut également répondre automatiquement à certaines requêtes de l'utilisateur et s'améliore au fil du temps grâce à des algorithmes d'apprentissage.

Conclusion

Ce chapitre a été consacré au début à une présentation de l'organisme d'accueil, ensuite nous avons donné la description du problème posé et nous avons ainsi défini les différents objectifs de notre application, et à la fin nous avons situé les différents outils de collaboration.

Chapitre 2: Introduction à Blockchain, Ethereum et Smart Contracts

1-Introduction

Le 31 octobre 2008, un inconnu utilisant le pseudonyme « **Satoshi Nakamoto** » a écrit dans une liste de diffusion d'e-mails réservée aux cypherpunks (un mouvement de personnes utilisant la cryptographie pour protéger la vie privée). : "Je travaille sur un nouveau système de monnaie électronique entièrement de pair-à-pair, sans tiers de confiance". Ce texte est accompagné d'un lien qui amène vers **Bitcoin.org** et sur lequel est hébergé le livre blanc du Bitcoin, rédigé dans un anglais impeccable, résumant le fonctionnement du nouveau protocole. Le premier concept de Blockchain a été appliqué le 03 Janvier 2009 dans le cadre de Bitcoin.

La technologie à la base de Bitcoin et d'autres crypto-monnaies, est une base de données de grand livre distribuée pour l'enregistrement des transactions, permettant ainsi aux utilisateurs de partager leur grand livre de transactions.

Dans ce chapitre, On présente et on explique la technologie Blockchain avec ses fonctionnalités les plus importantes et ses concepts associés.

2.La blockchain

La blockchain (chaîne de blocs) est une technologie de stockage et de transmission d'informations, sécurisée par des outils cryptographiques, infalsifiable, transparente car distribuée chez tous ses utilisateurs et sans organe central de contrôle. C'est une sorte de registre mondial de données, qui contient l'historique de tous les échanges réalisés entre ses utilisateurs depuis sa création.

2.1 Concept de la Blockchain

Une blockchain, ou chaîne de blocs, est définie comme une base de données distribué (ledger) qui conserve un enregistrement permanent et immuable (infalsifiable) des données transactionnelles liées entre elles par une chaîne (par blocs).

Propriétés	Blockchain	Base de données traditionnelle
Opérations	Seulement des opérations d'insertion	Peut effectuer des opérations CRUD
Réplication	Réplication complète du bloc sur chaque pair	Maître esclave multi-maître
Consensus	La majorité des pairs s'accordent sur le résultat des transactions	Transactions distribuées (validation en 2 phases)
Invariants	Tout le monde peut valider les transactions sur le réseau	Contraintes d'intégrité

Tableau 2 : Comparaison entre Base de données et Blockchain

Une blockchain est un système totalement décentralisé et basé sur un réseau pair à pair (peer- to-peer). Chaque objet du réseau conserve une copie du ledger afin d'éviter d'avoir un point unique de défaillance. Toutes les copies sont mises à jour et validées simultanément. Bien que l'objectif initial

de la création de la blockchain fût la résolution du problème de la dépense multiple en crypto monnaie (monnaie virtuelle). Cette technologie peut être explorée dans de nombreux cas d'utilisation et utilisée comme un moyen sécurisé de gestion et protection de toute sorte de données (monétaire ou pas).

Le ledger est composé d'un ensemble de blocs. Chaque bloc contient deux parties. La première partie représente le corps du bloc. Il contient les transactions, appelées également faits (facts), que la base de données doit enregistrer. Ces facts peuvent être des transactions monétaires, des données médicales, des informations industrielles, des logs systèmes, etc. La deuxième partie est l'entête (header) du bloc. Ce dernier contient des informations concernant le bloc telque l'horodatage (timestamp), le hach des transactions, etc. Ainsi que le hachage du bloc précédent. De ce fait, l'ensemble des blocs existants forme une chaîne de blocs liés et ordonnés. Plus la chaîne est longue, plus il est difficile de la falsifier.

En effet, si un utilisateur malicieux veut modifier ou échanger une transaction sur un bloc, il doit modifier tous les blocs suivants, puisqu'ils sont liés par leurs hachs. Ensuite, il doit changer la version de la chaîne de blocs que chaque objet participant stocke.

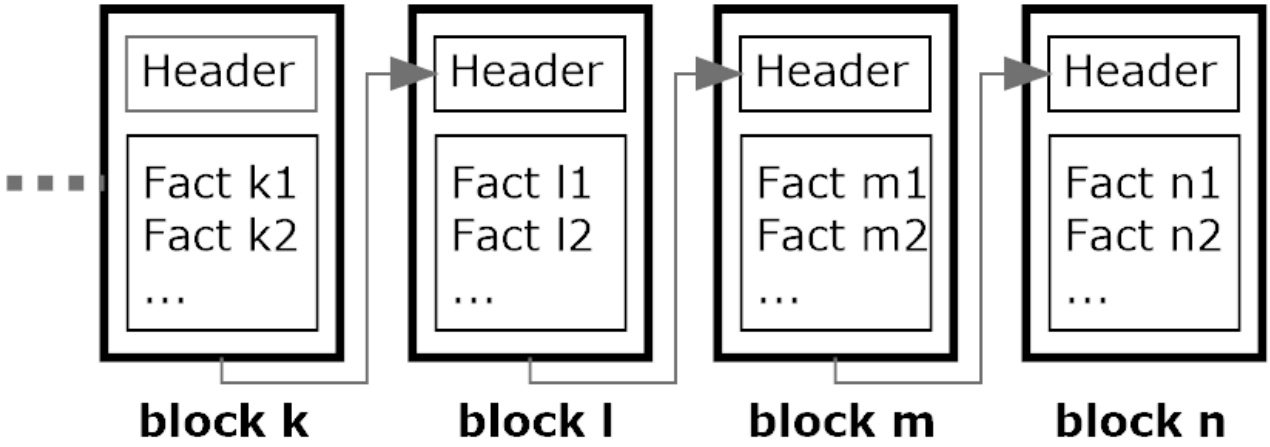


Figure XX : Exemple simplifié d'une Blockchain

Une blockchain suit un réseau P2P. il s'agit essentiellement d'un cadre de réseau multi-réseaux intégré entre pairs, composé de cryptographie, d'algorithmes et d'expressions mathématiques visant à résoudre les limitations classiques de la synchronisation de bases de données distribuées à l'aide d'algorithmes de consensus distribués.

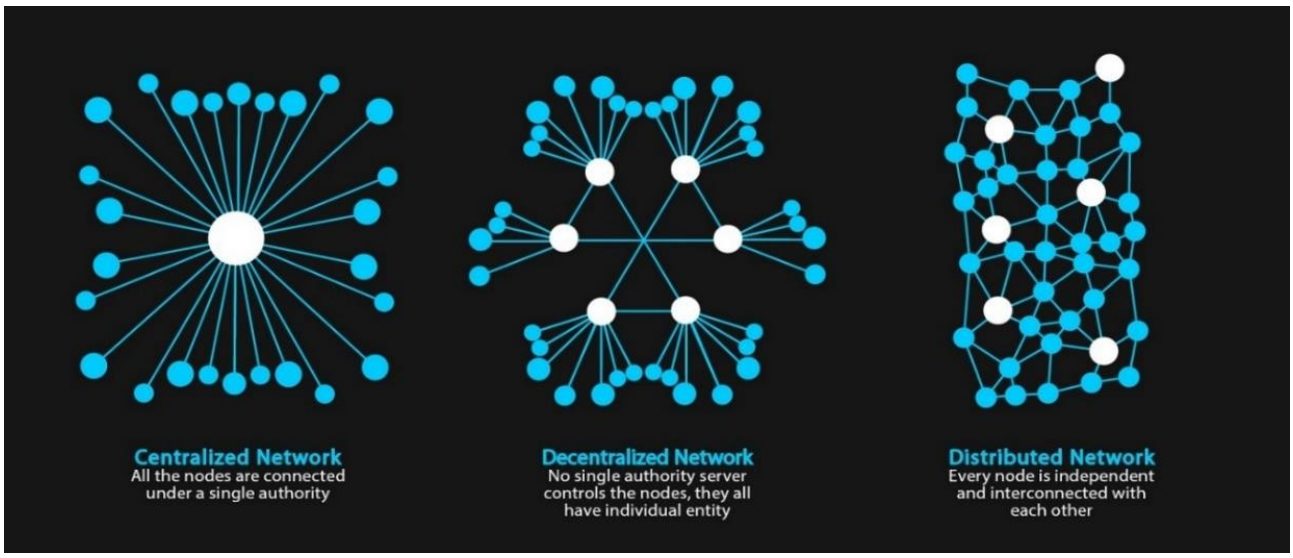


Figure xx : De gauche à droite, réseaux centralisés, décentralisés et distribués (Blockchain)

La technologie Blockchain se caractérise principalement de six éléments majeurs : décentralisé, transparente, sécurisé et immuable, autonome, open source et anonyme. Comme décrit ci- dessus :

