Republique Algerienne Democratiqueet Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientique
UNIVERSITE MOHAMMED SEDDIK BENYAHIA
JIJEL
FACULTE DE SCIENCES EXACTES ET D'INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

MEMOIRE DE MASTER

Présenté pour l'obtention du diplôme de :

MASTER

EN **INFORMATIQUE**

Option : INFORMATIQUE LÉGALE ET MULTIMEDIA

Thème

Primitives Cryptographiques dans la blockchain

Présenté par :
M. CHELAGHMA
Abdessamad

Encadrée par :
Dr. MAHAMDIOUA
Meriama

Promotion : 2021

REMERCIEMENTS

Grand merci à Allah, Miséricordieux, le tout puissant qui m'a donnée la force, la persévérance et la patience d'accomplir mon travail.

Ma gratitude, mes vifs remerciements et mes respects à mon encadrante Mme MAHAMDIOUA Meriama, pour tous ses judicieux conseils, son temps qu'elle m'a consacré et pour m'avoir toujours orientée vers un esprit purement scientifique.

Je remercie l'ensemble des membres du jury qui m'ont fait l'immense plaisir de juger ce travail,mes vifs remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer mon travail.

Un grand merci à tous les enseignants du département informatique qui ont été impliqués d'une manière ou d'une autre dans la formation en master et en licence.

J'exprime également mes remerciements à ma famille , mes amis et tous ceux qui ont contribué de près ou de loin à la cristallisation de ces souvenirs, ainsi qu'à la réussite de cette merveilleuse année universitaire...

RÉSUMÉ

Une blockchain est un réseau peer-to-peer décentralisé et distribué, permet d'effectuer des transactions en toute sécurité et sans interférence de tiers. L'utilisation des techniques cryptographiques tels que le cryptage asymétrique, les fonctions de hachage et les signatures numériques, permet à cette technologie de stocker et de transmettre des informations de manière sécurisée, fiable et transparente. Ces techniques sont aussi utilisées pour gérer et sécuriser les portefeuilles, qui sont les points d'accès d'une blockchain de crypto-monnaie, tel que bitcoin. Un portefeuille, qui permet de générer des clés privées, publiques et adresses publiques, est généralement sécurisé par un mot de passe. Une telle sécurisation peut être cassée, et par conséquent, le propriétaire perde l'accès à son portefeuille. Dans ce travail, nous avons ciblé deux problèmes : la sécurisation de portefeuille et la génération des clés. Notre solution permet de réaliser un portefeuille déterministe et sécurisé en basant sur les données biométriques et des données supplémentaire.

Mots-clés :blockchain , crypto-monnaie, portefeuille, transaction, primitives cryptographiques , donnée biométrique.

ABSTRACT

A blockchain is a decentralized and distributed peer-to-peer network, allowing transactions to be carried out securely and without interference from third parties. The use of cryptographic techniques such as asymmetric encryption, hash functions and digital signatures, allows this technology to store and transmit information in a secure, reliable and transparent manner. These techniques are also used to manage and secure wallets, which are the access points to a crypto-currency blockchain, such as bitcoin. A wallet, which can generate private keys, public keys and public addresses, is usually secured by a password. Such security can be broken, and consequently, the owner loses access to his wallet. In this work, we target two problems : wallet security and key generation. Our solution allows realizing a deterministic and secure wallet based on biometric data and additional data.

Keywords : blockchain, cryptocurrency, wallet, transaction, cryptographic primitives, biometric data.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTES DES ABRÉVIATIONS

AES Advanced Encryption Standard

BTC Bitcoin

DPOS Delegated Proof Of Stake

ETH Ethereum

HD Hierarchical Deterministic

P2P Peer to Peer

PoS Proof of Stake

PoW Proof of Work

RSA Ron Rivest, Shamir Adi et Aldeman Len

RIPEMD RACE Integrity Primitives Evaluation Message Digest

SHA Secure Hash Algorithm

UTXO Unspent Transaction Output

INTRODUCTION GÉNÉRALE

En heure de la crise de confiance et du mécontentement vis-à-vis des tiers et médiateurs traditionnels, institutions, banques et États, la technologie blockchain, qui porte la promesse d'une désintermédiation et de la transparence, séduit et intrigue. La technologie blockchain a été proposée et déployée, au début, afin de permettre d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière. Intégrant plusieurs techniques telles que la décentralisation, le calcul distribué, la cryptographie asymétrique, le hachage, l'horodatage et algorithme de consensus, cette technologie commence à être utilisée pour sécuriser d'autre domaine d'application. Grace au principe de fonctionnement de blockchain, on abandonne le mode traditionnel de maintenance des nœuds centraux et adopte la méthode de maintenance mutuelle par plusieurs utilisateurs pour réaliser la supervision des informations entre plusieurs parties, garantissant ainsi la fiabilité et l'intégrité des données. En tant que représentant d'une base de données distribuée, la blockchain stocke toutes les informations de transaction des utilisateurs sur le réseau blockchain, ce qui a des exigences élevées sur les performances de sécurité de la blockchain, qui doit garantir la sécurité des informations de transaction sur des canaux non sécurisés et maintenir l'intégrité de la transaction. On peut voir que les primitives cryptographiques (cryptographie asymétrique, signature numérique, fonc-

tion de hachage,...) occupent la position la plus centrale de la blockchain, qui est principalement utilisée pour protéger la confidentialité des utilisateurs et les informations de transaction, assurer la cohérence des données, etc.

D'autre part, les portefeuilles, qui sont des points d'accès à une blockchain de crypto-monnaie, sont des conteneurs des clés, dont la plupart sont implémentés sous forme de fichiers ou de bases de données structurés très simples. Un portefeuille, qui permet de générer des clés privées, publiques et adresses publiques, est généralement sécurisé par un mot de passe. Une telle sécurisation peut être brisée, et par conséquent, l'utilisateur perde l'accès à son portefeuille, et aux fonds liés à l'ensemble des clés y associées.

Dans ce travail, et dans le contexte de gestion des portefeuilles, nous avons ciblé deux problèmes : la sécurisation de portefeuille et la génération des clés. Notre proposition est basée sur l'utilisation des données biométriques en les combinant avec des données supplémentaires. Basant sur l'idée présentée dans [49], un utilisateur possède une carte intelligente (smart carte), contient, plus les données biométriques, un mot de passe et un nombre aléatoire qui sont utilisés comme des données supplémentaires. L'insertion de ces données supplémentaires permet de créer une autre carte si elle est perdue ou volée. Pour la génération des clés privées et au lieu d'utiliser un générateur aléatoire comme le cas de bitcoin, notre proposition est basée sur l'utilisation des données biométriques en les concaténant avec d'autres données. Ensuite nous avons suivi un ensemble d'étapes pour avoir un portefeuille déterministe et sécurisé.

Le reste de notre mémoire est organisé comme suit : le premier chapitre présente la technologie blockchain et son fonctionnement. Dans le deuxième chapitre, nous présentons des concepts généraux sur les primitives cryptographiques et leurs utilisations dans la blockchain. Le troisième chapitre expose notre proposition et nos solutions développées. Notre mémoire est enfin terminé par une conclusion générale.

CHAPITRE 1

BLOCKCHAIN

1.1 Introduction

Le terme blockchain est apparu en 2008 et depuis lors, nous avons assisté à une croissance des projets basés sur cette technologie. Elle est souvent présentée comme une innovation de rupture, non moins importante que la naissance de l'imprimé ou d'Internet. Ses effets potentiels pourraient révolutionner nos systèmes économiques et nos modes de commerce : la blockchain est porteuse de transformations profondes dans de nombreux domaines d'application. Il peut simultanément représenter une menace, dans son intention ou son utilisation, en créant des systèmes de confiance basés sur des lois mathématiques qui peuvent être libérés des exigences démocratiques ou une opportunité pour la démocratie, s'ils sont bien utilisés. Cette technologie en particulier est porteuse de promesses d'une nouvelle gouvernance, tant au niveau local que mondial, fondée sur des principes innovants : collaboration, décentralisation et transparence. [1].

Une blockchain, ou chaîne des blocs, est une technologie permettant de stocker et de transmettre des informations sans dispositif de contrôle. Techniquement, il s'agit d'une base de données distribuée dans laquelle les informations envoyées par

les utilisateurs et les liens internes à la base sont vérifiées et regroupées à intervalles réguliers en blocs, et le tout est sécurisé par cryptage, formant ainsi la chaîne. Par extension, une blockchain est une base de données distribuée qui maintient une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage.

La technologie blockchain est donc au cœur de l'actualité. Dans ce chapitre on va bien expliquer cette technologie (concepts, architecture, caractéristiques . . . etc.).

1.2 Concepts généraux de blockchain

Avant d'aborder le point lié au fonctionnement d'une blockchain (section 3), nous introduisons dans la présente section les principaux concepts utilisés dans la technologie de blockchain.

1.2.1 Bloc

Un bloc est un regroupement des transactions en attente, effectuées juste après le bloc précédent. Les blocs sont liés entre eux pour former une chaîne de blocs. Chaque bloc peut être considéré comme une page dans le grand livre. Ils sont diffusés à travers tout le réseau et forment une chaine ordonnée [2]. (Pour plus de détails, veuillez consulter la section 6.1).

1.2.2 Transaction

Une transaction blockchain peut être définie comme une petite unité de tâche stockée dans un bloc. Elle peut être présentée comme transfert de donnée, par exemple valeur de pièce qui est diffusé sur le réseau et collecté en blocs. Il est d'abord envoyé à tous les nœuds connectés. Pour augmenter les chances d'être ajouté à un bloc, et faire face au problème de double dépense, on ne peut transférer que les transactions non dépensées [2]. (Pour plus de détails sur les transactions, veuillez consulter la section 6.2).

1.2.3 Portefeuille

Un portefuille est un logiciel pour la sauvegarde des clés privées et des clés publiques d'un utilisateur de blockchain. Ce logiciel peut être une application sur le web, téléphone mobile ou ordinateur. Un portefeuille peut être considéré comme un compte dans une application, Il permet à cet utilisateur de contrôler son fonctionnement et exécuter des transactions.

Les clés sont utilisées pour recevoir et envoyer des transactions. Les clés publiques sont fournies aux autres utilisateurs pour identifier les destinataires, et les clés privées sont utilisées pour signer les messages de transaction et confirmer l'échange de transactions. Les préférences de l'utilisateur sont également conservées dans des fichiers de compte qui peuvent et doivent être cryptés pour atténuer le risque de perte de contenue pour un pirate informatique [3].

1.2.4 Minage et mineurs

Le minage est un terme utilisé pour décrire le processus consistant à la validation d'un bloc (transactions qui attendent d'être incluses dans la blockchain) par un des membres(nœuds) du réseau qui s'appelle mineur [4].

C'est donc considéré comme l'opération fondamentale d'une chaîne de blocs [5], quelle qu'elle soit, et qui la distingue d'un système centralisé classique.

Le minage contribue à la sécurité de la blockchain publique en apportant une contribution en termes de puissance de calcul, notamment la capacité d'un mineur à créer un bloc valide dans la blockchain.

Prenant l'exemple de Bitcoin, Il est nécessaire de résoudre un problème mathématique très complexe en utilisant des algorithmes de consensus, dont la solution ne peut être trouvée que par force brute, c'est-à-dire en testant au hasard des solutions jusqu'à tomber sur la bonne. Pour cela des sociétés ont identifié des fermes minières qui regroupent des machines minières dédiées à haute puissance de calcul, qui sont très couteuses et avec une consommation importante d'électricité.

FIGURE 1.1 – ferme de minage
[6]

Les mineurs les plus performants sont récompensés s'ils ajoutent avec succès un nouveau bloc à la blockchain. En bitcoins par exemple ils récompensent des nouveaux Bitcoins. Les mineurs ont été initialement récompensés avec 50 Bitcoins, la récompense est divisée par deux environ tous les quatre ans (6.25 BTC à partir de mai 2020) [7].

1.2.5 Réseau pair à pair (Décentralisé)

Le réseau de blockchain est composé de nombreux nœuds situés dans le monde entier, chacun d'entre eux conserve une copie locale de la blockchain qui contient une copier complet de toutes les transactions (pour les neouds complets). Il s'agit d'un réseau pair à pair distribué où tous les deux nœuds sont autorisés à communiquer entre eux sans avoir besoin d'une autorité centrale. Un nœud est un ordinateur lié au réseau de la blockchain, il représente un utilisateur particulier, on peut distinguer deux types de nœuds : les nœuds complets et les nœuds légers [8].

— **Nœuds complets :** contiennent une copie complète de la blockchain (l'historique complet de toutes les transactions), généralement suivent toutes les

règles de l'algorithme de consensus pour ajouter des blocs au réseau. Parmi les tâches principales de ceux nœuds la vérification de toutes les transactions et le maintien du consensus entre les autres. Un nœud complet peut être considéré comme un serveur [8].

— **Nœuds légers :** ne contiennent pas la copie complète de la blockchain, mais uniquement les en-têtes de bloc. Les nœuds légers dépendent entièrement de nœuds complets et ne peuvent exister sans un nœud complet, généralement ne disposant pas de capacités matérielles suffisantes [8].

De cette façon, les données se propagent d'un nœud à l'autre pair-à-pair (c'est à dire sans intermédiaire) et atteignent l'ensemble du réseau. Un nœud dans un réseau blockchain remplit diverses fonctions selon le rôle qu'il prend.

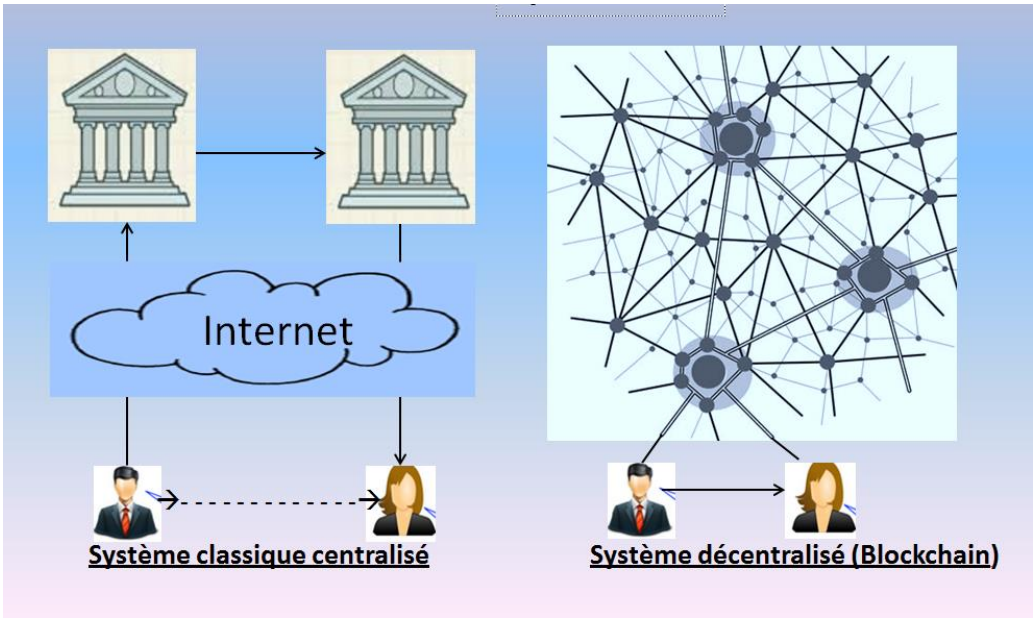

FIGURE 1.2 – Comparaison entre système classique et système basé sur blockchain [9]

Un nœud peut proposer et valider des transactions et effectuer du minage pour faciliter le consensus et sécuriser la blockchain.