- ➔ **Elle est décentralisé :** La blockchain contient Un système de bases de données décentralisé avec un contrôle en libre accès pour tous ceux qui sont connectés au réseau. Les données peuvent être consultées, surveillées, stockées et mises à jour sur plusieurs systèmes. Ces données ne sont pas toutes regroupées dans le serveur d'un intermédiaire central, mais au contraire « distribuées », c'est-à-dire hébergées chez chaque participant ; il n'y a donc pas d'autorité unique pouvant approuver les transactions ou définir des règles spécifiques pour que les transactions soient acceptées. Cela signifie que la confiance est énorme, car tous les participants du réseau doivent parvenir à un consensus pour accepter les transactions.
- ➔ **Elle est transparente :** C'est l'avantage le plus important. Tous les participants peuvent voir les blocs et les transactions qui y sont stockés dedans. Les données enregistrées et stockées dans la blockchain sont transparentes pour les utilisateurs potentiels et peuvent être mises à jour facilement. Cela ne signifie toutefois pas que tout le monde peut voir le contenu réel des transactions, qui sont protégés par une clé privée.
- ➔ **le consensus :** la blockchain correspond à un historique de transactions sur lequel tout le monde s'accorde, ce consensus sur le séquencement des transactions permet de résoudre le problème dit de la "double dépense" : un Bitcoin dépensé dans une transaction ne peut pas être dépensé une deuxième fois dans une transaction qui serait diffusée ultérieurement sur le réseau. La deuxième transaction serait rejetée par le réseau.
- ➔ **Elle est sécurisé :** La base de données peut uniquement être étendue et les enregistrements précédents ne peuvent pas être modifiés (au moins, le coût est très élevé si quelqu'un souhaite modifier les enregistrements précédents).

Ces enregistrements sont dits Immuables, une fois stockés, deviennent réservés pour toujours et ne peuvent pas être modifiés facilement sans le contrôle simultané de plus de 51% des nœuds du réseau.

Le système cryptographique de validation garantit qu'il est quasiment impossible de réécrire une transaction une fois son bloc validé (personne n'a réussi à le faire depuis la création du Bitcoin).

➔ **Autonome :** Le système blockchain est indépendant et autonome, ce qui signifie que chaque nœud du système blockchain peut accéder aux données, les transférer, les stocker et les mettre à jour en toute sécurité, ce qui les rend fiables et exemptes de toute intervention externe.

➔ **Open source :** La technologie de la blockchain est formulée de manière à fournir un accès open source à toutes les personnes connectées au réseau. Cette polyvalence inimitable permet à quiconque non seulement de vérifier publiquement les enregistrements, mais également de développer diverses applications imminentes.

➔ **Anonyme :** Lorsque le transfert de données à lieu entre nœuds, l'identité de l'individu reste anonyme, ce qui en fait un système plus sécurisé et fiable.

Une personne faisant partie de ce réseau doit vérifier chaque nouvelle transaction effectuée. Une transaction de recherche dans un bloc d'une blockchain est vérifiée par tous les nœuds du réseau, elle devient de plus en plus immuable. La figure 28 ci-dessous illustre le flux de travail du processus de la chaîne de blocs.

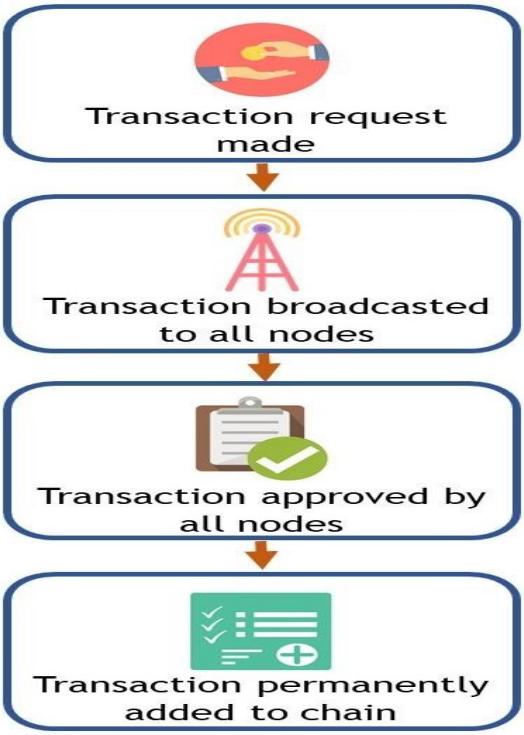


Figure 28 : Un flux de travail généralisé du processus de blockchain

Il existe deux types d'objets participants dans la blockchain : (1) des objets qui peuvent uniquement lire les facts (mode passif), et (2) des objets qui peuvent lire et écrire des facts (mode actif) appelés mineurs. Afin de rajouter un nouveau bloc à la blockchain, il faut suivre les étapes suivantes :

- Une transaction est regroupée avec d'autres transactions dans un bloc;
- Les mineurs vérifient quel est transactions du bloc respectent les règles définies.
- Les mineurs exécutent un mécanisme de consensus pour valider le bloc ajouté.
- Une récompense est donnée aux mineur/mineurs qui valident le bloc.
- Les transactions vérifiées sont stockées dans la blockchain.

Afin de prouver la validation honnête d'un bloc, il existe de nombreux mécanismes de validation. Les plus utilisés sont le mécanisme de Proof of Work (PoW) et le mécanisme de Proof of Stake (PoS).

2.2 Mécanismes de validation de blocs

2.2.1 Proof of work

Dans ce mécanisme, un mineur doit effectuer une quantité de travail, qui est souvent un puzzle ou un défi mathématique, difficile à calculer mais facile à vérifier. La difficulté du défi est adaptée, par la blockchain, en fonction du temps nécessaire à la validation d'un bloc.

Une PoW est exigée pour la validation de chaque bloc. D'une part, elle a l'avantage de protéger l'intégrité des transactions et des blocs, car afin qu'un attaquant puisse modifier un bloc, il doit modifier tous les blocs qui le succèdent et fournir une nouvelle PoW pour chacun de ces blocs, ainsi que la mise à jour de tous les objets par la nouvelle version de la chaîne (falsifiée). Ce qui nécessite une énorme puissance de calcul et d'énergie. D'autre part, la PoW souffre de certaines lacunes qui peuvent avoir des mauvaises conséquences. Sans parler du fait que la PoW consomme une grande quantité d'énergie lors de la résolution du défie mathématique, ce mécanisme peut mener à une potentielle tragédie des ressources d'usage commun (tragedy of commons) [122]. En effet, au fil du temps, les récompenses diminueront, ce qui entraînera une diminution du nombre de mineurs, car les seuls frais qui seront gagnés viendront des transactions. Ces frais de transactions vont également diminuer due à la concurrence d'autres systèmes similaires. La diminution du nombre de mineurs rend l'écosystème blockchain vulnérable à l'attaque du 51% . Cette dernière se produit lorsqu'un mineur malicieux (ou un pool de mineurs malicieux) contrôlent 51%, ou plus, de la puissance de calcul du réseau. Ainsi, il peut créer des blocs de transactions frauduleux pour lui-même, ou pour une autre entité, tout en invalidant les transactions des autres utilisateurs dans le réseau. Enfin, dans certains mécanismes de consensus, tel que celui de la chaîne la plus longue (longest chain) appliqué dans Bitcoin(voirsection4.2pageci-contre), de nombreux mineurs qui valident des blocs et réalisent la PoW ne sont pas récompensés, car ils n'ont pas assez de puissance pour construire la chaîne la plus longue, ce qui leur cause beaucoup de pertes. La PoW représente la méthode de validation de bloc la plus adoptée par les systèmes blockchain.

Le concept du l'algorithme le plus utilisé dans la Blockchain existait bien avant sa naissance. Il a été publié à l'origine par Cynthia Dwork et Moni Naor en 1993, mais le terme «preuve de travail» a été inventé par Markus Jakobsson et Ari Juels dans un document publié en 1999 (Blockgeeks, 2017). Dans le cas de Bitcoin, la preuve de travail suppose que tous les membres du réseau votent en utilisant leur puissance de calcul en résolvant le PoW et la construction et la validation du bloc. La preuve de travail peut être considérée comme le principal composant afin de définir un calcul informatique coûteux, également appelé extraction qui doit être effectuée afin de générer un nouveau bloc.

Les mineurs servent à deux fins : vérifier la légitimité d'une transaction et éviter les doubles dépenses.

3.3.2 Proof of Stake

Afin de résoudre les lacunes de la PoW (Preuve de Travail), la PoS (Preuve d'Enjeu) a été proposée. Dans ce mécanisme il n'y a pas de minage où on consomme beaucoup de ressources. Les mineurs sont appelés forgeurs. Un forgeur peut valider des blocs en fonction de la quantité d'argent qu'il possède. Ce qui signifie que plus il possède de monnaies, plus il augmente sa chance de validation. Si on compare la PoS à un jeu de pari, où chaque forgeur parie sur un bloc. On peut dire qu'une fois que les blocs honnêtes (ne contiennent aucune transaction frauduleuse) sont ajoutés à la chaîne, chaque forgeur touche une récompense relative à son pari. Et contrairement à la PoW où les mineurs malicieux sont pardonnés,dans la PoS un forgeur dont le bloc s'avère malhonnête est pénalisé et le montant du pari qu'il a mis est débité de son solde. Le point faible de la PoS est que les forgeurs qui possèdent beaucoup de monnaies sont ceux qui bénéficient le plus. Il existe plusieurs systèmes blockchain qui utilisent la PoS, et d'autres qui replacent la PoW par la PoS.

Il existe d'autres mécanismes de validation de blocs tel que la Delegated Proof-of-Stake (DPoS), la Proof of Stake/Time (PoST), la Proof of Existence (PoE), etc.

3.3.3 Delegated Proof of Stake (DPoS)

La principale différence entre les PoS et les DPoS réside dans le fait que les PoS sont un processus démocratique direct, tandis que le DPoS est démocratiquement représentatif – les parties prenantes élisent des délégués pour générer et valider un bloc. Avec beaucoup moins de nœuds pour valider le bloc, le bloc peut être confirmé rapidement, ce qui signifie que la transaction peut être confirmée rapidement (Zheng, 2016) et (Kikitamara, 2017)

3.3.4 Practical Byzantine Fault Tolerance (PBFT)

Cet algorithme de consensus a été développé pour tolérer les fautes byzantines, par exemple le comportement arbitraire du nœud, qui rejoint et quitte le réseau à tout moment qui se produit généralement dans un système distribué. Cet algorithme présente une technique de réplication de machine à états permettant de gérer les erreurs byzantines. Théoriquement, il utilise un algorithme de réplication de la machine d'état avec un seul aller-retour de message pour exécuter des opérations en lecture seule et deux pour exécuter des opérations de lecture-écriture. En outre, il utilise un schéma d'authentification efficace basé sur les codes d'authentification du message en cours de fonctionnement normal ; la cryptographie à clé publique est utilisée

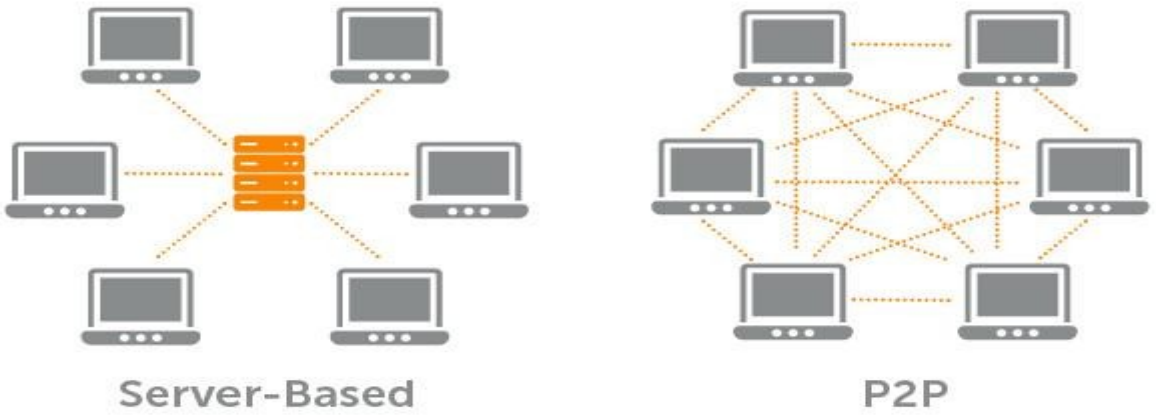
uniquement lorsqu'il y a des erreurs (Castro et Liskov, 1999).

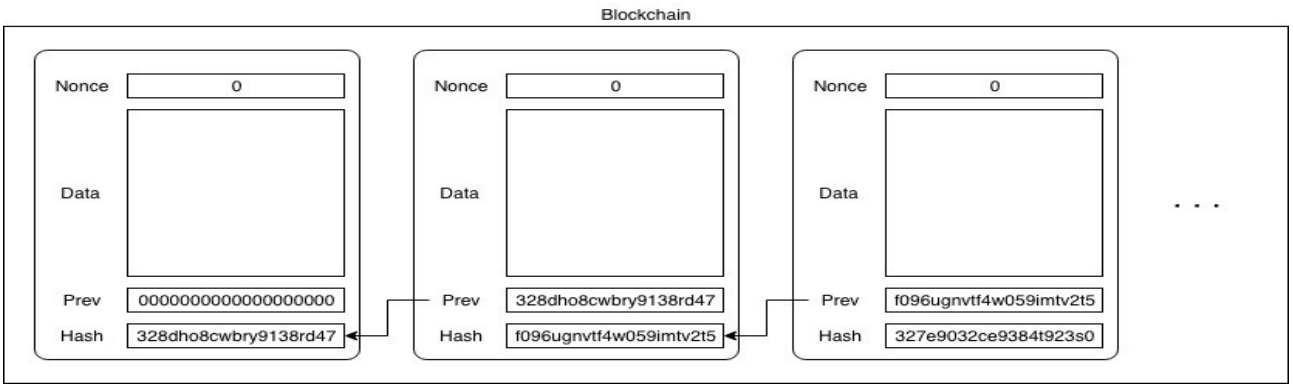
2.3 Architecture de la Blockchain

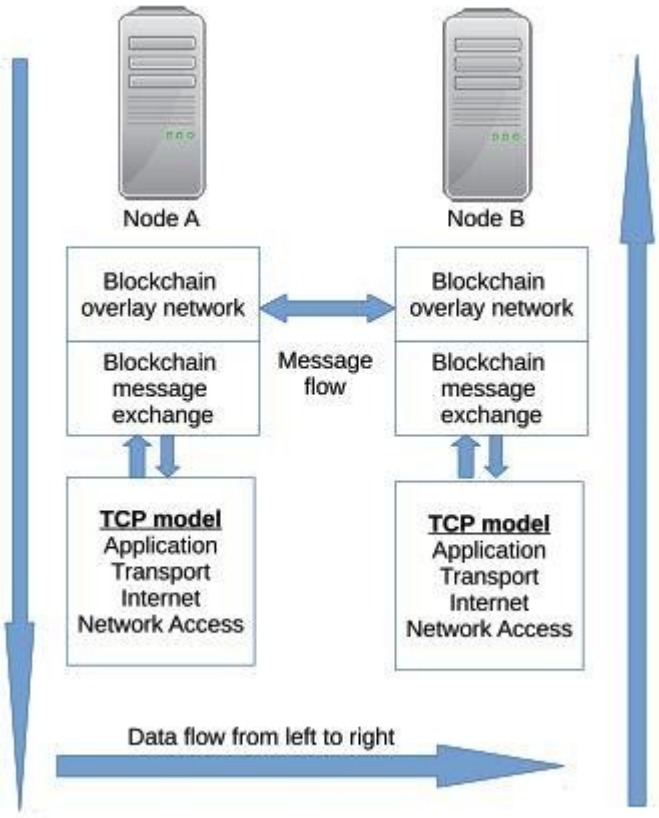
L'architecture réseau d'un réseau distribué Blockchain est Peer to Peer, Le réseau d'égal à égal, également appelé P2P, fait référence à un groupe d'ordinateurs agissant en tant que nœuds pour partager des fichiers entre eux-mêmes.

La Blockchain fonctionne donc sur un réseau distribué de serveurs, également appelé nœuds. Ces nœuds du réseau ont pour objectif de fournir un consensus sur l'état de la blockchain à tout moment, et contiennent une copie de la blockchain.

L'application fondamentale de la Blockchain est un grand livre de transactions, un peu comme un grand livre public sécurisé, qui stocke toutes les transactions qui ont lieu dans le réseau. Cela en fait un système décentralisé très sécurisé et transparent.







2.4 Fonctionnement de la Blockchain

Les interactions entre les comptes d'un réseau blockchain sont appelées "transactions". Il peut s'agir de transactions monétaires, comme l'envoi d'éther, la crypto-monnaie utilisée dans Ethereum. Elles peuvent également être des transmissions de données, comme un commentaire ou un nom d'utilisateur. Un ensemble de transactions est appelé un "bloc".

Chaque compte sur la blockchain possède une signature unique, qui permet à chacun de savoir quel compte a initié la transaction. Sur une blockchain publique, tout le monde peut lire ou écrire des données. La lecture des données est gratuite, mais l'écriture sur la blockchain publique est payante. Ce coût, appelé "gaz" et fixé en éther, contribue à décourager le spam et à sécuriser le réseau.