1.3 Fonctionnement

Pour expliquer le fonctionnement d'une blockchain, nous prenons l'exemple de cryptomonnaie Bitcoin, ou une blockchain avec un token "simple" (Un token est un actif numérique émis et échangeable sur une blockchain), qui peut être décrit en plusieurs étapes à partir de la création d'une transaction :

— Création d'une portefeuille (compte) pour la sauvegarde des clés privées et clés publiques d'un utilisateur de blockchain), pour qu'un utilisateur de blockchain puisse envoyer ou recevoir des crypto-monnaie. A utilise son portefeuille et effectue une transaction vers B. Cette transaction est diffusée sur le réseau [10].

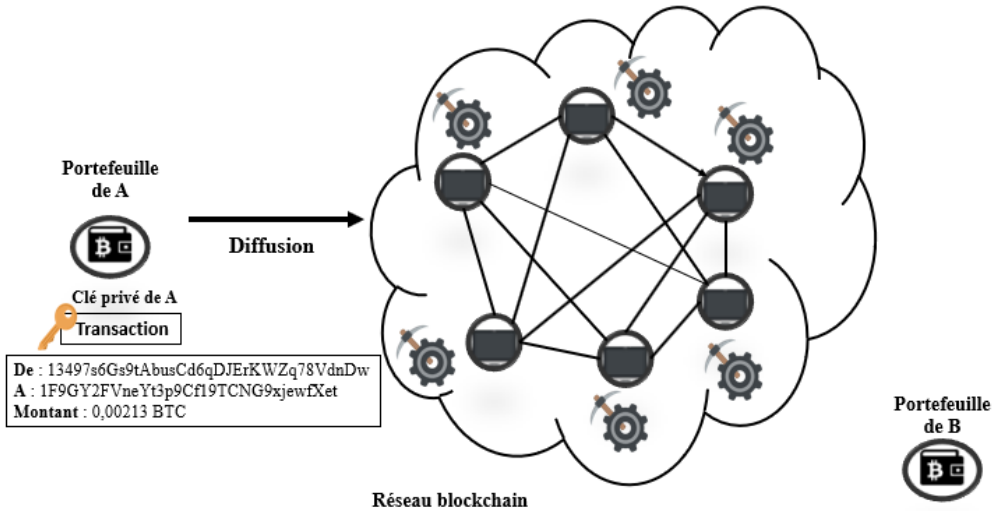

FIGURE 1.3 – Envoi et distribution d'une transaction sur le réseau

— Après avoir reçu la transaction, chaque mineur utilise la clé publique de A pour authentifier la transaction et combiner cette transaction avec d'autres transactions récentes. Chaque transaction sera vérifiée par tous les mineurs [10].

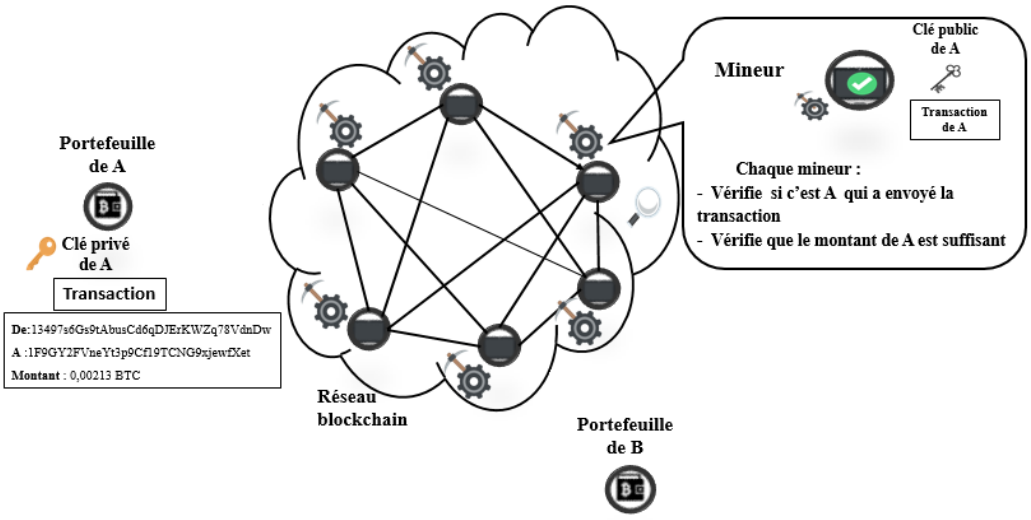

FIGURE 1.4 – Vérification de transaction par les mineurs

— Après sa vérification, la transaction est ajoutée à un bloc

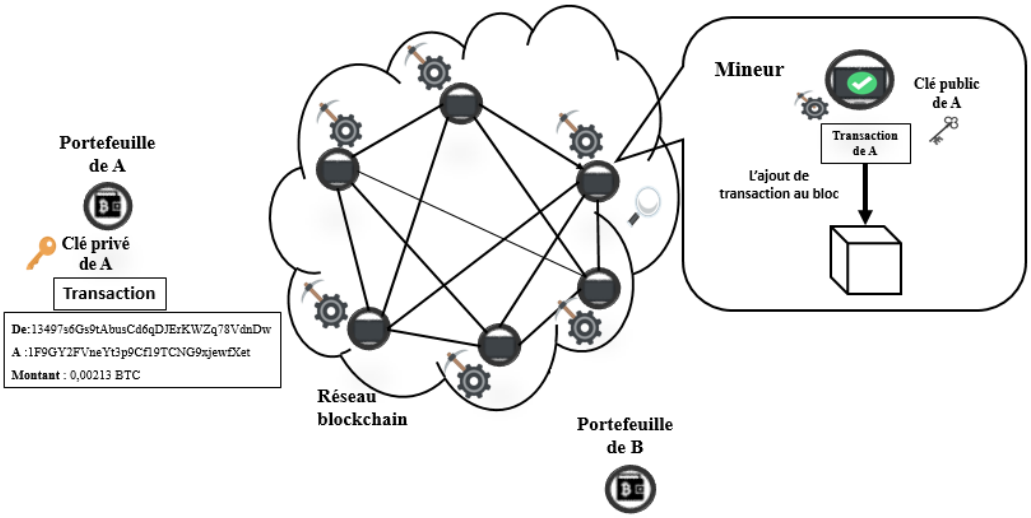

FIGURE 1.5 – Regroupement des transactions dans un bloc

— Après, chaque mineur passe en course pour valider son bloc, selon la technologie de consensus.

Il doit initier le processus de cryptage et calculer le hash du bloc et Chacun de ses blocs possède un identifiant en forme de hache. Ce hash permet de relier le bloc aux autres blocs [10].

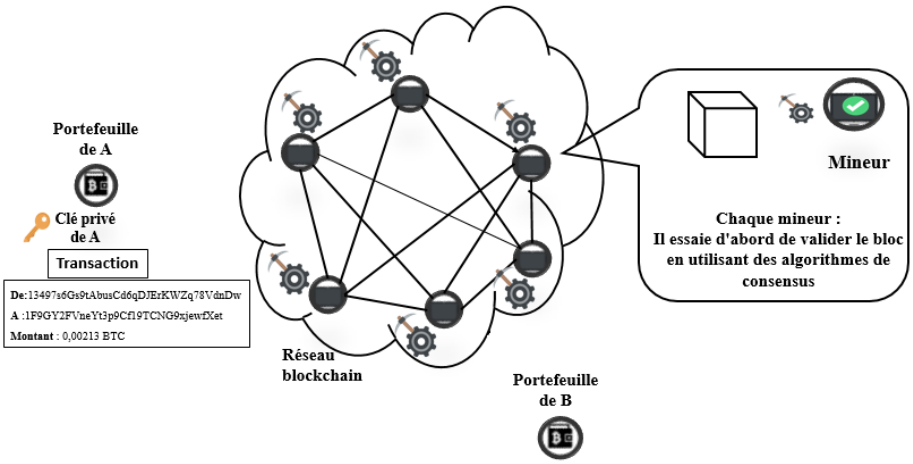

FIGURE 1.6 – Vérification de bloc par les mineurs

— Le nœud qui valide en premier le bloc, le distribue au réseau blockchain pour être vérifié.

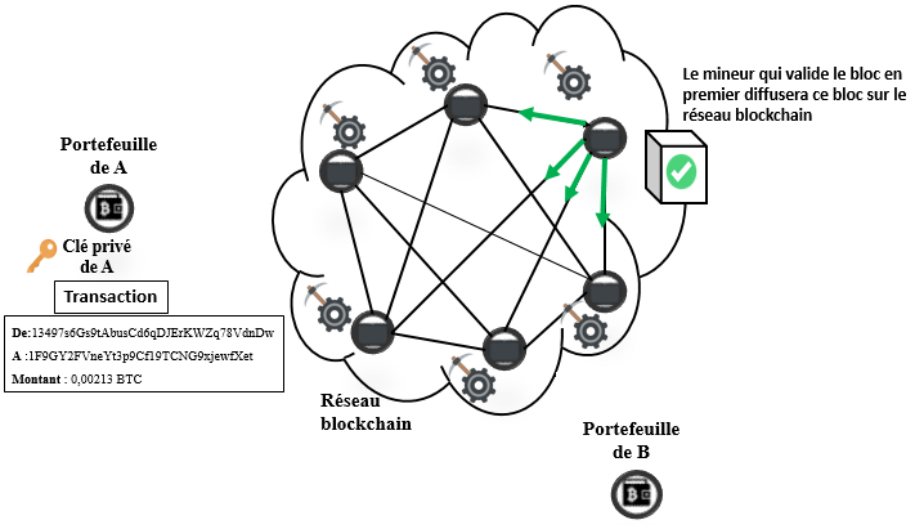

FIGURE 1.7 – Distribution de nouveau bloc sur le réseau et vérification

— Après la vérification de bloc, il sera daté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs peuvent accéder.

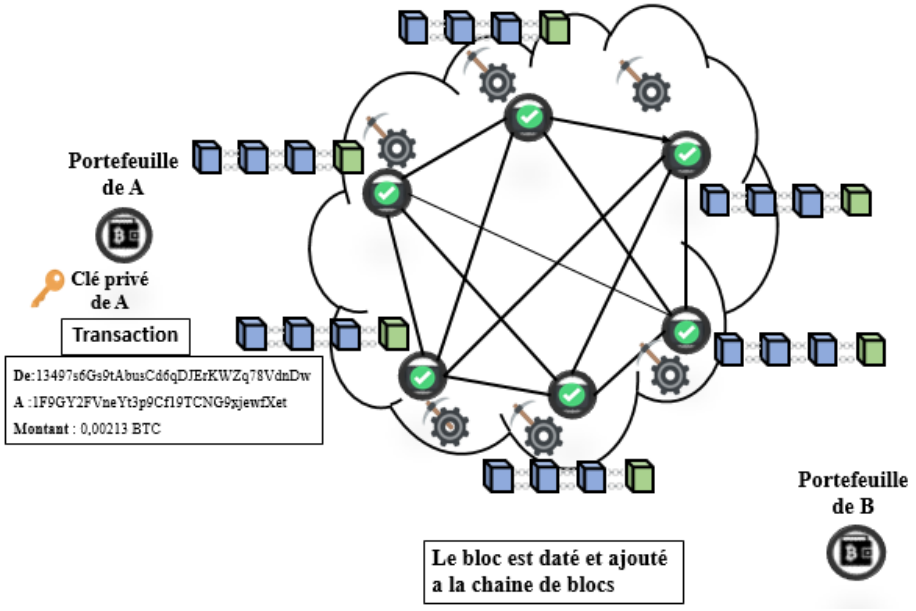

FIGURE 1.8 – validation de bloc par les nœuds de réseau blockchain

— Enfin, "B" reçoit la transaction de A. En récompense du travail fourni, le mineur reçoit une certaine quantité de cryptomonnaie créée pour l'occasion (6,25 Bitcoins à ce jour, mais ce rendement décroît au fil du temps)

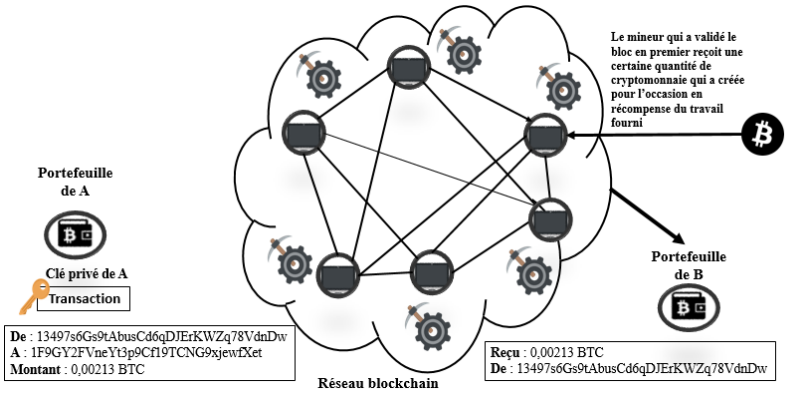

FIGURE 1.9 – Recevoir la transaction

1.4 Caractéristique de blockchain

En tant que registre numérique distribué en temps quasi réel, la chaîne de blocs comporte plusieurs caractéristiques intéressantes qui, avec le temps, pourraient transformer divers secteurs d'activité.

1. **Décentralisation :** l'un des principaux aspects de la blockchain est qu'il s'agit d'un registre décentralisé, ce qui signifie que les données sont détenues par tous les nœuds du réseau. Il n'y a pas d'autorité centrale pour maintenir ou mettre à jour le grand livre général. Chaque paire du système peut ajouter de nouvelles transactions. Chaque transaction qui passe la phase de consensus sera enregistrée dans le grand livre [7]. La figure 1.10 montre la structure d'un système centralisé et décentralisé

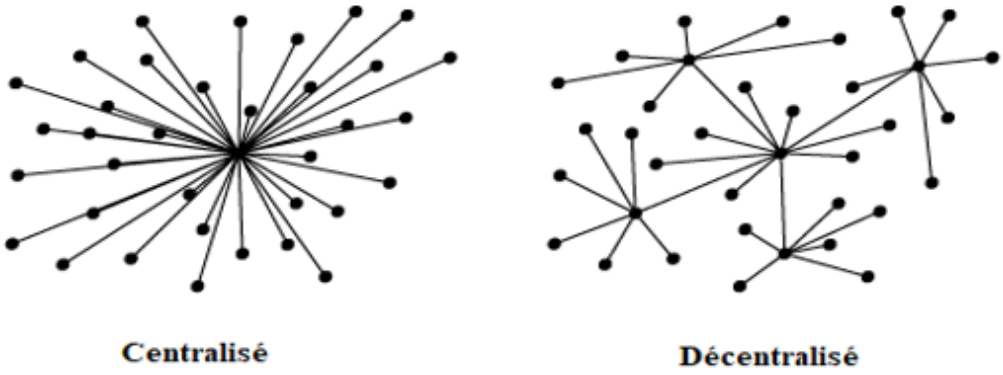

FIGURE 1.10 – Structure d'un système centralisé et décentralisé [7]

2. **Inchangeable :** une fois qu'une transaction est ajoutée à la blockchain, elle ne peut pas être supprimée ou modifiée. Cette immuabilité est l'un des principaux aspects qui contribue à la fiabilité du système blockchain. La manière dont le mécanisme de consensus est atteint rendra impossible de tromper le système et de rendre très fiable. Les registres distribués peuvent être prévus comme des enregistrements permanents irréversibles [7].
3. **Sécurisé :** les chaînes de blocs sont cryptographiquement sécurisées, les signatures numériques garantissant que les données contenues dans les blocs n'ont pas été modifiées.
4. **Transparent :** le grand livre est partagé entre plusieurs pairs du réseau, ce qui signifie que tout utilisateur du réseau peut voir toutes les transactions depuis la création de la blockchain jusqu'au dernier bloc enregistré.
5. **Persistance :** Les transactions peuvent être validées rapidement et les transactions non valides ne seraient pas admises par des mineurs. Les blocs contenant des transactions non valides pourraient être découverts immédiatement.
6. **Anonymat :** Chaque utilisateur peut interagir avec la blockchain avec une adresse générée, qui ne révèle pas la véritable identité de l'utilisateur [7].

1.5 Architecture en couche de blockchain

Bien que la blockchain ait imposé des impacts significatifs sur la crypto-monnaie, la finance et même les activités socio-économiques, ce n'est pas une nouvelle technologie inventée à partir de zéro. En fait, la blockchain peut être considérée comme une innovation d'ensemble combinant un groupe de technologies existantes dans les domaines de la cryptographie, de l'économie et de l'informatique.

La blockchain n'est pas encore normalisée, et dans la littérature, on peut trouver plusieurs propositions d'architecture en couches. Dans cette section, nous présentons celle proposée dans [11].

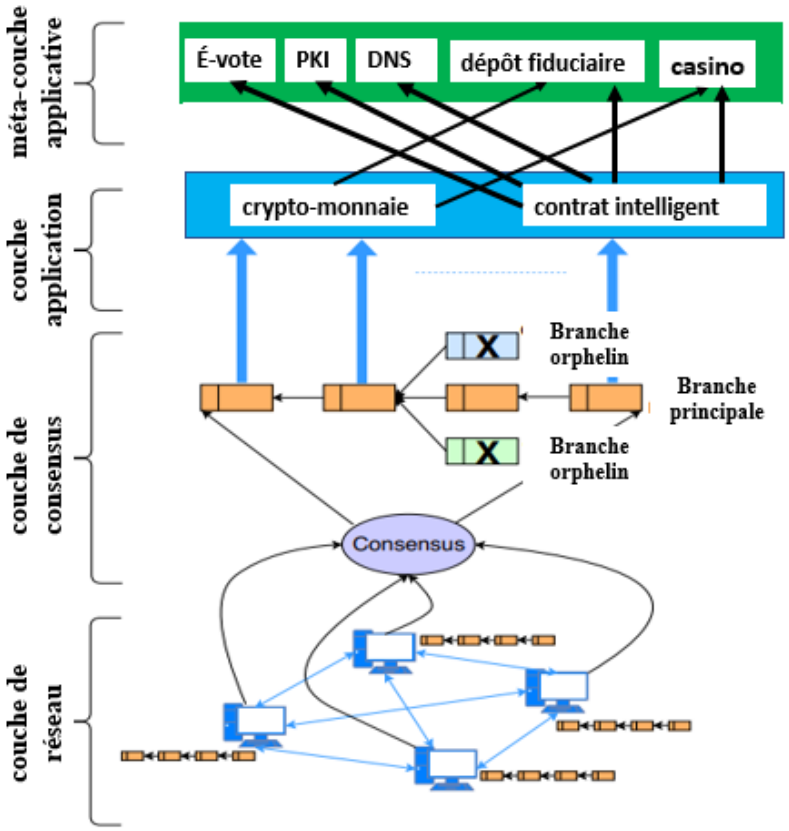

FIGURE 1.11 – Les couches de blockchain [11]

1.5.1 Couche méta-application

Les fonctionnalités de la couche méta-application dans un système blockchain (voir Figure 1.11) consistent à fournir une superposition au-dessus de la couche application pour exploiter l'interprétation sémantique d'un système blockchain à d'autres fins dans d'autres domaines d'application [11].

1.5.2 Couche d'application

La couche application (dans la figure 1.11) définit l'interprétation sémantique d'un système de blockchain. Un exemple d'interprétation sémantique serait de définir une crypto-monnaie, puis de mettre en place des protocoles sur la façon dont une telle devise peut être échangée entre différentes entités. Un autre exemple consiste à établir des protocoles pour maintenir une machine à états incorporant des capacités de programmation au sein de la blockchain, qui peuvent être exploitées pour créer et déployer un code immuable (le soi-disant contrat intelligent). L'application définit également le mécanisme de récompense, le cas échéant, dans le système de blockchain [11].

1.5.3 Couche de consensus

La couche de consensus, telle que présentée à la figure 1.11, est chargée de fournir le mécanisme de consensus distribué dans la blockchain qui régit essentiellement l'ordre des blocs.Un exemple de protocole très utilisé est le protocole de preuve (par exemple, preuve de travail et preuve d'enjeu) qui est utilisé pour vérifier chaque bloc, afin d'atteindre le consensus requis dans le système [11].

1.5.4 Couche réseau

Les composants de la couche réseau sont responsables de la gestion des fonctionnalités du réseau, notamment l'adhésion au réseau P2P sous-jacent, le maintien dans le réseau en suivant le protocole réseau sous-jacent, la diffusion de l'état actuel

de la blockchain aux nœuds nouvellement joints, la propagation et la réception de transactions et de blocs, etc [11].

1.6 Composants de la blockchain

La technologie de blockchain comme nous avons déjà signalé dans les sections précédentes se base sur plusieurs concepts tels que transaction, bloc,consensus. Dans cette section, nous présentons plus en détail ces différents composants.

1.6.1 Bloc

Les blocs sont une structure de données fondamentale (fichier) dans la blockchain, ils sont liés entre eux pour former une chaîne de blocs. Chaque bloc peut être considéré comme une page dans le grand livre. Un bloc est un enregistrement de certaines transactions valides qui n'ont pas encore été enregistrées dans les blocs déjà chaînés.

Un bloc est composé de : l'entête qui contient les méta-donnés, et de corps qui regroupe les transactions .

1. **En-tête de bloc**

   Contient les éléments suivants :

   — **Version de bloc :** indique quel ensemble de règles de validation de bloc à suivre, ceci est utilisé pour que les ordinateurs puissent lire correctement le contenu de chaque bloc [7].

   — **Hachage de la racine de l'arbre Merkel :** la valeur de hachage de toutes les transactions dans le bloc [7]. (Voir le principe de l'arbre de Merkel dans la section 2.4 de chapitre 2).

   — **Horodatage :** heure actuelle en secondes dans le temps universel depuis le 1er janvier 1970 [7].

   — **Nonce :** la partie de hash que le mineur va devoir faire varier et trouver pour résoudre la preuve de travail, un champ de 4 octets, qui commence généralement par 0 et augmente pour chaque calcul de hachage [7].

— **ParentHash :** une valeur de hachage de 256 bits qui pointe vers le bloc précédent. S'il s'agit du premier bloc (bloc genèse), cet hash vaut 0.

— **Données supplémentaires :** il peut s'agir par exemple de l'index (hauteur) qui indique l'emplacement du bloc à l'intérieur de la blockchain. Le premier bloc est indexé « 0 » ; cela s'appelle le bloc de genèse, le prochain "1", et ainsi de suite [7].

2. **Corps de bloc**

Le corps de bloc est composé d'un compteur de transactions et transactions. Le nombre maximal de transactions qu'un bloc peut contenir dépend de la taille du bloc et de la taille de chaque transaction [7]. Dans le contexte d'une blockchain, il existe différents types de blocs :

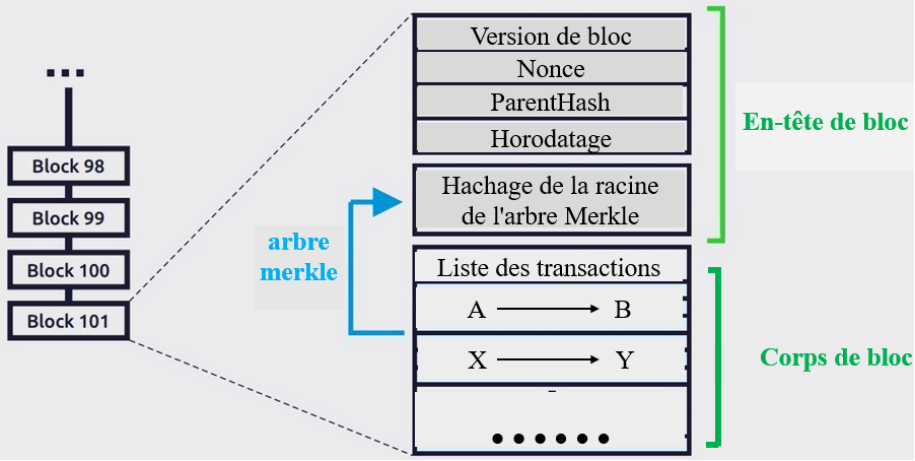

FIGURE 1.12 – Structure simplifié d'un bloc
[3]

— **Bloc genèse :** c'est le premier bloc de toute blockchain (hauteur = 0). Il fournit la base sur laquelle une blockchain entière est construite. En termes de Bitcoin, le bloc genèse a été créé le 3 janvier 2009 et contient 50 BTC.

— **Blocs de branche principale :** les blocs de branche principale font référence aux blocs qui se trouvent dans la chaîne la plus haute.

— **Blocs orphelins :** les blocs orphelins sont les blocs qui ont la même hauteur, ils se produisent lorsque deux mineurs produisent un bloc à des moments similaires.

Les blocs orphelins sont considérés comme des blocs valides pour la première fois mais ils ne font pas partie de la chaîne principale.

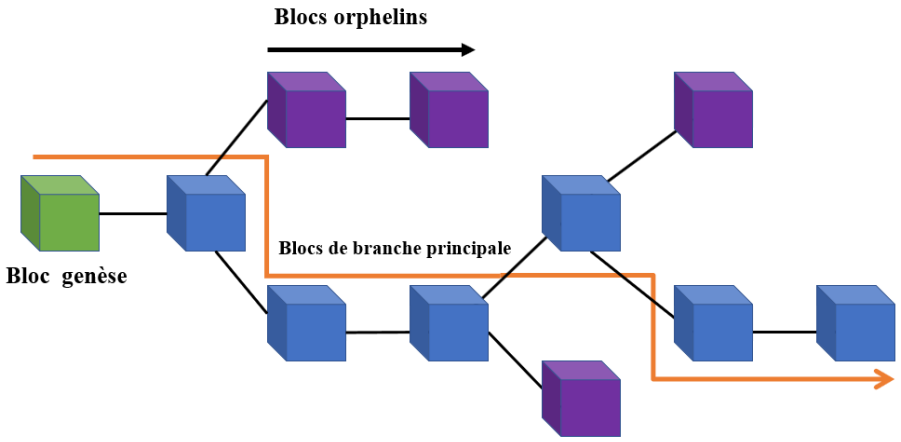

FIGURE 1.13 – Chaine de blocs

1.6.2 Transactions

La transaction est l'unité de base de la blockchain. La façon la plus simple de penser à une transaction est en termes de transactions financières ou d'échanges tels que Bitcoin.

Cependant, les transactions ne doivent pas nécessairement être financières et peuvent être n'importe quel événement qui déclenche un changement dans la blockchain.

Dans ce qui suit, nous présentons le cycle de vie, la structure input et output des transactions en prenant le cas de crypto-monnaie Bitcoin. [2].

1.6.2.1. Transaction bitcoin

Pour le bitcoin, une transaction représente le transfert de valeur d'un compte (adresse) à un autre. Les portemonnaies et autres applications envoient de nouvelles transactions en permanence vers le réseau [2].

1. **Cycle de vie d'une transaction**
   - Le cycle de vie d'une transaction commence avec sa création.
   - La transaction est ensuite signée avec une ou plusieurs signatures ce qui signifie qu'il est autorisé de dépenser les fonds références dans la transaction.
   - N'importe quel réseau peut être utilisé pour la diffuser publiquement, car la transaction est signée et ne contient aucune information confidentielle, tels que clés privées ou identifiants.
   - Lors sa diffusion sur le réseau bitcoin, chaque nœud réseau (participant) valide et poursuit sa diffusion jusqu'à ce qu'elle arrive à tous les nœuds réseau ou presque.
   - Ensuite, la transaction est vérifiée par un mineur et intégrée dans un bloc de transactions qui est diffusé sur le réseau.
   - A la réception d'un bloc du réseau bitcoin, un mineur (récepteur) a perdu la course pour ce bloc et il commence directement une nouvellecourse pour miner un nouveau. en ajoutant des transactions non déjà traitées, le hash du bloc précédent puis commence à calculer la PoW. Une transaction spéciale est ajoutée aussi dans ce nouveau bloc qui paie une récompense vers l'adresse du mineur (6.25 BTC aujourd'hui) qui a validé ce bloc. Il gagne aussi les frais de transaction (valeur de bitcoin fournisse par l'émetteur de transaction pour payer le service de traitement de son transaction).
   - L'ajout d'un nouveau bloc après celui contenant une transaction est considérée comme une "confirmation" de cette transaction. Il sera plus difficile d'annuler cette transaction, au fur et à mesure que les blocs seront ajoutés : on pourra donc lui faire plus de confiance. Par convention on considère

qu'un bloc confirme 6 fois est irrévocable, parce qu'il faudrait une énorme puissance de calcul pour le remplacer 6 autres blocs.

— Après son enregistrement sur la blockchain et confirmation par les blocs suivants, la transaction devient partie intégrante du registre bitcoin et elle est considérée comme valide par tous les participants.

— Les fonds allouent à un nouveau propriétaire par la transaction peuvent alors être dépenses dans une nouvelle transaction, tout en répétant à nouveau le cycle de vie d'une transaction.

2. **Structure des Transactions**

— Une transaction est une structure de données qui encode un transfert de valeur d'une source de fonds, appelé input, a un point de destination, appelée output [12].

— Les inputs et output de transaction sont traités comme des montants en bitcoin verrouilles grâce à une clé secrète que seulement le propriétaire pourrait déverrouiller. Une transaction a un certain nombre de champs,

Taille	**Champ**	**Description**
4 octets	Version	Spécifie quelles règles suit cette transaction
1-9 octets (VarInt)	Compteur d'Input	Combien d'inputs sont inclus
Variable	Inputs	Un ou plusieurs inputs de transaction
1-9 octets (VarInt)	Compteur d'Output	Combien d'output sont inclus
Variable	Outputs	Un ou plusieurs outputs de transaction
4 octets	Locktime	Un horodateur Unix ou le numéro d'un bloc

TABLE 1.1 – La structure d'une transaction
[2]

3. **Outputs et Inputs de transaction**
   - L'élément constitutif fondamental d'une transaction bitcoin est un unspent transaction output, ou UTXO.
   - Les UTXO sont reconnu comme des unîtes monétaires sur le réseau. Ce sont des morceaux indivisibles de bitcoin lies à un utilisateur précis, enregistres sur la blockchain.
   - Un UTXO peut représenter n'importe quelle valeur arbitraire. Il est indivisible comme une pièce qu'on ne peut pas couper en deux. Si le montant d'un UTXO est plus important que la valeur de la transaction, il doit être consomme totalement dans le processus et générer un retour de monnaie a l'émetteur.
   - Le réseau bitcoin garde la trace de tous les UTXO disponible (non dépenses).
   - A chaque fois qu'un utilisateur reçoit des bitcoins, le montant est enregistré dans la blockchain en tant qu'UTXO.
   - Le portemonnaie (le wallet) calcule le solde d'un 'utilisateur tout en examinant la blockchain et en agrégeant tous les UTXO qui lui appartiennent. L'application wallet de l'utilisateur sélectionnera les UTXO de l'utilisateur disponibles pour composer un montant supérieur ou égal au montant de la transaction, en combinant –par exemple- plusieurs unirent d'un montant inférieur, trouvant la monnaie exacte ou utiliser une unité d'un montant plus grand et récupérer la monnaie.
   - Les UTXO consommées par une transaction sont appelées les inputs de transaction, les UTXO créées par une transaction sont appelées outputs de transaction.
   - — Les transactions consomment des UTXO en les déverrouillant avec la signature du propriétaire actuel et créent des UTXO en les verrouillant sur l'adresse du nouveau propriétaire.

a. Outputs de transaction :

Pour envoyer des bitcoins à quelqu'un, on doit créer de UTXO associées à son adresse qu'il pourra dépenser par la suite.