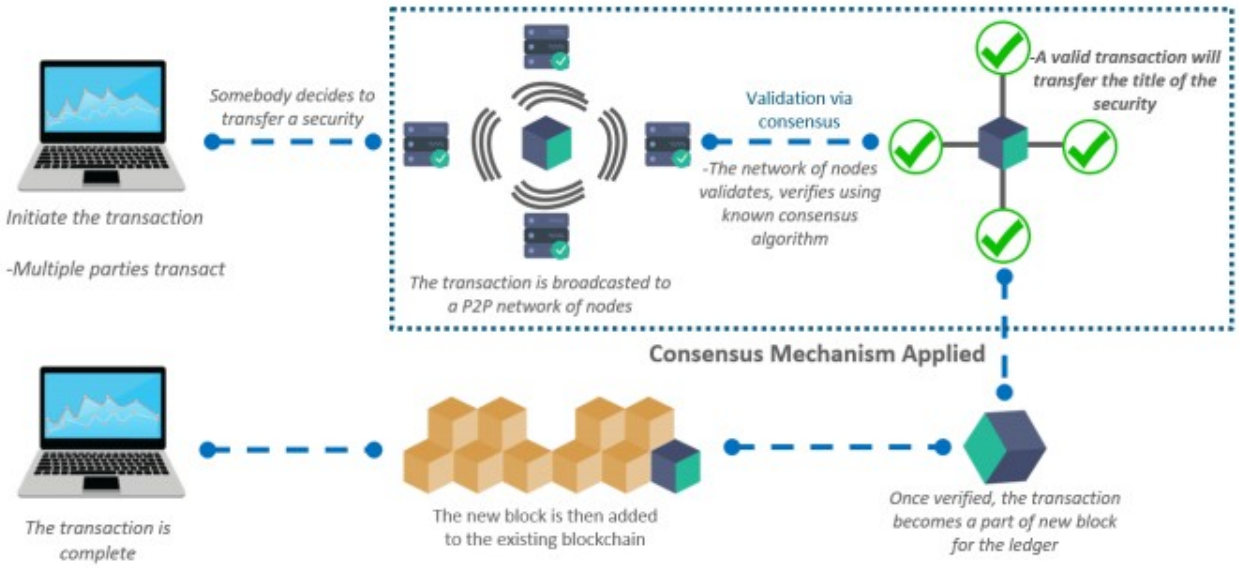


Figure XX : Les étapes sur un réseau Blockchain

La figure XX illustre le mécanisme de fonctionnement des transactions dans le réseau Blockchain.

Les étapes de ce mécanisme sont les suivantes :

- ➔ Quelqu'un demande une transaction.
- ➔ La transaction est diffusée sur un réseau P2P public (réseau Blockchain) composé de plusieurs nœuds.
- ➔ Le réseau de nœuds valide la transaction en utilisant les algorithmes de hachage.
- ➔ Une fois vérifiée, la transaction est combinée avec d'autres transactions pour créer un nouveau bloc de données pour le grand livre.
- ➔ Le nouveau bloc est ajouté à la chaîne de blocs existante, sous une forme qui est permanente et inaltérable.
- ➔ Enfin la transaction sera effectuée avec succès.

3.7 Définitions autour de la technologie Blockchain

Dans cette section, On explique les principaux concepts liés à la technologie Blockchain et son fonctionnement. Ces concepts sont : Nœuds, peer to peer (P2P), DLT (Distributed Ledger Technologies), Transactions, Blocs, Hachage , Merkle tree, Minage, Consensus, Attaque 51%, Ether, Dapp, Gas.

Les nœuds ou les clients connectés au réseau dans le système Blockchain constituent une partie essentielle du système. Ils prennent en charge diverses fonctions telles que le routage, l'extraction, le stockage des données de la blockchain et leur utilisation en tant que portefeuille. Tous les nœuds participent à la vérification et à la propagation des transactions et sont activés avec des fonctionnalités telles que la découverte et le maintien de la connexion avec leurs pairs. Ils conservent également une copie du registre, ou de la blockchain, qui contient des données sur toutes les

transactions qui se sont déjà produites, éliminant ainsi la nécessité de disposer d'un serveur centralisé pour le stocker. Les nœuds peuvent également agir en tant que mineurs et aider à vérifier et valider toutes les transactions effectuées par tous les utilisateurs. Tous les mineurs sont des nœuds, mais tous les nœuds ne sont pas nécessairement des mineurs. Les nœuds sont principalement de trois types, à savoir les nœuds complets, les clients SPV (Simple Paiement Verification) et les clients Web.

Les clients Web, généralement appelés portefeuilles, sont stockés sur des serveurs tiers et sont accessibles via les navigateurs Web.

Les nœuds SPV incluent généralement des clients ne disposant pas de capacités matérielles suffisantes, telles que des périphériques mobiles, ou de périphériques plus limités, tels que des systèmes intégrés. Ces nœuds SPV n'ont pas besoin de stocker une copie de toutes les transactions dans la blockchain, mais uniquement les en-têtes de bloc. Ces nœuds ont un moyen légèrement différent de vérifier les transactions des nœuds complets, car ils ne gardent pas une trace de toutes les transactions se déroulant sur la blockchain. Ils dépendent de leurs nœuds homologues pour fournir les informations de transaction dont ils ont besoin, à la demande.

Les nœuds complets, en revanche, sont les nœuds qui stockent une copie à jour de la chaîne de blocs dans son intégralité.

Une fois que l'un des nœuds est connecté au réseau local sans fil, le système recherche d'autres pairs auxquels se connecter, sur un port particulier via TCP. Ce processus de découverte de nœud est également appelé protocole de découverte.

P2P (Peer to Peer) est un réseau dans lequel les ordinateurs servent de nœuds pour le partage de fichiers au sein du groupe. Les périphériques ou ordinateurs participant à ce réseau sont appelés Pairs. Chaque pair est égal à une autre. Il n'existe donc aucun périphérique administrateur central au centre du réseau ni une partie privilégiée.

DLT (Distributed Ledger Technology) est un type de base de données consensuel partagé, répliqué et synchronisé sur les membres d'un réseau. La principale caractéristique de cette base de données est que les transactions et leurs détails sont enregistrés simultanément à plusieurs endroits. DLT n'a pas de magasin de données central.

Les transactions sont stockées dans les fichiers appelés blocs. Ils sont cryptés et sont généralement liés à des transactions précédentes, formant ainsi une chaîne. Un propriétaire d’une valeur (devise numérique dans BC Bitcoin) signe numériquement la transaction précédente avec sa clé publique et crée un hachage. Le propriétaire de la transaction précédente signe alors le hachage avec sa clé privée.

La figure XX illustre une version simplifiée de la chaîne de propriété. Dans des cas plus complexes, le nombre d'entrées et des sorties peuvent être multiples. Une transaction contient un certain nombre de champs, comme indiqué dans le tableau 6.

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1-9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1-9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

Tableau 6 : Champs dans une transaction

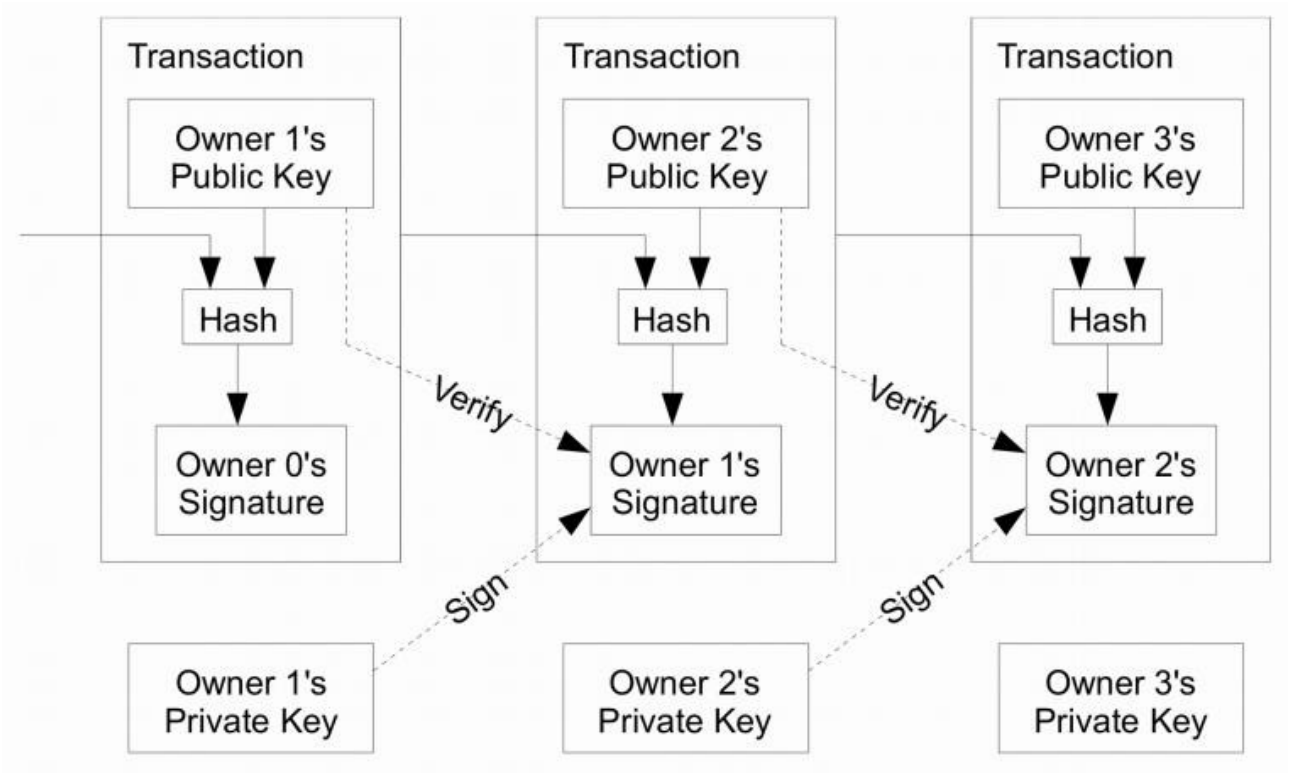


Figure XX : Chaîne de propriété de transaction

Dans BC Bitcoin la transaction est un transfert de valeur Bitcoin qui diffuse sur le réseau et est collecté en blocs. Les transactions ne sont pas cryptées. Il est donc possible d'afficher chaque transaction collectée dans un bloc. Elles sont regroupées en blocs et exécutées sur tous les nœuds participants.