Les outputs de transaction sont constitués de deux parties :

- Un montant de bitcoin en satoshis, l'unité la plus petite de bitcoin.
- Un locking script (ou script de verrouillage), qui peut être une simple adresse de destinataire, ou un script qui verrouille le montant de cette sortie,

Par exemple, la sortie d'une transaction envoyer par X vers Y contient un script qui signifie "cette sortie sera payée à celui qui fournira une signature valide pour la clef correspondante à l'adresse publique de Y".

Tant que Y est la seule personne possédant les 2 clefs (publique et privée) correspondant à cette adresse, alors Y est la seule personne pourra fournir une telle signature.

X va donc verrouiller cette sortie en exigeant une signature provenant de Y.

b. Inputs de transaction :

- On peut définir simplement les inputs de transaction comme des pointeurs vers des UTXO. Ils pointent vers un UTXO spécifique en référençant un hash de transaction et un numéro de séquence ou est enregistré l'UTXO dans la blockchain [2].
- Pour dépenser un UTXO, un input de transaction inclut également un script de déverrouillage qui remplit les conditions de dépenses de l'UTXO.
- Quand les utilisateurs effectuent un paiement, leurs porte-monnaies construisent une transaction en piochant dans les UTXO disponibles.

Exemple

— Joe envoie une transaction à Alice contient une valeur de bitcoin.

— Alice utilise les bitcoins reçus de la transaction envoyée par Joe contre un bien livré de Bob. Pour cela, les outputs de transaction de transaction de Joe sont utilisés pour composer les inputs de la transaction d'Alice.

— Bob aussi envoie une transaction à Gopesh, en utilisant lui-même l'output de la transaction d'Alice pour construire les inputs de sa transaction.

— Voyant qu'une unité bitcoin garde une trace de leur propriétaire depuis sa création.

— Chaque unité est consommée entièrement à la fois. Par exemple, si vous avez un UTXO de 20 bitcoins et que vous désirez payer 1 bitcoin, alors la transaction doit d'abord consommer les 20 bitcoins de l'UTXO avant de produire deux outputs : le paiement de 1 bitcoin aux destinataires de la transaction et un autre paiement de 19 bitcoins vers votre wallets, comme si on vous rendait la monnaie. En conséquence, la plupart des transactions en bitcoin génère un rendu de monnaie.

La figure 1-14 illustre comment les transactions sont dépensées.

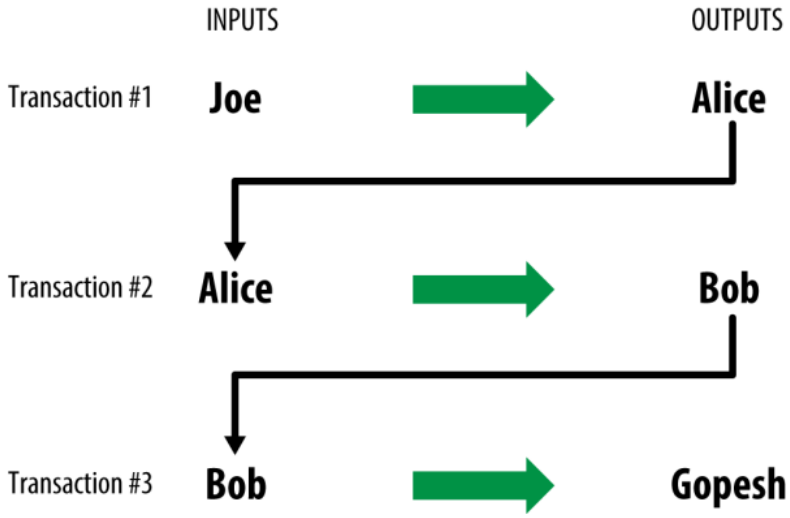

FIGURE 1.14 – La transaction d'Alice incluse dans la chaine de transactions de Joe vers Gopesh

[2]

4. **Catégories de transactions Bitcoin**

   Fondamentalement, il existe deux catégories de transactions Bitcoin :

   — **Transactions Coinbase :** est la première transaction d'un bloc. Chaque bloc de la blockchain Bitcoin contient une transaction Coinbase incluse par les mineurs eux-mêmes pour pouvoir extraire de nouvelles pièces. Elle est positionnée par le mineur "gagnant" et créée de tous nouveaux bitcoins payables à ce mineur comme récompense du minage [2]. Le nombre de pièces qui peut être extrait à chaque fois est contrôlé par le réseau lui-même. Il a commencé avec 50 BTC au début et continue de diminuer de moitié jusqu'à ce qu'il atteigne 21 millions de Bitcoins au total [13].

   — **Transactions régulières :** sont très similaires aux échanges de devises en général, où l'on essaie de traiter une somme d'argent qu'il possède avec un autre [13].

1.6.3 Consensus

Le consensus est un grand problème dans les réseaux distribués comme la blockchain, puisqu'il n'y a pas d'entité centrale pour décider quels nouveaux blocs sont valides, chaque nœud doit décider s'il accepte ou non un nouveau bloc reçu [14]. On peut définir le consensus comme l'épine dorsale de la blockchain (système de grand livre distribué), car la sûreté et la sécurité de la blockchain sont assurées dans cette couche, généralement c'est la couche de base de la plupart des systèmes de blockchain. Le but principal de cette couche est de faire en sorte que tous les nœuds se mettent d'accord sur un état cohérent du registre, tous suivant des règles simples [15]. Dans un réseau blockchain, le consensus sert à la vérification des transactions (simple) plus des algorithmes de consensus (PoW, PoS...) (Compliqué). Il existe de nombreuses variantes de protocoles de consensus tels que la preuve de participation (PoS), PoS délégué (dPoS)...etc.

1. **Preuve de travail (Proof of Work (PoW))**

   Le mécanisme de preuve de travail est considéré comme le mécanisme de consensus le plus célèbre de la blockchain car il a été utilisé avec la première crypto-monnaie qui ait jamais existé. L'idée de preuve ou de travail est que les ordinateurs agissent pour résoudre un puzzle ou pour proposer un hachage qui vérifie une propriété prédéfinie. Chaque mineur travaille pour trouver un nombre aléatoire appelé nonce (nombre utilisé une fois) en hachant deux fois les données à l'intérieur de l'en-tête du bloc, puis en les comparant à la cible de difficulté, dans le cas du bitcoin, la cible est un nombre de 256 bits qui peut être trouvé dans l'en-tête de chaque bloc et sa valeur diffère d'un bloc à l'autre. La fonction de hachage cryptographique utilisée pour hacher les données à l'intérieur d'un bloc dans PoW est SHA256 :

   H [H (Version | Hachage de bloc précédent | Racine Merkel | Horodatage | Cible de difficulté | Nonce)] < [Cible de difficulté]

   Les mineurs continuent de changer le nonce qui part de zéro en l'incrémentant de 1 afin de trouver un hachage inférieur à la difficulté cible. Une fois que le hachage a plus de zéros non significatifs que la cible, alors il satisfait la

condition. Plus il y a de zéros dans la cible, plus il devient difficile de trouver le hachage qui peut satisfaire la condition. Ce mineur diffusera ensuite le bloc à l'ensemble du réseau pour vérifier si le résultat est correct puis il ajoutera ce bloc à la blockchain ainsi que les autres mineurs [16].

Parce que PoW devient plus difficile avec le temps, les mineurs joignent leurs efforts pour obtenir plus de puissance de calcul en formant des clusters. Ces groupes sont connus sous le nom de pools miniers.

La technique permet aux personnes qui font équipe d'augmenter leurs chances d'exploiter de nouveaux blocs et ainsi de collecter les récompenses.

Cependant, de telles techniques peuvent être dangereuses pour la sécurité de la blockchain. Si une entité (ou une minorité) contrôle une grande partie de la blockchain bitcoin, elle pourra centraliser le processus de minage. C'est ce qu'on appelle une attaque à 51% et a d'abord été discuté comme un point faible de l'algorithme PoW si un seul mineur ou groupe de mineurs peut obtenir 51% de la puissance de hachage, ils peuvent contrôler efficacement la blockchain [17].

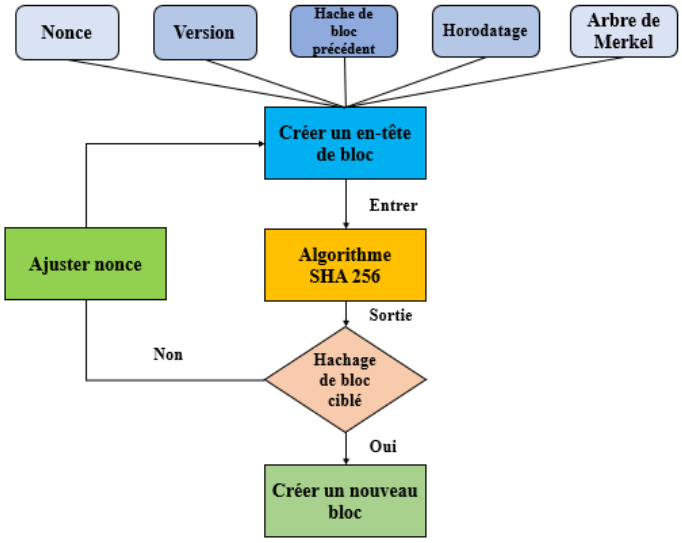

FIGURE 1.15 – Preuve de travail
[17]

2. **Preuve d'enjeu (Proof-of- stake (PoS))**

   Ce consensus a été développé dans le but de prouver une meilleure solution à l'algorithme précédemment utilisé, Proof-of-Work (PoW) qui était inefficace et mal protégé contre le comportement non professionnel des délégués. Les systèmes de sélection des témoins garantissent que la personne la mieux adaptée est choisie de manière démocratique. Dans le système PoS, une personne peut extraire et certifier des transactions en bloc en fonction de la valeur de sa mise. Plus l'enjeu d'un utilisateur est important, plus il tirera d'avantages du système. Grâce aux algorithmes, les utilisateurs sont tenus de miser un certain nombre de leurs jetons pour leur offrir une chance d'être choisis pour valider les blocs de transaction et obtenir une récompense pour la validation des blocs. La première considération de sélection est la quantité de monnaie que le contrefacteur mise. Il est obligatoire pour chaque utilisateur de placer une mise en déposant un certain nombre de jetons dans le réseau [18].

   Le pieu est enfermé dans un coffre-fort virtuel et utilisé comme garantie pour garantir les blocs. Les chances d'être choisi augmentent en fonction du montant que le contrefacteur est prêt à miser. Plus l'enjeu est élevé, plus un utilisateur a de chances d'être choisi. Le contrefacteur sélectionné n'est récompensé que par les frais de transaction puisqu'il n'y a pas de récompense en bloc [18]. Les principaux avantages de la preuve d'enjeu sur la preuve de travail sont :

   — Réduits la consommation d'énergie.

   — Plus de décentralisation entraînant une diminution des chances d'attaque de 51%.

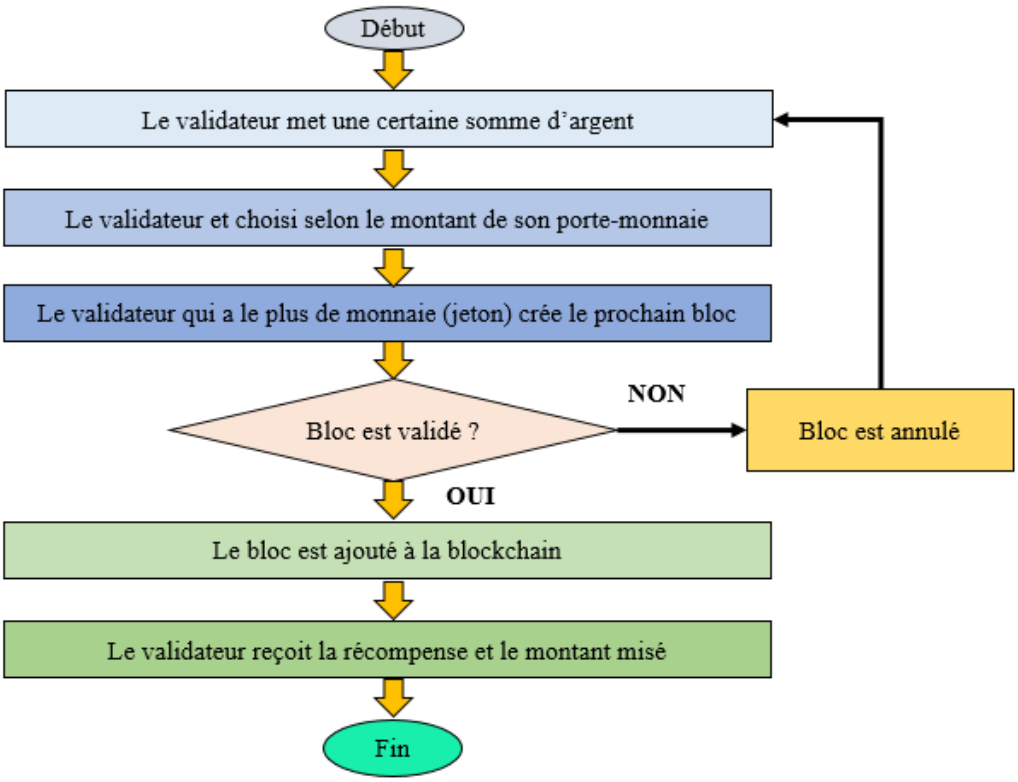

FIGURE 1.16 – Preuve d'enjeu
[17]

3. **Preuve de mise déléguée (Delegated proof of stake (DPoS))** L'algorithme de consensus preuve d'enjeu délégué (DPoS) a été développé par Daniel Larimer, en 2014. Bitshares, Steem, Ark et Lisk sont quelques-uns des projets de cryptomonnaie qui utilisent l'algorithme de consensus DPoS [19].
   - Une blockchain basée sur DPoS compte les parties prenantes sous-traitent leur travail a un tiers. En d'autres termes, ils peuvent voter pour quelques délégués qui sécuriseront le réseau en leur nom. Les délégués peuvent également être appelés témoins et ils sont chargés de parvenir à un consensus lors de la génération et de la validation de nouveaux blocs [19].
   - Le droit de vote est proportionnel au nombre de pièce détenues par chaque utilisateur.

Le système de vote varie d'un projet à l'autre, mais en général, chaque délégué présente une proposition individuelle lorsqu'il demande des votes.

— Habituellement, les récompenses recueillies par les délégués sont partagées proportionnellement avec leurs électeurs respectifs. Par conséquent, l'algorithme DPoS crée un système de vote qui dépend directement de la réputation des délégués.

— Si un nœud élu se comporte mal ou ne fonctionne pas efficacement, il sera rapidement expulsé et remplacé par un autre.

— En ce qui concerne les performances, les chaînes de blocs DPoS sont plus évolutives, pouvant traiter plus de transactions par seconde, par rapport à PoW et PoS.

Les rôles des délégués sont :

— S'assurer que leur nœud est toujours opérationnel.

— Collecte des transactions sur le réseau.

— Signer et diffuser ces blocs, valider les transactions.

— S'il y a des problèmes de consensus, le département de la sûreté et de la sécurité permet de les résoudre d'une manière juste et démocratique.

Les délégués n'ont pas le pouvoir de modifier les détails d'une transaction. Toutefois, en tant que validateurs, ils pourraient théoriquement exclure certaines transactions d'un bloc. Néanmoins, cela n'a que trés peu d'effet puisque le prochain bloc crée inclura ces transactions, ce qui donnera au prochain délégué les frais associés à leur validation [20].

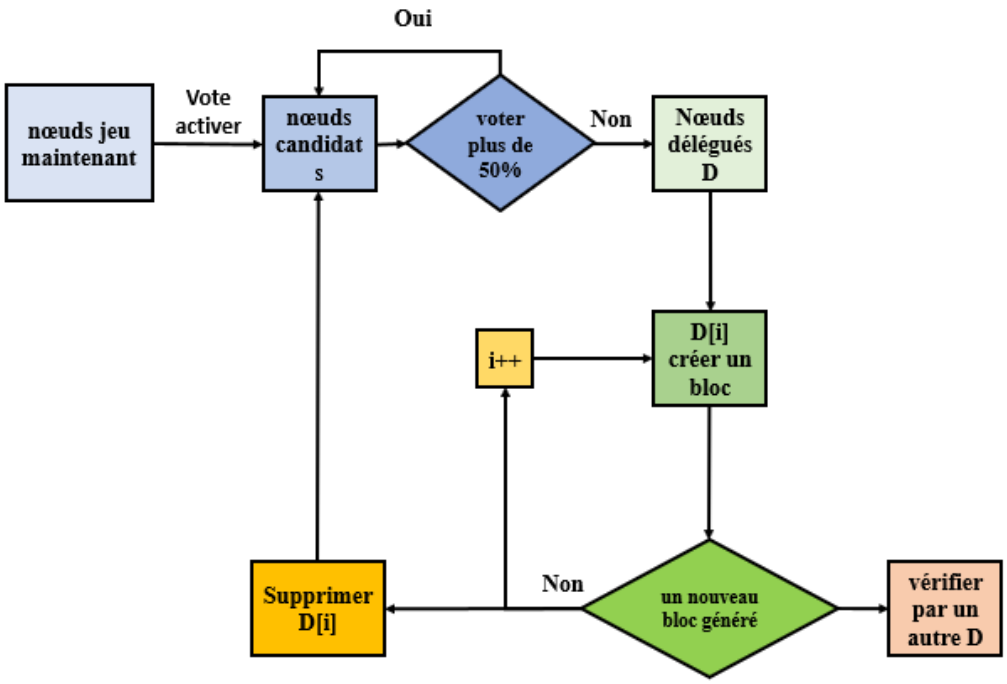

FIGURE 1.17 – Preuve de mise déléguée
[17]

1.6.4 Contrat intelligente

Les contrats intelligents sont des programmes informatiques autonomes auto-exécutables qui sont exécutés en fonction d'une condition définie par le programmeur [21].

Ces contrats sont capables de faciliter, de faire respecter et d'exécuter des accords entre deux parties en utilisant la blockchain. Contrairement aux contrats traditionnels, où un tiers (banque, notaire) est requis, les contrats intelligents permettent une entreprise indépendante entre des parties anonymes avec des frais moins chers.

Les contrats intelligents peuvent être utilisées pour assurer plusieurs application telles que :

— **Vote numérique :** les contrats intelligents reposant sur la blockchain peuvent améliorer la sécurité des systèmes de vote, par exemple des applications utilisent

les contras intelligents et la blockchain pour protéger les votes de la fraude [22].

— **Gestion d'entreprise :** les entreprises peuvent bénéficier des contrats intelligents et économiser beaucoup de temps et d'argent, ils peuvent établir un contrat intelligent simplement indiquant quand la date est telle date les salaires seront envoyés automatiquement aux employeurs.

— **Paiement :** par exemple, on peut payer le loyer de la chambre automatiquement à la fin du mois sans impliquer une banque entre les deux, un développeur écrit un programme informatique system (contrat intelligent). Ce programme définit l'intégralité des règles telles qu'elles ont été définies au début du projet : un mois de souscription, à qui les fonds seront envoyés, quel montant minimum sera récolté, quand les conditions (règles) les conditions sont remplies, telles que la date de paiement, le code sera exécuté et le paiement est effectué automatiquement Il y'a d'autres utilisations des contrats intelligents comme le trading ou prêt de propriété, commerce d'actions ou d'obligations sur des marchés distribués [21]. En outre, il peut également être utilisé pour un système de contrat de notaire numérique autonome.

1.7 Classification des systèmes blockchain

La diversité de la recherche et du développement de la blockchain offre une opportunité de classer la blockchain en catégories selon un ensemble de critères.

1.7.1 Blockchain publique

L'identifiant principal d'un système blockchain sans autorisation est son modèle de participation ouverte où tout le monde peut rejoindre ou quitter le réseau blockchain à tout moment. La blockchain publique appelée également sans autorisation est accessible au public par tout le monde dans le réseau et n'a aucune restriction sur qui peut participer ou être un validateur. Dans la blockchain publique, tous les enregistrements sont visibles par le public et tout le monde peut participer au processus de consensus.

Ces plateformes sont souvent des logiciels open source, librement accessibles à quiconque souhaite les télécharger. Étant donné que n'importe qui a le droit de publier des blocs, cela se traduit par la propriété que n'importe qui peut lire la blockchain ainsi qu'émettre des transactions sur la blockchain (en incluant ces transactions dans les blocs publiés). Les exemples de blockchain publics les plus connus sont : blockchain Bitcoin et Ethereum [23].

1.7.2 Blockchain privée

Une blockchain privée ou une blockchain autorisée est entièrement gérée par une organisation où tous les nœuds du système sont identifiés et connus. Étant donné que seuls les utilisateurs autorisés maintiennent la blockchain, il est possible de restreindre l'accès en lecture et de restreindre qui peut émettre des transactions.

Les réseaux de blockchain autorisés peuvent ainsi permettre à n'importe qui de lire la blockchain ou ils peuvent restreindre l'accès en lecture aux personnes autorisées. Ils peuvent également permettre à quiconque de soumettre des transactions à inclure dans la blockchain ou, encore une fois, ils peuvent restreindre cet accès uniquement aux personnes autorisées. Les réseaux blockchain autorisés peuvent être instanciés et maintenus à l'aide d'un logiciel open source ou fermé [23].

1.7.3 Blockchain Consortium

Également connu sous le nom d'hybride, il s'agit d'un autre type qui n'est pas beaucoup mentionné dans la littérature. Ce type n'est pas contrôlé par une seule autorité mais par un groupe spécifié qui est créé pour contrôler le processus de consensus. La blockchain du consortium est un système « semi-privé » et dispose d'un groupe d'utilisateurs contrôlé, mais fonctionne dans différentes organisations. Ils sont souvent associés à une utilisation en entreprise, avec un groupe d'entreprises collaborant pour tirer parti de la technologie blockchain afin d'améliorer les processus métier [23].

1.8 Quelques domaines d'application de blockchain

L'utilisation la plus connue et la plus courante de la blockchain est actuellement dans les cryptomonnaies. C'est compréhensible car la première blockchain jamais utilisée était celle introduite par Satoshi Nakamoto dans Bitcoin, qui était aussi la première crypto-monnaie.

Le succès que les crypto-monnaies ont connu a attiré l'attention et l'imagination des développeurs et des innovateurs sur la blockchain et la technologie qui la sous-tend, alors ils commencé à chercher les possibilités de cette technologie et elle a été adaptée pour être utilisée non seulement dans le secteur financier mais dans de nombreux autres domaines. Dans cette section, nous présentons des exemples des domaines d'application de blockchain.

1.8.1 Bitcoin

En 2008, Satoshi Nakamoto a expliqué l'idée principale de son invention dans son livre blanc intitulé 'Bitcoin : A Peer-to-Peer Electronique Cash System", il a déclaré : "ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur une preuve cryptographique au lieu de la confiance, permettant à deux parties de traiter directement l'une avec l'autre sans avoir besoin d'un tiers de confiance" ; Avant la sortie du bitcoin, il y avait plusieurs sorte de monnaie numérique, le premier était ecash qui a été développé par 'David Chaum' et utilisé par digcash corporation en 1990, après cela un autre concept a été développé par 'Adam Back' avec le nom hashcash qui est un système de preuve de travail utilisé pour contrôler le spam par courrier électronique et les attaques par déni de service. B-money a été la première proposition d'argent numérique distribué par Wei Dai, puis Satoshi a rassemblé ces concepts dans une crypto-monnaie appelée "bitcoin" [24].

1.8.2 Ethereum

Ethereum est une plate-forme informatique conçue pour faciliter les contrats intelligents dans lesquels Ether est la crypto-monnaie utilisée [25]. Son prix a légèrement

augmenté au fil des ans, mais il reste assez précieux. Ethereum, en tant que plateforme, utilise le même système de blockchain que Bitcoin mais ne se limite pas aux transactions pair-à-pair et va plus loin pour prendre en charge les contrats intelligents. Étant donné la variété des applications qu'Ethereum facilite, Ether a de nombreuses utilisations immédiates.

1.8.3 Vote

Blockchain peut transformer le système de vote traditionnel sur papier en un système numérisé et peut fournir une plate-forme de vote sécurisée servant de support à tout le processus ; voter, dépister et compter les votes et éviter des problèmes tels que la perte de registres et la fraude électorale. Les électeurs pouvaient compter les votes eux-mêmes et vérifier qu'aucun vote n'avait été supprimé, manipulé ou modifié [26].

1.8.4 Blockchain et l'écosystème de la santé

La blockchain a le pouvoir de faire une percée massive dans l'écosystème de la santé car elle peut facilement apporter des changements spécifiques dans la gestion des soins de santé du patient. Grâce à cette technologie, le pouvoir reviendra aux mains des gens. Cela signifie que les individus seront ainsi responsables de gérer leurs propres enregistrements, obtenant ainsi le contrôle global de leurs propres donnés [26].

1.9 Conclusion

La blockchain est essentiellement une technologie de stockage et de transmission d'informations sécurisées, telle qu'une base de données transmises, change une protection des données cryptées et permet l'historique de tous les échanges participants, ayant ses sessions de transfert de propriété ou encore l'authentification. Ces transactions s'effectuent au travers d'une chaîne de blocs qui contiennent des données, d'où le terme « bloc » - « chaîne ». Mais plutôt qu'une base de données traditionnelle, la blockchain propose un nouveau type de gouvernance décentralisée, intégrée et gérée par la technologie, sans intermédiaire qui nécessite un niveau de contrôle d'autorité.

Dans ce chapitre, nous avons présenté la blockchain et ses concepts, une nouvelle technologie révolutionnaire qui attire l'attention des chercheurs et des innovateurs du monde entier. La technologie ainsi que son fonctionnement, son ingénierie et ses composants, les différents types de blockchain et certaines applications de cette technologie dans la vie humaine sont aussi exposés dans ce chapitre.

Le fonctionnement de la blockchain est basé sur l'utilisation des primitives cryptographiques. Ces deniers et leurs utilisations dans la blockchain sont l'objectif de chapitre suivant.

CHAPITRE 2

PRIMITIVES CRYPTOGRAPHIQUES ET LA BLOCKCHAIN

2.1 Introduction

La cryptographie est la science qui utilise les mathématiques pour crypter et décrypter les données. Il vous permet de stocker ou de transmettre des informations confidentielles sur des réseaux non sécurisés (comme Internet), afin que personne d'autre que le destinataire ne puisse les lire. [27].

Avec l'avancement de la technologie, de nombreuses techniques complexes ont été utilisées pour protéger le message afin qu'aucune interférence ne puisse pénétrer l'information. Plusieurs algorithmes mathématiquement complexes tels que AES (Advanced Encryption Standard) et RSA (du nom de ses inventeurs Ron Rivest, Adi Shamir et Aldeman Len, qui ont inventé le principe en 1978) sont utilisés pour crypter et décrypter les données. En raison des progrès de l'informatique, la cryptographie a récemment été utilisée dans le développement de crypto-monnaies à partir de crypto-monnaies. La technologie Blockchain est identifiée comme la base de la crypto-monnaie bitcoin, et elle implémente une technologie de cryptage de haut ni-

veau telle que la cryptographie asymétriques, les fonctions de hachage, l'arbre Merkle, les signatures numériques, etc...

Ces techniques de cryptage avancées sont utilisées pour assurer la sécurité des données de la blockchain et pour la transmission sécurisée des informations, rendant la blockchain plus populaire et plus exigeante.

Dans ce chapitre, nous présentons des généralités sur les primitives cryptographiques puis nous présentons leurs utilisations dans la blockchain, en prenant le bitcoin comme exemple.

2.2 Généralités sur les primitives cryptographies

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité [28].

— **La confidentialité :** consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

— **L'intégrité :** vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.

— **L'authentification :** consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

— **Le non répudiation :** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction [28].

Les primitives cryptographiques jouent un rôle essentiel pour assurer la sécurité dans un blockchain. Avant de traiter leur utilisation pour ce but, nous présentons d'abord

des notions de base de la cryptographie liés au blockchain, tels que la cryptographie asymétrique, la signature numérique, la fonction de hachage et l'arbre de Merkel.

2.2.1 Cryptographie Asymétrique

La cryptographie asymétrique (à clés publiques) exige que chacun des correspondants possède une clé publiée dans un annuaire utilisée par tout le monde pour chiffrer des messages destinés à un individu particulier, et l'autre privée que cet individu est seul à détenir et qui lui permet de déchiffrer les messages qu'il reçoit [29]. Le fonctionnement de la cryptographie asymétrique peut être résumé comme suit :

- Un utilisateur écrit un message, et souhaite l'envoyer à un destinataire en s'assurant qu'aucun intermédiaire ne puisse le lire.
- Cet utilisateur comme le destinataire possèdent tous deux une paire de clés, et chacun connait la clé publique de l'autre.
- Afin de chiffrer un message pour le destinataire, l'utilisateur va alors utiliser la clé publique du destinataire.
- Cette clé active un algorithme, et le message écrit est alors transformé en texte incompréhensible, qui peut alors être envoyé au destinataire.
- Du côté du destinataire, et lorsqu'il reçoit le message chiffré, il devra utiliser sa propre clé privée, celle que lui seul déteint, afin d'activer l'algorithme pour le déchiffrer.
- Ainsi, même si quelqu'un intercepte le message en chemin, il ne pourra pas le déchiffrer, puisqu'il ne dispose pas de la clé privée du destinataire [29].