Un bloc contient une liste de transactions, l'état le plus récent, un numéro de bloc et une valeur de difficulté. S'il existe des transactions en conflit sur le réseau (par exemple, des transactions qui doublent les dépenses), une seule d'entre elles est sélectionnée pour faire partie du bloc. Les blocs sont ajoutés à la Blockchain à intervalles régulières.

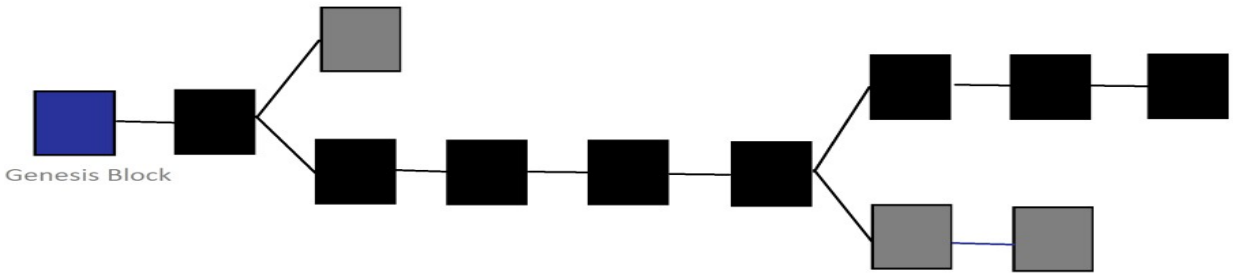


Figure xx : Blocs dans la Blockchain

La figure 36 illustre les liens entre les blocs de la chaîne de blocs. Les blocs marqués en noir indiquent la blockchain active en cours. Ceux qui sont marqués en gris sont appelés des blocs rassis.

La Blockchain est techniquement une liste de blocs ordonnée et horodatée, qui fournit un enregistrement de toutes les transactions qui ont eu lieu. Chacun de ces blocs est lié au précédent, à savoir son parent, par un hachage unique. Ces hachages sont générés via l'algorithme de hachage SHA256. En d'autres termes, l'en-tête de chaque bloc contient une référence au hachage de son parent. Cette liaison se poursuit jusqu'au premier bloc de la blockchain, également appelé bloc de genèse. Le bloc de genèse est le bloc bleu le plus à gauche indiqué à la figure 8. Un bloc peut avoir plusieurs enfants simultanément. Chaque enfant fait référence au hachage du même bloc parent. En fin de compte, l'un de ces blocs enfants devient la partie de la blockchain principale. Ce phénomène est connu sous le nom de forking. Cela se produit lorsque plusieurs mineurs extraient et vérifient différents blocs au même moment. La blockchain est également appelée immuable car c'est une dépense astronomique de recalculer les hachages de tous les blocs à partir du bloc de genèse.

Le tableau 7 décrit plus en détail la structure de l'entête du bloc, en expliquant les différents types de métadonnées associées aux blocs

Size(bytes)	**Field**	**Description**
4	Version	Software version
32	Previous Block Hash	Reference to hash of the previous block
32	Merkle Root	Hash of the root of the merkle tree containing all the transactions included in the block
4	Timestamp	Approximate time when the block was created
4	Difficulty Target	Proof of work difficulty for the block
4	Nonce	Proof of work counter

Tableau 7 : Structure de l'entête d'un bloc

Le champ racine merkle fait référence à la racine d'un arbre à distorsion qui stocke les informations de transaction dans chaque bloc.

Puisque l'entête de bloc fait partie du bloc, un bloc complet, y compris toutes les informations de transaction, a une taille beaucoup plus grande qu'un en-tête de bloc. C'est la raison pour laquelle les clients et les portefeuilles SPV téléchargent uniquement les fichiers d'en-tête de la blockchain tout

en récupérant les informations de leur bloc souhaité des nœuds complets connectés au réseau. Le tableau 8 décrit les différents champs d'un bloc, ainsi que leur taille.

Size (bytes)	Field	Description
4	Block Size	The size of the block
80	Block Header	Consists of several fields, as shown in Table 3
1-9	Transaction Counter	Number of transactions included in the block
Variable	Transactions	Recorded transactions included in the block

Tableau 8 : Structure d'un bloc

Le hachage précédent (hachage du bloc précédent) est présent pour assurer un lien entre les blocs. Chaque bloc peut être identifié de manière unique par son hachage de bloc qui est généré à partir des quatre paramètres de l'en-tête de bloc (voir diagramme). Maintenant, puisqu'il s'agit d'un réseau d'égal à égal, chaque homologue peut ne pas recevoir les transactions dans le même ordre. Donc, en fonction de leur arrangement de transactions, le hachage de bloc pourrait être différent. Un seul de ces blocs peut être ajouté à la blockchain car un seul enregistrement d'une transaction peut exister. En outre, chaque pair ne peut pas avoir sa propre version d'un bloc car cela met tout le système en jeu. Il devrait donc y avoir un moyen pour tous les pairs de s'accorder sur un bloc unique comme valide, de sorte que seul ce bloc soit ajouté à la blockchain. Pour atteindre ce consensus, le bitcoin a pour règle que le hachage de bloc doit avoir un certain non. des zéros non significatifs. Ainsi, tous les nœuds ont trois entrées: le hachage précédent (Prev_Hash), l'horodatage et la racine de la transaction (Tx_Root). Ils savent également que la sortie doit être dans un certain format. Maintenant, ils continuent à ajouter une valeur de nonce aléatoire aux entrées jusqu'à ce qu'elles parviennent à un hachage cible. En raison de la nature de la fonction de hachage, il est impossible de deviner cette valeur de nonce. Le seul processus permettant de le savoir consiste à utiliser la méthode des essais et des erreurs. La difficulté est exponentiellement proportionnelle au no. des zéros au début du bloc. Cette valeur nonce est très difficile à trouver et nécessite souvent d'effectuer des milliards de hachages. Ce processus n'est pas économe en énergie et nécessite du matériel spécial avec une énorme capacité de calcul. Une fois que cette valeur de nonce est trouvée, le nœud diffuse l'ensemble du bloc vers le réseau et il est très facile pour les autres nœuds de vérifier s'il s'agit du nonce correct. Cette valeur de nonce prouve qu'un nœud a effectué un travail considérable avant de générer un bloc, d'où le nom Preuve de travail.

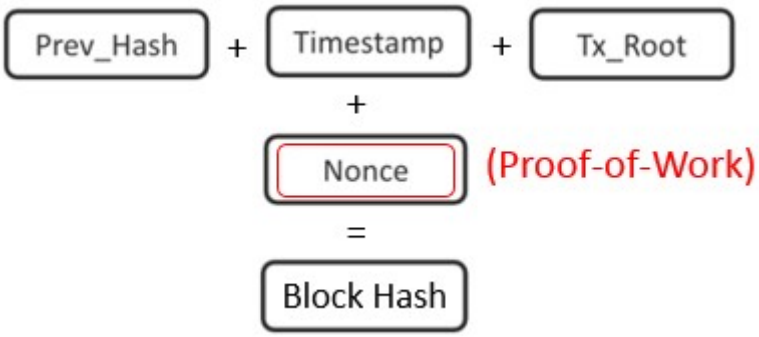


Figure 37 : Contenus d'un hachage de Bloc

Après vérification, ce bloc est ajouté à la blockchain et tous les nœuds commencent à travailler sur le prochain ensemble de transactions.