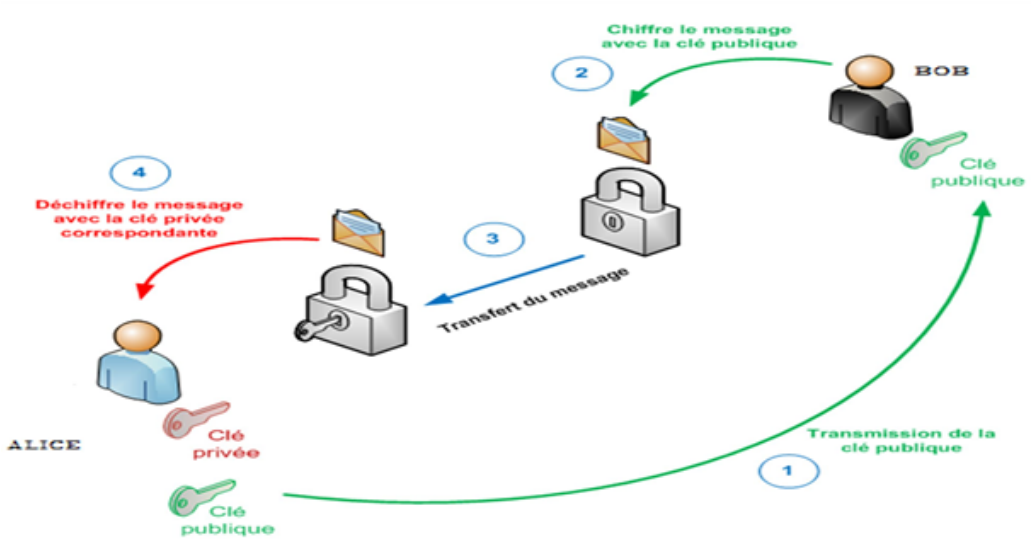

FIGURE 2.1 – ferme de minage
[30]

2.2.2 Signature numérique

La signature numérique est la méthode de cryptographie la plus sécurisée pour assurer la sécurité des informations. Pour prouver l'origine(authentification), l'intégrité des données et la non-répudiation du message, il est courant d'envoyer une signature numérique avec le message lui-même. Le processus de signature illustrer dans les étapes suivantes et la figure 2-2.

— Calcul de l'empreinte de hachage des données à signer.

— Chiffrement de l'empreinte à l'aide de la clé privée. On obtient alors la signature qui sera liée avec un certificat pour authentifie l'identité du signataire.

— Déchiffrement de la signature avec la clé publique. Cela permet de retrouver l'empreinte associée aux données signées.

— Calcul de l'empreinte des données signées. On vérifie que cette empreinte correspond à la précédente, auquel cas la signature est valide : les données sont donc intègres et l'identité de l'expéditeur est vérifiée [31].

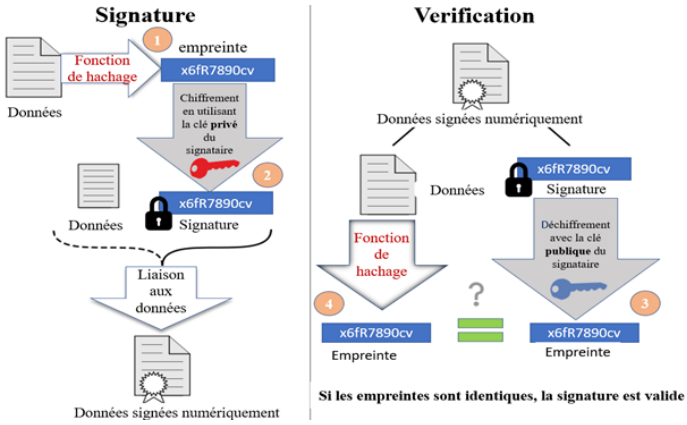

FIGURE 2.2 – Illustration de la signature et de la vérification d'un message [32]

2.2.3 Fonction de Hachage

La fonction de hachage cryptographie est une fonction mathématique qui prend n'importe quelle chaîne d'entrée (données) de n'importe quelle longueur et génère une chaîne alphanumérique de taille fixe [33]. La chaîne de sortie est appelée valeur de hachage ou empreinte numérique ou somme de contrôle. De plus, la sortie est de longueur fixe et unique. La fonction produit toujours le même hachage à partir des mêmes données malgré le nombre de recalcules. Le hachage ne peut pas être inversé pour obtenir l'entrée données (très difficile) et, par conséquent, il peut être utilisé pour vérifier l'intégrité des données. Ainsi, il est également appelé fonction de hachage unidirectionnelle. La fonction de hachage a trois propriétés principales :

— **Résistance à la collision :** cette propriété rend très improbable (probabilité très faible) que deux entrées aléatoires génèrent le même résultat de hachage et qu'il est impossible (par calcul) de trouver un ensemble de données différent qui génère le même résultat de hachage donné d'un autre ensemble de données malgré le recalcule plusieurs fois. Plus formellement, la résistance à la collision d'une fonction de hachage peut être définie comme suit : Il est très difficile de trouver deux entrées différents X, Y : Hash (x) = Hash (y).

— **Résistance à la pré-image :** la deuxième propriété stipule que la fonction de hachage doit être une fonction unidirectionnelle. Cette propriété implique qu'étant donné la sortie d'une fonction de hachage, il ne devrait y avoir aucun moyen de récupérer l'entrée d'origine [33].

— **Distribution uniforme :** : La troisième propriété indique que les résultats de hachage sont uniformément distribués dans l'espace de sortie. Étant donné une entrée aléatoire, la probabilité d'obtenir un résultat choisi est la même pour toutes les valeurs dans l'espace de sortie. Cela signifie que toutes les sorties possibles ont la même chance d'être "touchées" [33].

2.2.4 Arbre de Merkel

Un arbre de Merkel où arbre de hachage est une structure de données binaires arborescente qui permet de condenser un ensemble de blocs de données en un seul code de hachage au moyen d'une fonction de hachage cryptographique. Les feuilles contiennent les valeurs à stocker et les autres nœuds internes sont le hachage de ses deux fils [34].

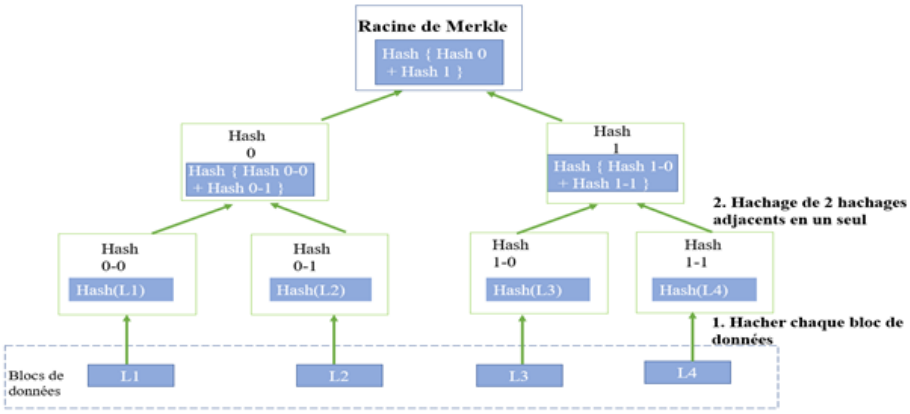

FIGURE 2.3 – Représentation de l'arbre de Merkel [33]

2.3 Utilisation de cryptographie dans la blockchain

Dans cette section nous prendrons l'exemple de la crypto-monnaie Bitcoin. Le protocole de la blockchain se fonde sur des primitives cryptographiques alors déjà connus et étudiés : la signature numérique à clé publique fondée sur des algorithmes asymétriques, les algorithmes de hachage et l'arbre de Merkel [35].

2.3.1 La cryptographie asymétrique dans la blockchain

La cryptographie asymétrique est un élément fondamental de la technologie blockchain. C'est la technologie sous-jacente pour les portefeuilles et les transactions.

2.3.1.1 Cryptographie asymétrique dans les portemonnaies (ou portefeuilles ou wallets)

- Les portefeuilles sont des conteneurs clés, dont la plupart sont implémentés sous forme de fichiers ou de bases de données structurés très simples [2].
- Lorsqu'un utilisateur crée un portefeuille, il génère des paires de clés publique-privée.
- L'utilisation d'un ensemble de clés permet de garantir l'anonymat de l'utilisateur lors de l'envoi de transactions.
- Alors, les portemonnaies bitcoin contiennent des clefs, pas de l'argent.
- Chaque utilisateur a son propre portefeuille pour gérer ses clés.
- Bitcoin utilise la cryptographie à clef publique pour générer une paire de clefs qui permet de contrôler les fonds : une clef privée, et une clef publique dérivée à partir de la clef privée.
- La clef publique est utilisée pour recevoir des bitcoins, et la clef privée pour signer des transactions qui dépensent ces bitcoins.
- Il existe une relation mathématique entre la clef privée et la clef publique qui permet d'utiliser la clef privée pour signer un message, et la clef publique pour valider cette signature sans révéler la clef privée.

— Pour le bitcoin, la clé privée est un nombre, généralement aléatoire.

— La clé publique est générée à partir de la clé privée en utilisant la multiplication de courbes elliptiques, une cryptographie irréversible.

— On utilise ensuite une fonction de hachage cryptographique pour générer pour chaque clé publique une adresse qui est une chaîne de chiffres et de lettres générée à partir de la clé publique.

— En raison de la nature de la technologie blockchain, cette adresse est publique pour tout le monde et peut être utilisée pour vérifier le solde de ce portefeuille ou lui envoyer des pièces [2].

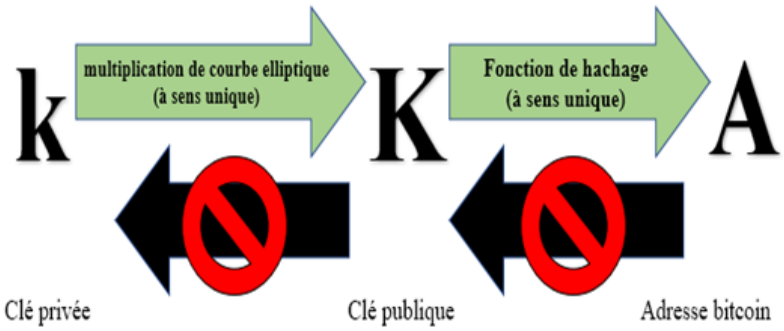

FIGURE 2.4 – Clef privée, clef publique et adresse bitcoin [2]

2.3.1.2 Cryptographie asymétrique dans les transactions

— Une transaction " Prenez X pièces de mon portefeuille et créditez X pièces dans un autre portefeuille ", nécessite une signature d'une clé privée du portefeuille expéditeur pour être valide.

— Après la diffusion, n'importe qui peut utiliser la clé publique associée pour s'assurer que la signature numérique provenant de la clé privée est authentique.

— C'est l'un des rôles des validateurs de bloc avant d'ajouter une transaction à la blockchain.

On peut trouver plusieurs types de portemonnaie expliqué dans les lignes suivantes [2] :

1. **Portemonnaie non-déterministes (aléatoires)** Dans les premiers clients bitcoin, les portemonnaies gêneraient leurs clefs privées de façon aléatoire. Ce type de portemonnaie est appelé portemonnaie non-déterministe de type 0. Par exemple, un client Bitcoin génère 100 clefs aléatoires lors de sa première utilisation, et génère ensuite d'autres clefs si nécessaire.
   - Ils sont difficiles et fastidieux à gérer (sauvegarde, import de clefs, ...) et on les remplace de plus en plus par des portemonnaies déterministes.
   - Le problème avec les clefs aléatoires est qu'il faut toutes les sauvegarder, sinon les fonds associes sont perdus.
   - Les portemonnaies non-déterministes de type 0 sont un mauvais choix, surtout si l'on veut éviter de réutiliser les mêmes adresses (ce qui oblige à générer beaucoup de clefs, et sauvegarder son portemonnaie fréquemment).
2. **Portemonnaies déterministes**
   - Les portemonnaies déterministes contiennent des clefs privées qui sont toutes dérivées d'une même "graine" (valeur d'initialisation) grâce à une fonction de hash à sens unique.
   - Les clefs privées sont dérivées à partir de cette graine (qui est un nombre aléatoire) et d'autres données, telles que l'index de la clef ou son "code chaine" ("chaincode").
   - La graine est suffisante pour retrouver toutes les clefs d'un portemonnaie déterministe, et on peut donc ne faire qu'une seule sauvegarde, au moment de la création du portemonnaie. On n'a besoin que de cette graine pour exporter/importer les clefs, ce qui facilite les transferts entre différents portemonnaies [2].

3. **Portemonnaie déterministe hiérarchique**

   — Les portemonnaies déterministes appelés portemonnaie HD (HD pour Hierarchical Deterministic en anglais) ont été créés pour faciliter la dérivation de multiples clefs privées à partir d'une "graine" unique.

   — Les portemonnaies déterministes hiérarchiques permettent de gérer des arbres de clefs : une clef parent peut générer une série de clefs filles, qui peuvent elles-mêmes générer une série de clefs filles, et ainsi de suite sans limite de profondeur. Cette structure en arbre est illustrée ici

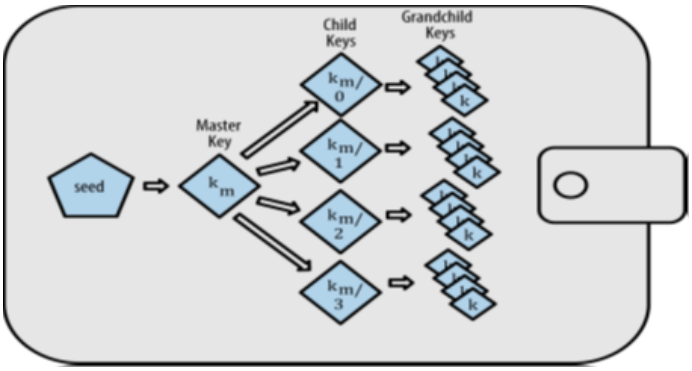

FIGURE 2.5 – Portemonnaie déterministe hiérarchique
[2]

2.3.2 La signature numérique dans la blockchain

Une deuxième application de la cryptographie asymétrique est celle de signature numérique. Ce dernier est le produit d'une cryptographie asymétrique et constituent un excellent moyen d'établir la confiance entre les parties dans un environnement sans confiance [36].

— Les signatures numériques sont utilisées dans la couche applicative de la blockchain.

— Elles sont principalement utilisées pour valider les événements dans les transactions qui sont insérées dans les blocs.

— Une signature numérique est utilisée dans la blockchain pour signer la transaction, authentifiant ainsi l'expéditeur prévu et assurant l'intégrité de la transaction ainsi que la non-répudiation de l'expéditeur, car la vérification peut être effectuée par toute personne qui possède la clé publique de la paire de clés publique-privée générée.

— La signature numérique dans Bitcoin est utilisée pour fournir la preuve du propriétaire de la clé privée sans avoir à la révéler (prouve donc qu'il est autorisé à dépenser les fonds associés). De plus, une signature numérique garantit que personne ne peut modifier la transaction après l'avoir signée [36].

— Une signature numérique est nécessaire pour le transfert de fonds et l'interaction avec le réseau Bitcoin [37].

— Dans Bitcoin, nous avons la transaction (comme un message) et la clé privée, qui est utilisée comme clé de signature pour le message (la transaction).

— Dans Bitcoin, chaque entrée peut être signée indépendamment. Cela signifie que les signatures numériques respectives ne doivent pas nécessairement appartenir aux mêmes propriétaires. Cela permet de créer certaines transactions appelées coinjoin, auxquelles plusieurs propriétaires participent pour créer un système de transaction à confidentialité renforcée [37].