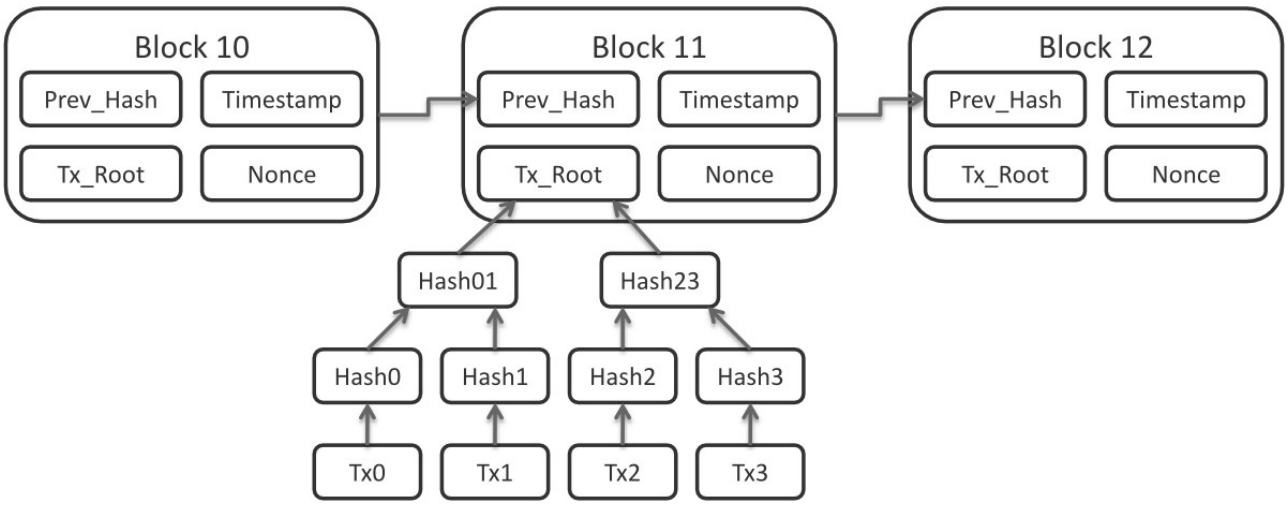


Figure 38 : Preuve de Travail

Ce mécanisme de preuve de travail est ce qui rend la blockchain immuable. Imaginons un scénario dans lequel un pirate informatique voudrait supprimer une transaction (Tx1) du bloc 11, comme indiqué dans le diagramme ci-dessus. Ici, tous les autres nœuds travaillent sur la génération du bloc 13. Ainsi, si le pirate informatique souhaite supprimer Tx1, la racine Tx_Root du bloc 11 change et la valeur de nonce précédente n'est plus valide. Le pirate informatique doit effectuer à nouveau ces milliards de calculs et découvrir une nouvelle valeur de nonce. Etant donné que le hachage du bloc 11 (Prev_Hash) est également utilisé lors du calcul du hachage du bloc 12, le processus complet doit être répété pour rechercher une nouvelle valeur de nonce pour le bloc 12. Il ne s'arrête pas là car le pirate doit également créer un bloc 13 avant tout autre nœud, car tous les nœuds suivent toujours la chaîne la plus longue puisqu'il s'agit de la chaîne dans laquelle la majorité de la puissance du processeur est investie. En bref, un seul nœud doit modifier 2 blocs et créer un nouveau bloc tandis que tous les autres nœuds tentent de générer ce nouveau bloc uniquement. Ainsi, il est impossible pour un pirate informatique de modifier les données présentes sur la blockchain. L'ensemble de ce mécanisme de validation de travail et de génération de blocs maintient la chaîne de blocs sécurisée, transparente et immuable.

Hachage est l'équivalent du concept d'empreinte digitale, c'est l'identifiant unique d'une personne. Lorsque deux objets sont envoyés à la Blockchain, ils ont des hachages différents. De plus, si vous avez l'objet, il est très facile de créer le hachage, mais il est presque impossible d'effectuer l'opération inverse. Pour s'assurer que l'inverse n'existe pas, la sortie est plus courte que les entrées et il y a plus de deux entrées qui donnent la même sortie. Ce mode de fonctionnement rend impossible le calcul de l'inverse.

Hachage du bloc et sa hauteur Il y a deux façons d'identifier un bloc ; Tout d'abord, par son hash. Ce hachage est calculé par les nœuds homologues du réseau chaque fois qu'un bloc est généré. Le hachage pourrait être stocké dans une base de données incluse dans les métadonnées du bloc pour une indexation et une récupération plus rapide des blocs du disque.

La deuxième façon d'identifier un bloc serait par sa hauteur. Le bloc de genèse est à la hauteur 0. Cette méthode d'identification n'est pas absolue car deux blocs ou plus de la chaîne de blocs peuvent

avoir la même hauteur et il est également possible que deux blocs de même hauteur aient le même parent.

Merkle Tree Un type spécial de structure de stockage de données basé sur des fonctions de hachage est appelé arbre de Merkle :

- Il est structuré comme un arbre binaire ; les feuilles contiennent les valeurs à stocker et chaque nœud interne est le hachage de ses deux enfants.
- Il fournit des recherches efficaces et une protection contre la falsification, car la vérification d'une transaction est incluse dans l'arborescence. Peut être accompli en envoyant uniquement la transaction, le hachage contenu dans chaque nœud entre le nœud feuille de transaction et la racine, ainsi que les valeurs de hachage utilisées pour créer chaque hachage envoyé.
- La recherche d'une transaction dans une arborescence Merkle à trois niveaux inclut l'envoi de deux transactions (celle souhaitée et l'autre enfant de son parent) et de trois hachages (le parent de la transaction, la racine et l'autre enfant de la racine).

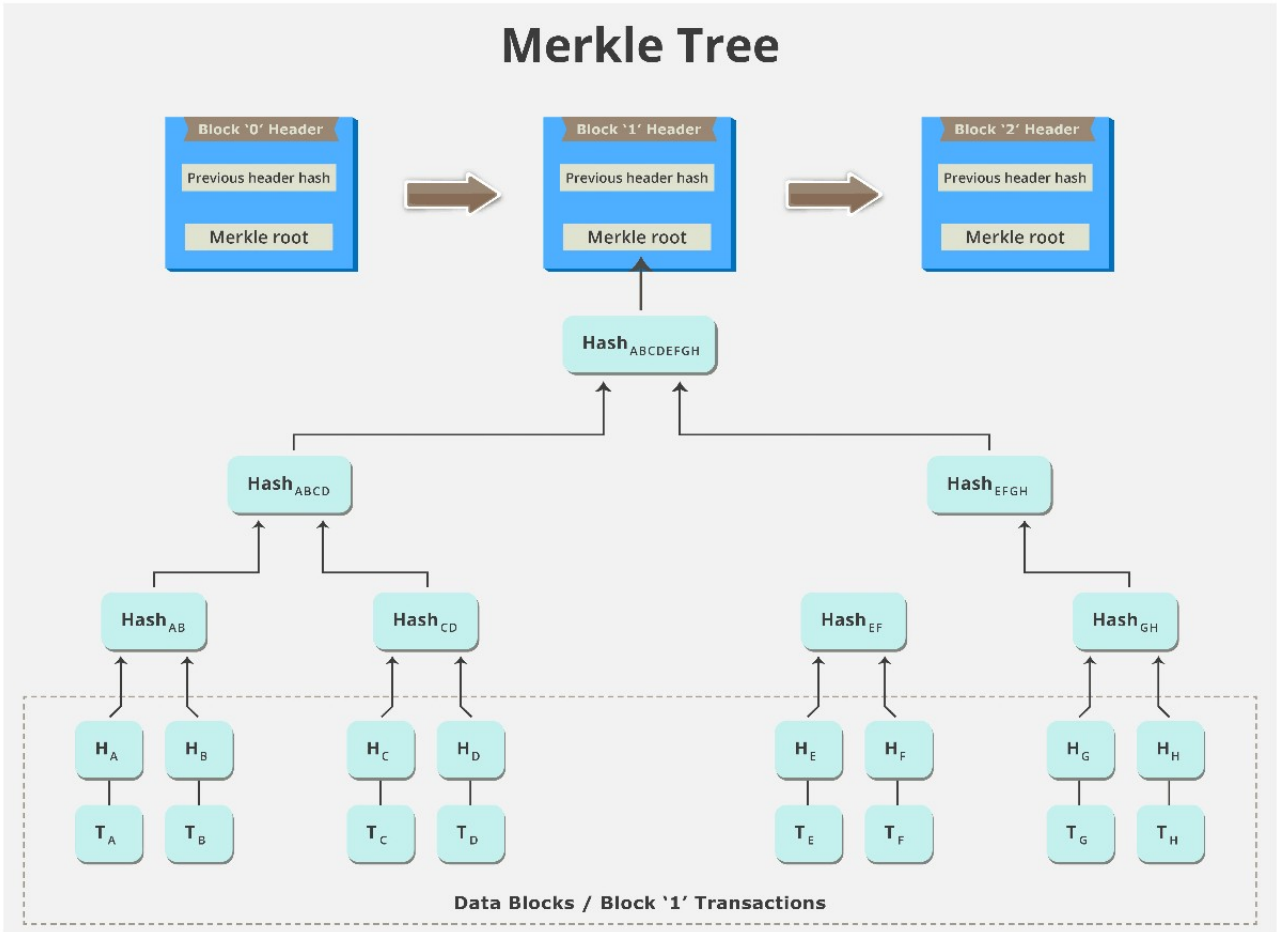


Figure 39 : Arbre de Merkel

Minage qui fait référence au processus de revue de calcul distribué effectué sur chaque "bloc" de données dans une chaîne de blocs. Cela permet de parvenir à un consensus dans un environnement où personne ne se connaît.