La signature numérique est l'une des primitives cryptographiques les plus importantes qui rend la blockchain publiquement vérifiable et avec un consensus réalisable. Les schémas de signature sont utilisés dans presque toutes les blockchains. La figure 2-6 représente un exemple général sur la façon dont un utilisateur de blockchain (signataire) crée une transaction ou un bloc signé numériquement à l'aide de sa clé privée [38].

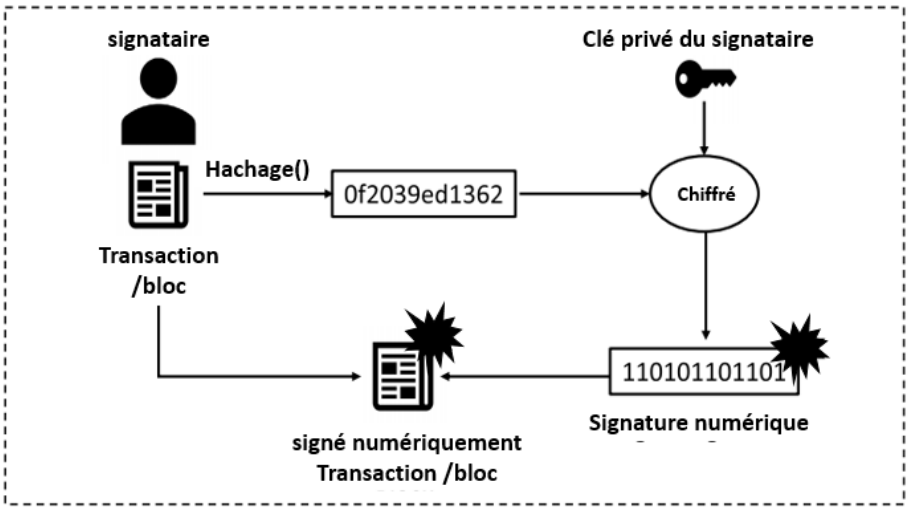

FIGURE 2.6 – Processus de signature de la transaction/bloc blockchain. [38]

De plus, la figure 2-7 montre comment d'autres nœuds de blockchain (vérificateur) vérifient si la signature de la transaction ou du bloc est valide ou non à l'aide de la clé publique du signataire.

Blockchain applique différents schémas de signature pour fournir des fonctionnalités supplémentaires telles que la confidentialité, l'anonymat et la dissociation. Le schéma de signature peut également être appliqué pour générer une signature de taille constante en utilisant l'agrégation de signatures [39].

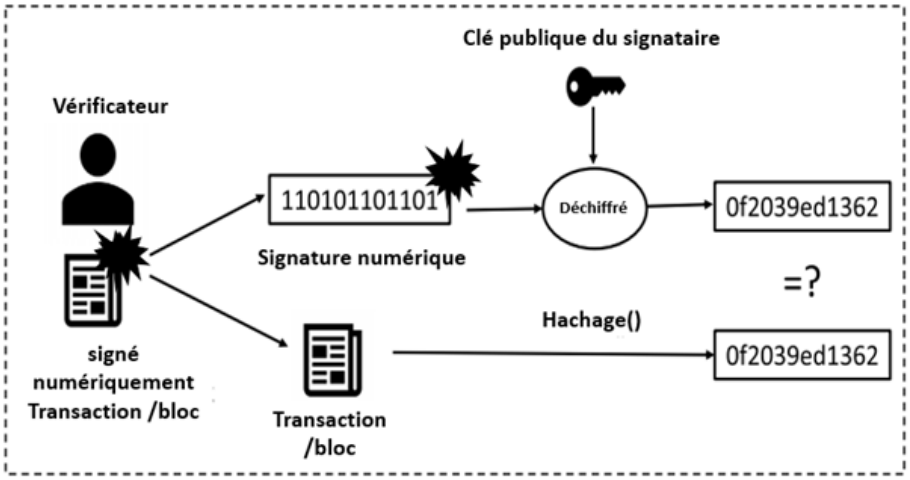

FIGURE 2.7 – Vérification de la transaction/bloc signé numériquement [38]

Certains des schémas de signature appliqués dans la blockchain sont :

— **Multi-Signature :** Dans un schéma de multi-signature, un groupe d'utilisateurs signe un seul message. Dans un réseau blockchain, lorsqu'une transaction nécessite une signature d'un groupe de participants, il peut être avantageux d'utiliser un schéma de multi-signature. Les plates-formes Blockchain telles que **Openchain** et **MultiChain** [40] prennent en charge le schéma multi-signature M-of-N qui réduit le risque de vol en tolérant la compromission de jusqu'à M-1 clés cryptographiques. Boneh et al. A également conçu des multi-signatures compactes pour des blockchains plus petites [41].

— **Signature aveugle :** dans ce schéma, les signatures sont utilisées dans des protocoles liés à la confidentialité où le signataire et les auteurs du message (transaction en cas de blockchain) sont des parties différentes. Les signatures aveugles sont utilisées pour assurer la dissociation et l'anonymat du Transaction. Dans une configuration blockchain, une signature aveugle peut être utile pour fournir l'anonymat et la dissociation lorsque la partie effectuant la transaction et la partie signataire sont différentes. Les signatures aveugles sont également testées dans Bitcoin pour assurer l'anonymat des transactions Bitcoin

en chaîne et hors chaîne [42].

— **Signature en anneau :** ce schéma utilise un protocole dans lequel une signature est créée sur un message par tout membre d'un groupe au nom du groupe tout en préservant l'identité du signataire individuel de la signature. Les signatures en anneau sont utilisées pour garantir l'anonymat du signataire dans le réseau blockchain. La technologie CryptoNote (est un protocole conçu pour être utilisé avec des crypto-monnaies qui vise à résoudre des problèmes spécifiques identifiés dans Bitcoin) utilise un schéma de signature en anneau pour créer des paiements introuvables dans les crypto-monnaies [43].

— **Signature à seuil :**ce schéma de signature est une signature à seuil (t ; n) où n parties reçoivent une part de la clé secrète pour créer la signature et t parties sur n créent une signature sur n'importe quel message. Comme les parties construisent directement la signature à partir des actions, la clé n'est jamais révélée dans l'ensemble du schéma. La signature de seuil peut être utile pour assurer l'anonymat dans le réseau blockchain [44].

2.3.3 Utilisation des Fonctions de hachage dans la blockchain

Chaque bloc, possède un identifiant (case à fond noir du bloc 90 dans le schéma ci-après), qui prend la forme d'un « hash » permettant de relier les blocs les uns aux autres. Cet hash est toujours le résultat du « hachage » du bloc précédent [45].

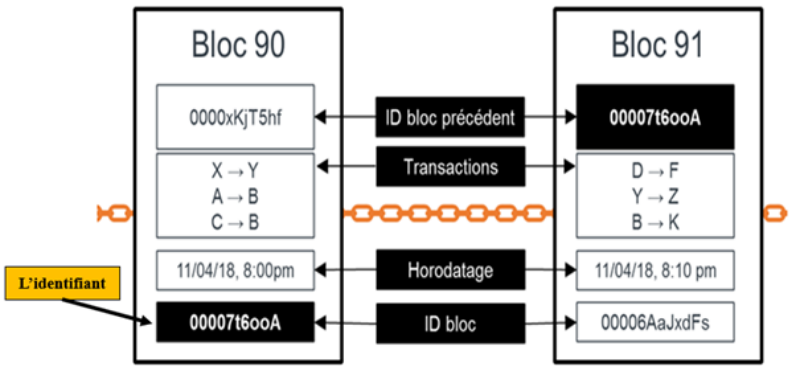

FIGURE 2.8 – Deux blocs relié et le rôle des haschs
[45]

Dans le cas d'une chaîne de bloc, le hachage est effectué à partir du contenu du bloc, c'est-à-dire le hash du bloc précédent, un certain nombre de transactions et un horodatage.

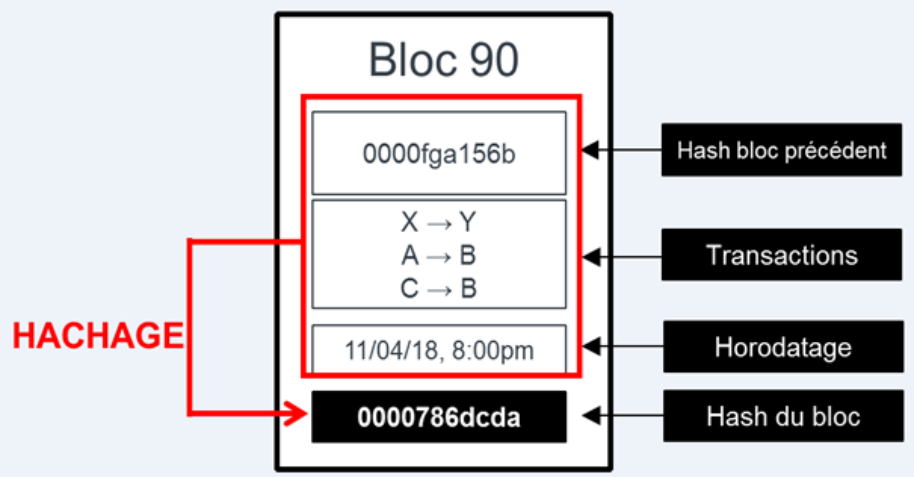

FIGURE 2.9 – Le rôle des haschs dans les blocs
[45]

La modification étant visible dans l'ensemble des blocs suivants, les blocs sont tous liés entre eux cryptographiquement. En conséquence, modifier le contenu d'un

bloc suppose de recalculer les haschs de tous les blocs qui le suivent [45].

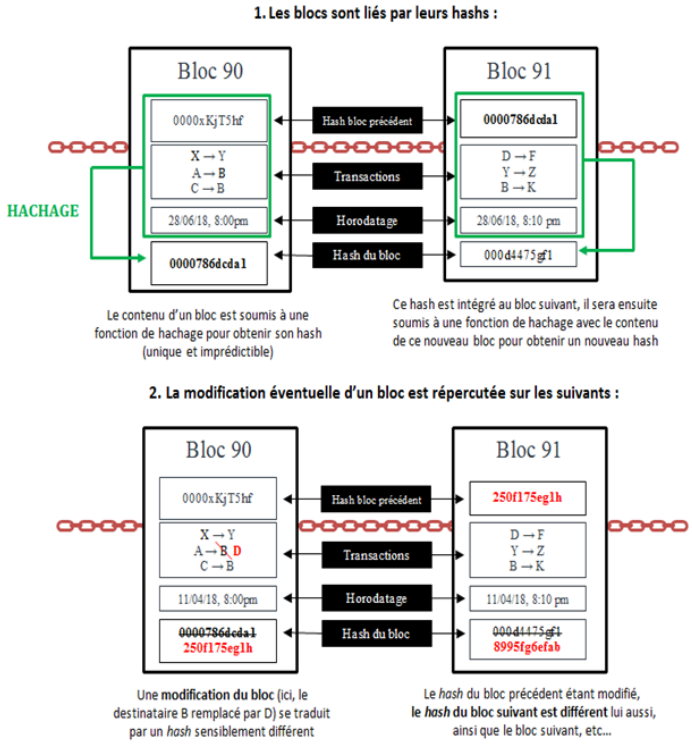

FIGURE 2.10 – Le rôle du hachage dans l'intégrité de la chaîne de blocs [45]

Les fonctions de hachage cryptographique dans la blockchain sont utilisées à diverses fins telles que :

— Résoudre des énigmes cryptographiques (le Proof of Work (PoW) en Bitcoin.

— Génération d'adresses (pour les clés publiques et privées).

— Résumés de message dans les signatures.

Les fonctions de hachage cryptographiques les plus populaires utilisées dans les blockchains sont SHA-2 (en particulier la variante SHA256 - une variante qui produit des sorties de 256 bits) [38]. Une manière typique dont les fonctions de hachage cryptographiques sont utilisées dans les conceptions de blockchain est sous la forme d'un mode de fonctionnement, c'est-à-dire une combinaison de plusieurs invocations d'une

même fonction de hachage ou de différentes fonctions. Par exemple, dans Bitcoin [38], SHA256 est utilisé deux fois et cette construction est appelée SHA256d, c'est-à-dire SHA256d(message) = SHA256(SHA256(message))

2.3.3.1 Résoudre des énigmes cryptographiques (le Proof of Work (PoW) en Bitcoin

Dans le cas du bitcoin, la cible est un nombre de 256 bits qui peut être trouvé dans l'en-tête de chaque bloc et sa valeur diffère d'un bloc à l'autre [16]. La fonction de hachage cryptographique utilisée pour hacher les données à l'intérieur d'un bloc dans PoW est SHA256, la formule suivante décrit son fonctionnement :

H [H (Version | Bloc Hash précédent | Racine Merkel | Horodatage | Cible de difficulté | Nonce)] < [Cible de difficulté]

2.3.3.2 Génération d'adresses (pour les clés publiques et privées)

Nous résumons dans cette section, les différentes étapes de génération d'adresses (voir la figure 2.11) :

1. Génération d'une clé privée aléatoirement, et sa transformation en Base 58 de clé privée. La base 58 permet d'afficher le hachage de manière plus compacte [46].
2. Obtenez la clé publique associée en fonction de la clé privée (en utilisant les courbes elliptiques)
3. Application de la fonction de hachage SHA-256 sur la clé publique (doit décoder l'hexadécimal avant SHA-256) créée à l'étape 2.
4. Application de la fonction de hachage RIPEMD-160 sur le résultat de l'étape 3 (SHA-256 de la clé publique).
5. Ajoutez le préfixe d'octet de version à l'étape 4, qui est utilisé pour définir différents formats d'adresse — 00 est l'octet de version (0x00 pour le réseau principal).

6. Appliquer la fonction de hachage SHA-256 deux fois sur le résultat de l'étape 5 (SHA-256(SHA-256 (ripemd-160WithVersionByte))).
7. Double hachage SHA-256 pour le hachage RIPEMD-160 avec l'octet de version.
8. Obtenez les 4 premiers octets de mot résulte de l'étape 7, qui présente « somme de contrôle ».
9. Ajoutez la somme de contrôle (étape 8) à la fin du hachage RIPEMD-160 avec l'octet de version (étape 5).
10. Appliquer et convertir l'adresse Bitcoin binaire à l'aide de la fonction Base58 au format d'adresse Bitcoin [46].

FIGURE 2.11 – Les étapes de génération d'adresses Bitcoin [46]

2.3.3.3 Résumés de message dans les signatures

Les fonctions de hachage sont une partie vitale des algorithmes de signature numérique.

Les fonctions de hachage dans une blockcahin peuvent être utilisées pour résumer les messages en préservant leur intégrité. Un algorithme de résumé de message qui est une fonction de hachage, est une procédure qui mappe des données d'entrée d'une longueur arbitraire à une sortie de longueur fixe.