- L'extraction minière présente deux avantages majeurs :

Le réseau de chaînes de blocs, à savoir la validation et la vérification des transactions. L'exploitation génère également de nouvelles pièces de monnaie numériques sur le réseau, car ces pièces nouvellement frappées servent de récompense au mineur qui résout le prochain bloc de la blockchain. La première étape de l'extraction consiste à calculer le niveau de difficulté de la blockchain. Tous les nœuds complets connectés au réseau de chaînes de blocs recalculent ce niveau de difficulté après certains intervalles. Le niveau peut augmenter ou diminuer en fonction du temps nécessaire pour générer un certain intervalle de blocs. Dans le cas de Bitcoins, qui était la première implémentation de blockchains, l'intervalle est de 2016 blocs. Ainsi, les nœuds complets doivent réévaluer le niveau de difficulté après chaque bloc 2016, ce qui donne un temps de consensus moyen de 10 minutes. À mesure que le nombre de mineurs augmente, le taux de création de blocs augmente également. Ceci entraîne à son tour une augmentation du niveau de difficulté, car il réduit le taux de création de blocs à 10 minutes, dans le cas de Bitcoin. Le mineur télécharge ensuite toutes les transactions et les informations de blocage qui se sont déroulées précédemment, et construit un chemin de merkle à partir de celles-ci, générant finalement une racine de mot clé.

Mécanisme de consensus

Le consensus est un problème fondamental dans les systèmes distribués qui nécessite que deux agents ou plus se mettent d'accord sur une valeur donnée nécessaire à des fins de calcul. Certains de ces agents peuvent être peu fiables, et le processus de consensus doit donc être dépendant. Ainsi, la nécessité de mécanismes de consensus est de faciliter la mise à jour sécurisée d'un processus ou d'un état, conformément à certaines règles de transition d'état, dans lesquelles un ensemble distribué a le droit d'effectuer les transitions d'état.

Un consensus est un processus qui permet à un ensemble de processus répartis de parvenir à un accord sur une valeur ou une action en dépit d'un certain nombre de processus défaillants (Correia, 2011). Blockchain nécessite vérification et acceptation par tous les membres du réseau, généralement appelée consensus.

Pour parvenir à un consensus dans le mécanisme distribué, quatre algorithmes peuvent être appliqués. Dans un réseau de blockchain, un consensus est utilisé pour éviter que des acteurs mensongers ne provoquent informations potentiellement non valides dans la base de données (Swanson, 2015).

Le mécanisme de consensus concret utilisé pour une blockchain donnée dépend d'un certain nombre de y compris le degré de confiance entre les parties et l'alignement de leurs intrigues, ainsi que en tant que facteurs concernant la forme et la synchronisation du réseau (Correia, 2011).

Attaque 51%

Outre le fait que l'algorithme de preuve de travail consomme beaucoup d'énergie, il présente un autre inconvénient : l'attaque à 51%. Si une seule entité devait contribuer à plus de 51% des activités du réseau Bitcoin, elle serait en mesure de contrôler totalement le réseau et de modifier le grand livre en fonction de leurs besoins. Bien que cette attaque soit théoriquement possible, elle coûterait aux mineurs une énorme somme d'argent ainsi que de la puissance de calcul

Ether est la devise utilisée dans le réseau Ethereum. Contrairement aux bitcoins, les éthers n'ont pas été créés pour devenir une monnaie numérique mondiale décentralisée et leurs aspirations vont au-delà de l'envoi ou du transfert d'argent.

Gas est le nom du carburant crypté utilisé pour effectuer les opérations sur un réseau Blockchain Ethereum. Le prix du gas payé est proportionnel à la quantité de travail requise pour exécuter la transaction.

Dapp (application décentralisée) est une application qui fournit une interface aux contrats intelligents. Un exemple de Dapp pourrait être une application crypto-devise.

2.8 Types de la Blockchain

La blockchain peut être ”avec permission” (privée) ou ”sans permission” (publique). La première catégorie impose des restrictions aux contributeurs du consensus. Seul ceux de confiances et choisis qui ont le droit de valider des transactions. Elle ne nécessite pas beaucoup de calcul pour atteindre un consensus, ainsi, elle est économique en termes de temps d'exécution et en énergie. Généralement les transactions sont privées et ne sont accessibles que par les objets autorisés. La deuxième catégorie (blockchain publique) utilise un nombre illimité d'objets anonymes. En se basant sur la cryptographie, chaque acteur peut communiquer d'une manière sécurisée. Chaque objet est représenté par une paire de clés (publique/privée), et a le droit de lire, d'écrire et de valider des transactions dans la blockchain. La blockchain est sûre si 51% des objets (ou plus) sont honnêtes et lorsque le consensus du réseau est atteint. Généralement, les blockchains sans permission consomment beaucoup d'énergie et de temps, car elles exigent un montant de calcul pour renforcer la sécurité du système (ex. en utilisant la PoW).

Il existe trois types de Blockchain, selon leur mode de fonctionnement :

- **Blockchain public :** Tout le monde peut lire ou écrire des données et la seule condition est de disposer d'un ordinateur et d'une connexion Internet. Une partie de ce type de réseau restreint l'accès uniquement en lecture ou en écriture. Ethreum et Bitcoin sont des exemples qui utilisent une approche où tout le monde peut écrire.
- **Blockchain privée :** N'est pas ouvert au public, mais est accessible uniquement sur invitation et tous les membres participants se connaissent et se font confiance. Ceci est très utile lorsque la Blockchain est utilisée entre entreprises appartenant à la même branche. Parmi les plus célèbres, citons Hyperledger (de Linux Foundation) et Ripple (protocole permettant les transferts internationaux).
- **Blockchain permissionnée :** Aussi connu sous le nom de Consortium Blockchain, est un hybride entre Blockchain publique et privée. Dans ce type, seuls quelques nœuds sélectionnés sont prédéterminés et les nœuds participants sont invités, mais toutes les transactions sont publiques. Cela signifie que les nœuds participent à la maintenance et à la sécurité de ce réseau, mais que toutes les transactions sont visibles pour les utilisateurs du monde entier. Le droit de lecture peut être public ou limité aux participants. Les Blockchains du consortium préservent la confidentialité des données, comme les Blockchains privés. BigchainDB est un exemple de consortium Blockchain.

3.11 Avantages de la technologie Blockchain

Les chaînes de blocs peuvent renforcer la sécurité principalement sur trois aspects :le blocage du vol d'identité, la prévention de la manipulation des données et l'arrêt des attaques par déni de service .

Blocage de vol d'identité

La structure de la preuve de travail du mineur de réseau de Blockchain et son grand livre distribué de transactions de données réduisent les risques de vol et de corruption des données.

Prévenir la manipulation et la fraude des données

Dans la technologie Blockchain, la cryptographie, le hachage et une structure décentralisée empêchent quasiment tout membre de modifier les données du grand livre. Cela empêche et détecte toute forme de manipulation et permet aux organisations de maintenir la protection des informations. Une solution importante qui a été développée pour éviter la fraude et la manipulation est KSI (Keyless Signature Infrastructure), qui assure la protection des réseaux ainsi que la sécurité et la confidentialité des données.

Avec KSI, personne ne peut manipuler les données et l'authenticité des données électroniques peut être prouvée mathématiquement. KSI stocke les signatures numériques des fichiers originaux dans une Blockchain, puis vérifie les copies en revérifiant les signatures des copies par rapport à celles stockées dans la Blockchain. Si une quelconque manipulation est effectuée, elle est détectée très rapidement car les hachages stockés dans la chaîne de caractères résident dans des milliers de nœuds. KSI Technology est utilisée activement dans les secteurs de l'aérospatiale et de la défense, ainsi que dans le secteur de la santé, afin de mieux contrôler le dossier médical du patient.

Prévention des attaques par déni de service distribué

Il existe un grand nombre d'infrastructures critiques à protéger. Blockchain peut aider avec DNS (Domain Name System) qui fournit un accès à des sites Web utilisant des noms de domaine plutôt que des adresses IP. Le système DNS est dangereusement centralisé dans quelques serveurs racine sous le contrôle de l'ICANN (Internet Corporation for Assigned Names and Numbers), qui est responsable des adresses de protocole IP, des identificateurs de protocole, des fonctions de gestion de système de domaine et de la gestion de système du serveur racine. Blockchain pourrait créer un DNS distribué, beaucoup plus transparent, rendant pratiquement impossible la manipulation des enregistrements par une seule entité.

Il existe certaines différences entre les réseaux Blockchain et le paradigme du Cloud Computing. Dans le modèle en nuage, les périphériques IoT sont identifiés, authentifiés et connectés via des serveurs en nuage, où le traitement et le stockage sont souvent effectués. Les réseaux IoT ayant des coûts élevés sont concernés par le modèle de cloud centralisé. Les appareils IoT sont vulnérables aux attaques DDoS, au vol de données, au piratage et au piratage à distance. Si un périphérique IoT connecté à un serveur fait l'objet d'une violation, toutes les personnes connectées au serveur pourraient être affectées. En outre, le modèle de nuage centralisé est sujet à la manipulation. Les données collectées ne garantissent pas que les informations sont utilisées de manière appropriée. Blockchain peut éliminer ces problèmes de Cloud Computing. Dans Blockchain, les échanges de messages entre périphériques peuvent être traités de la même manière que les transactions financières dans un réseau bitcoin. Les appareils reposent sur des contrats intelligents qui

garantissent plus de sécurité. Le fait que Blockchain vérifie de manière cryptographique les transactions signées, elle élimine la possibilité d'attaque par interférence, de rejeu ou d'autres attaques.

3.1 Défis de la Blockchain

La blockchain est une technologie émergente qui se répand dans divers secteurs et qui présente un grand nombre d'avantages et d'opportunités. Cependant, cette technologie présente son propre ensemble de défis à relever (voir figure 43). Quelques-uns de ces défis majeurs sont abordés dans cette section.

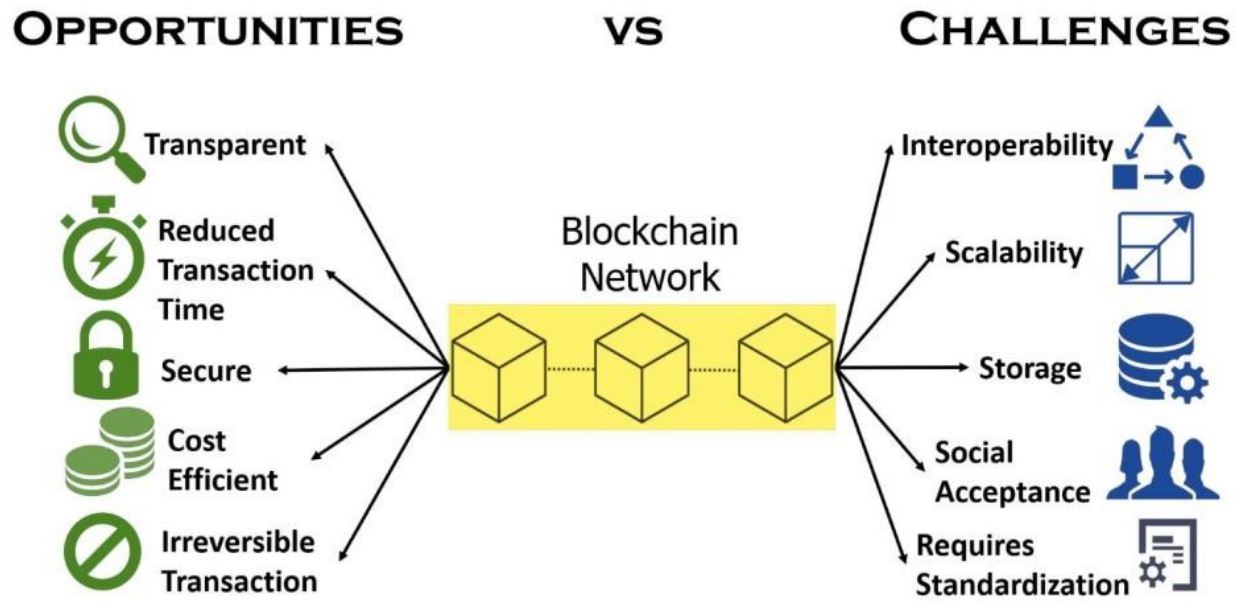


Figure 43 : Opportunités et défis des blockchains.

Sécurité et confidentialité des données

Le premier et le plus important défi concerne la sécurité et la confidentialité des données. Avec la mise en œuvre d'applications basées sur la technologie de la blockchain, la nécessité pour un tiers d'effectuer une transaction est éliminée. Étant donné que le mécanisme de blockchain permet à l'ensemble de la communauté, plutôt qu'à un seul tiers de confiance, de vérifier les enregistrements dans une architecture de blockchain, les données sont exposées à des risques potentiels en matière de sécurité et de confidentialité. Étant donné que tous les nœuds peuvent accéder aux données transmises par un nœud, la confidentialité des données ne sera pas active. En cas d'absence d'une tierce partie pour autorisation, le patient doit sélectionner un ou plusieurs représentants qui peuvent accéder à ses informations et / ou à ses antécédents médicaux en son nom, en cas d'urgence. Désormais, ce représentant peut également autoriser un ensemble de personnes à accéder aux enregistrements du même patient, ce qui peut créer une menace énorme pour la sécurité et la confidentialité des données. L'implication de mécanismes de haute sécurité dans les données entraînera à son tour des obstacles pour le transfert des données d'un bloc à un autre et, par conséquent, les destinataires auront accès à des données limitées ou incomplètes. En outre, les réseaux blockchain sont sujets à une sorte de violation de la sécurité connu sous le nom d'attaque 51%. Cette attaque implique une équipe de mineurs qui possèdent plus de 50% des blocs d'un réseau

blockchain. Les mineurs obtiennent une autorité du réseau et pourraient empêcher toute nouvelle transaction en ne leur donnant pas leur consentement. Cinq crypto- monnaies ont récemment été victimes de cette attaque. En outre, un dossier patient peut contenir des données sensibles qui ne conviennent pas pour figurer dans la chaîne de blocs.

Gestion de la capacité de stockage

Un autre défi qui apparaît sur ce front est la gestion de la capacité de stockage. La Blockchain a été conçue pour enregistrer et traiter les données de transaction, qui ont une portée limitée, de sorte qu'elle n'a pas besoin de beaucoup de stockage. Avec le temps, au fur et à mesure de son expansion dans le domaine de la santé, les défis du stockage devinrent évidents. Le secteur de la santé contient une grande quantité de données qui doivent être traitées quotidiennement. Des dossiers des patients aux antécédents médicaux, en passant par les rapports de test, en passant par les analyses IRM, les rayons X et autres images médicales, toutes les données du scénario de la blockchain seront disponibles pour tous les nœuds de la chaîne, ce qui nécessite un espace de stockage considérable. De plus, les applications de la blockchain étant basées sur des transactions, les bases de données utilisées pour cette technologie ont tendance à se développer rapidement. En raison de la taille croissante des bases de données, la vitesse de recherche et d'accès à l'enregistrement devient lente, ce qui est tout à fait inadéquate pour les types de transactions pour lesquels la rapidité est essentielle. Par conséquent, une solution de chaîne de blocs doit être évolutive et résiliente.

Problèmes d'interopérabilité

La blockchain souffre également du problème de l'interopérabilité, c'est-à-dire que les chaînes de blocs de divers fournisseurs et services de communication communiquent entre elles de manière transparente et appropriée. Ce défi crée des obstacles au partage efficace des données.

Défis de la normalisation

La technologie de la blockchain en est encore à ses balbutiements et elle sera donc certainement confrontée à des problèmes de standardisation en vue de son application pratique en médecine et en soins de santé. Un certain nombre de normes bien authentifiées et certifiées seraient exigées des autorités internationales de normalisation. Ces normes prédéfinies seraient utiles pour évaluer la taille, la nature des données et le format des informations échangées dans les applications blockchain. Ces normes examineront non seulement les données partagées, mais devront également servir de mesures de sécurité préventives.

Défis sociaux

La technologie des chaînes de blocs évolue toujours et fait donc face à des défis sociaux, tels que le changement de culture, en plus des défis techniques susmentionnés. Accepter et adopter une technologie complètement différente des méthodes de travail traditionnelles n'est jamais chose facile. Bien que l'industrie médicale s'achemine lentement vers la numérisation, il lui reste encore beaucoup à faire pour passer complètement à cette technologie, en particulier celle comme la blockchain, qui n'a pas encore été validée sur le plan clinique. Il faudra du temps et des efforts pour convaincre les médecins de passer de la paperasserie à la technologie. En raison de son faible taux d'adoption dans le secteur de la santé, la technologie et les politiques proposées sont relativement

peu fiables. En raison de tous ces défis et menaces, nous ne pouvons pas, à ce jour, le qualifier de solution viable et universelle pour tous les problèmes de santé.

Conclusion

La technologie Blockchain est révolutionnaire. Elle va rendre la vie plus simple et plus sûre, en changeant la façon dont les informations personnelles sont stockées et dont les transactions de biens et de services sont effectuées.

Chapitre 3 Analyse et Conception

Introduction

La conception est l'étape principale dans le cycle de vie de création d'une application, elle a pour but de réaliser l'étude des données et les traitements à faire, elle aide également à réduire la complexité du système. C'est dans cette phase que s'appliquent les techniques de modélisation.

Dans ce chapitre, nous allons présenter les objectifs à atteindre de notre projet suivi d'une description générale de l'application, finalement nous allons présenter la modélisation de notre projet.

1. Description des besoins fonctionnels

1.1. Objectifs à atteindre

Notre travail doit accomplir certains buts. Ces buts peuvent être résumés dans ces points :

- Flux de trésorerie instantané
- Conversion automatique
- Acceptation de jetons inégalée

1.2. Description de l'application

L'application se compose de plusieurs espaces :

- **Index** : Contient une présentation de l'application et de tous les services présents.
- **Espace d'authentification :** L'utilisateur doit s'authentifier en utilisant un authentification Web3 ensuite il dispose d'un accès facile à ses informations.
- **Espace Overview :**
- **Espace Payments :**
- **Espace Integrations :**
- **Espace Documentations :**

2. Modélisation UML

2.1. Acteurs et leurs rôles

Dans notre application, nous envisageons trois acteurs qui sont :

Acteur	Rôle
Super Adm inistrateur (Super Admin)	

Payer	
Customers	

2.2. Diagrammes des cas d’utilisations

➔ Utilisateur : tous les acteurs héritent de l’acteur utilisateur