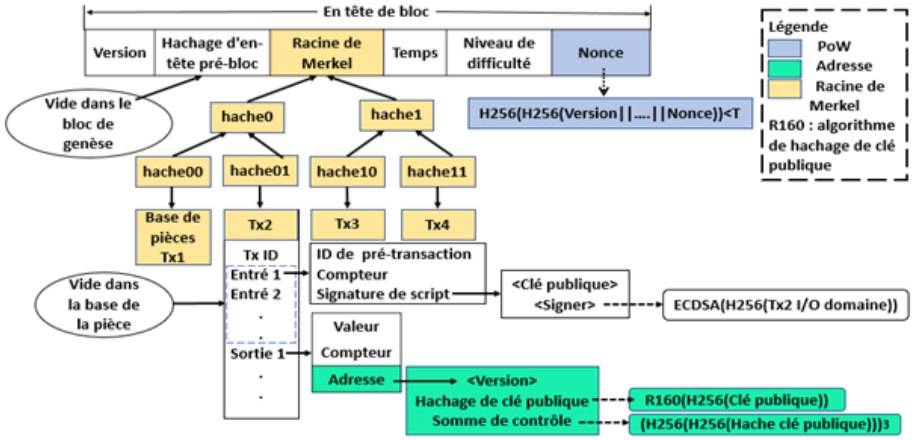

FIGURE 2.12 – Utilisations de la fonction de hachage dans Bitcoin [47]

2.3.4 L'arbre de Merkel dans la blockchain

L'arbre de Merkel est une unité fondamentale dans la blockchain, elle est utilisée pour organiser le stockage des transactions dans chaque bloc. La figure 2-13 montre comment un arbre de Merkel est utilisé pour calculer le hachage d'un bloc. Tout d'abord, un arbre binaire est formé avec les hachages des transactions individuelles comme feuilles. Ceux-ci sont désignés par Hachage 0, ... Hachage 3 sur la figure. Un arbre binaire est un graphe orienté, où chaque parent a deux enfants. Le hachage du nœud parent est le hachage de ses deux enfants, eux-mêmes des hachages. Ceci est illustré à la Figure 2-13, où Hachage 01 = Hachage (Hachage0 + Hachage1) et

Hachage est la fonction de hachage SHA256. Finalement, le hachage du nœud racine, le hachage racine ou la racine Merkel, est calculé. Avec cette racine Merkel, l'en-tête de bloc peut maintenant être assemblé [48].

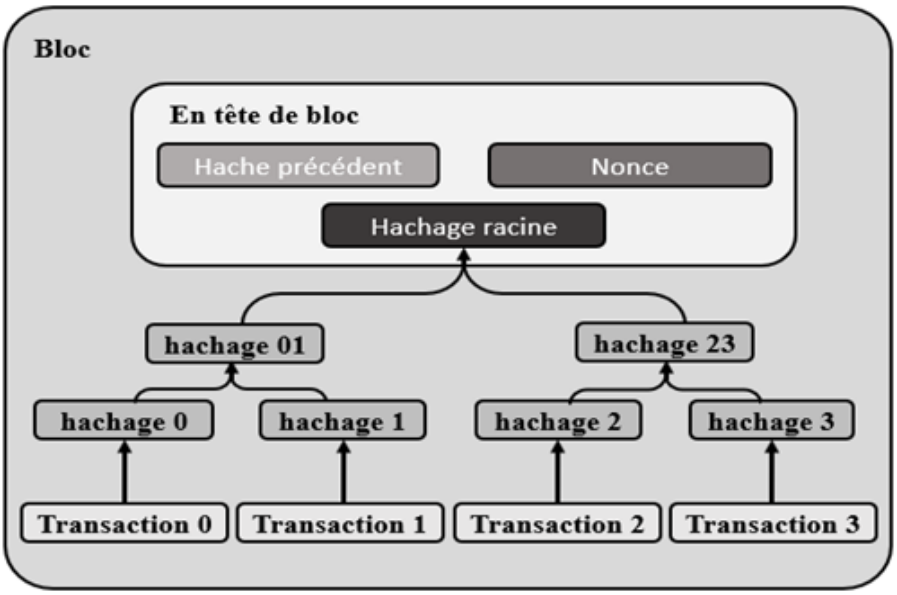

FIGURE 2.13 – Arbre Merkel des transactions dans un bloc [48]

— L'en-tête de bloc contient le hachage du bloc précédent dans la blockchain, la racine de l'arbre Merkel des transactions et le nonce inclus par le mineur. Le hachage du bloc est alors le hachage de l'en-tête du bloc uniquement : les transactions sont représentées dans ce hachage via la racine de l'arbre Merkel.

— • L'un des grands avantages de l'utilisation des arbres Merkel est la vérification des transactions. Supposons qu'un nœud veuille vérifier qu'une transaction, disons Transaction 3, appartient à un bloc comme dans la figure 2-14. Un nœud peut effectuer cette opération dans un temps qui est lié de manière logarithmique au nombre de nœuds dans l'arbre. Suivant la Figure 2-14, le nœud n'a qu'à calculer Hachage 3, Hachage 23 et le hachage racine, et vérifier le résultat par rapport au hachage racine stocké dans le bloc [48].

— Cette structure est très utile pour prouver que toute une chaîne de transaction est restée inchangée. Grâce à la chaîne de hachage cryptographiques, il est en effet possible de remonter jusqu'à la transaction recherchée et s'assurer que toute la branche (depuis la racine jusqu'à la transaction) n'a pas été modifiée.

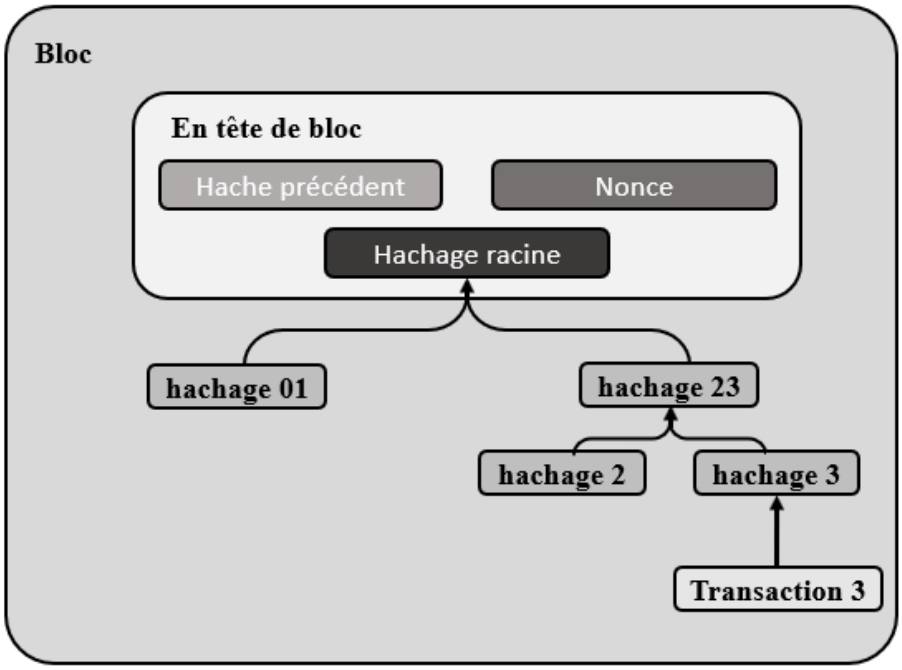

FIGURE 2.14 – Élagage des transactions dans un bloc
[48]

C'est-à-dire que le nœud n'a qu'à vérifier la branche Merkel, la partie de l'arbre qui permet de prouver cryptographiquement qu'une transaction est incluse dans l'arbre.

2.4 Conclusion

La cryptographie est un excellent outil pour accomplir certaines des tâches requises pour remplacer les tiers de confiance et créer un environnement non fiable dans un réseau décentralisé.

La cryptographie est également cruciale pour le succès de la technologie blockchain, la plupart des primitives cryptographiques ont un rôle ou un autre dans la création d'une application blockchain décentralisée.

La cryptographie utilisée dans la blockchain qui donne une identité aux participants du réseau et prouver la propriété des actifs. Les signatures numériques sont utilisées pour signer et vérifier des événements tels que des transactions. Le hachage est utilisé dans la plupart des applications blockchain pour créer des liens entre les blocs. Il est également utilisé dans des algorithmes de consensus tels que Proof of Work, qui exploitent principalement la puissance de hachage des systèmes informatiques qui composent le réseau blockchain. Arbres Merkel organisent les transactions tout en permettant aux blockchains d'être plus efficaces.

Après la présentation de tous ces concepts liés aux primitives cryptographiques dans une blockchain, le prochain chapitre est consacré à la exposition de notre proposition atour de la réalisation et sécurisation d'un portefeuille déterministe.

CHAPITRE 3

RÉALISATION ET SÉCURISATION D'UN PORTEFEUILLE DÉTERMINISTE

3.1 Introduction

Le fonctionnement de blockchain est très lié à l'utilisation des clés numériques (privées et publiques), des adresses publiques et des signatures électroniques.

Pour le bitcoin, les clés ne sont pas stockées sur le réseau, mais sont plutôt créées et stockées par les utilisateurs dans un fichier, sous forme d'une base de données basique qui est le portefeuille. Les clés d'un portefeuille sont totalement indépendantes du protocole bitcoin, et peuvent être créées et gérées par un logiciel tiers, indépendamment de la blockchain et même sans accès à Internet [2]. Ce sont ces clés qui rendent possibles de nombreuses caractéristiques intéressantes de bitcoin, comme le contrôle et la confiance décentralisée, la preuve de propriété, et le modèle de sécurité protège par la cryptographie. Pour le bitcoin, un portefeuille est sécurisé par un mot de passe. Si quelqu'un d'autre que le propriétaire possède ce mot de passe, il peut

avoir une copie des clés et peut utiliser les fonds qui y sont associés. Basée sur la blockchain pour l'authentification des utilisateurs, cette gestion de l'identité tout en préservant la vie privée est un problème difficile. Dans la littérature, on trouve que peu de travaux qui traitent ce point.

Dans [49], le système proposé se compose de trois rôles principaux, à savoir, Utilisateur (U), Centre d'enregistrement (RC), Serveur d'authentification (AS). Un nouveau membre introduit par RC, est autorisé à rejoindre le réseau avec l'acceptation de la majorité des membres du forum existant (consensus). Une fois le minage réussi, les informations d'identité de l'utilisateur (IDInfo), présenté par ses données biométriques plus d'autres données, seront mises à jour sur le grand livre de la blockchain. L'utilisateur utilise ces informations pour prouver son identité auprès de n'importe quel serveur d'authentification AS sans l'aide de RC. Pour la génération des clés, les auteurs de [49] proposent une méthode basée sur un extracteur flou (fuzzy extractor).

Dans ce chapitre, nous présentons une méthode pour gérer un portefeuille déterministe en assurant la sécurisation de ce dernier et la génération des clés, en basant sur les données biométriques et d'autres données supplémentaires.

3.2 Problématique

Pour un bon fonctionnement d'une blockchain de crypto-monnaie, on doit avoir une bonne méthode pour gérer et sécuriser le portefeuille (portemonnaie).

— Les portefeuilles sont les points d'accès à un réseau de crypto-monnaie. Si on perde l'accès au portefeuille, on perde l'accès aux clés privés et aux fonds y associés. Alors, une bonne sécurisation des portefeuilles assure la sécurité des fonds de crypto-monnaie.

  En générale, ces portefeuilles sont protégés par des mots de passe, qui peuvent être faibles et facilement cassables. Cette nature des mots de passe est un point faible pour la sécurisation des portemonnaies.

— D'autre part, les portefeuilles permet de générer les clés privées, clés publiques

et adresses publiques. Une mauvaise méthode de génération des clés implique une difficulté importante pour gérer ces clés (sauvegarde, import de clefs, ...).

3.3 Idée et proposition

Il est connu que l'utilisation des données biométrique est plus sécurisée que l'utilisation des mots de passe qui peut être oublié ou volé. La biométrie peut fournir un niveau élevé d'unicité et de sécurité. Mais, l'utilisation des systèmes biométriques entraîne d'autres problèmes de sécurité et de confidentialité. Premièrement, la biométrie est généralement difficile à modifier, de sorte qu'elle n'est pas révocable une fois qu'elle a été compromise. Si un adversaire vole les informations biométriques de l'utilisateur (qui peuvent être présentées par un vecteur de caractéristiques sauvegardé sur un support), l'utilisateur peut perdre la sécurité pour toujours [50]. D'autre part, la précision de la reconnaissance a un impact significatif sur la décision des systèmes biométriques. Par exemple, des dispositifs biométriques de faible précision peuvent fournir des informations inexactes indiquant qu'un utilisateur illégal est capable de passer l'authentification.

Pour ces raisons, nous proposons une méthode de sécurisation des portefeuilles et génération des clés basée sur les données biométriques en les combinant avec des données suplémentaires. Les détails de notre proposition sont présentés dans les lignes suivantes. Mais avant de les présenter, nous signalons que notre proposition peut être utilisée pour une blockchain hybride.

3.3.1 Sécurisation de portefeuille par utilisation des données biométriques et des données supplémentaires

Basant sur l'idée présentée dans [49], dans notre système, un utilisateur possède une carte intelligente (smart carte), contient les informations présentes dans la figure 3.1. Plus que les données biométriques, un mot de passe et un nombre aléatoire sont utilisés comme des données supplémentaires. L'insertion de ces données supplémentaires permet de créer une autre carte si elle est perdue ou volée.

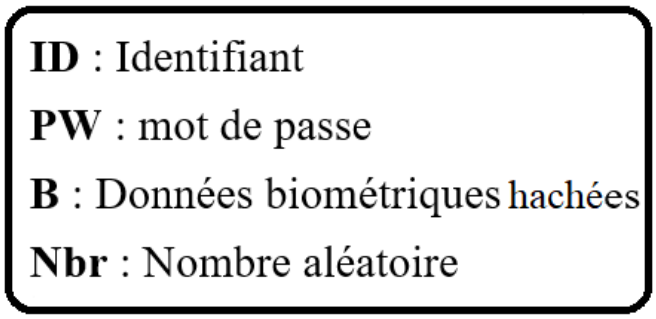

FIGURE 3.1 – carte d'identification

L'utilisation de notre système passe par la phase d'enregistrement et la phase d'authentification.

a. Phase d'enregistrement

L'utilisateur est premièrement enregistré au niveau de centre d'enregistrement, en présentant ses données biométriques, et en fournissant les données supplémentaires. Après cette phase, l'utilisateur possède une smart carte.

b. Phase d'authentification

Les étapes de l'authentification sont décris comme suit :

— L'utilisateur insére la carte (qui contient les données biométrique haché **B**, identifiant **ID**, mot de passe **PW**, nombre aléatoire **Nbr**) dans le lecteur de la carte.

— Capture ses données biométriques vivantes **B'** par le capteur biométrique.

— Les données B et B' sont comparées. S'il y a une différence dans le hachage, la carte est rejetée, et la connexion est échouée. Si non, on continue le processus de l'authentification.

— Ensuite, l'utilisateur envoi les données **(ID, h(PW,ID,B,Nbr)** au serveur qui a sauvegardé les informations des cartes, où h() est une fonction de hachage.

— Le serveur compare les données réceptionnées avec celles enregistrées.

3.3.2 Génération des clés par utilisation des données biométriques

Bitcoin utilise un générateur aléatoire pour gérer une clé privée. En général, ce générateur est initialisé par des données aléatoires produites par l'utilisateur. La clef publique est calculée à partir de la clef privée en utilisant la multiplication en courbes elliptiques.

Dans notre proposition, le schéma initial est présenté dans la figure suivante :

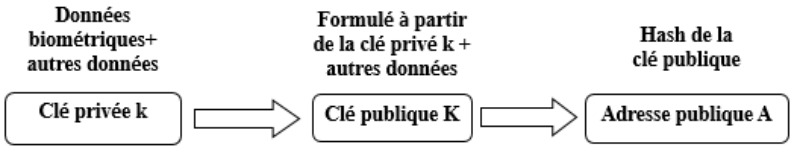

FIGURE 3.2 – Génération des clés par utilisation des données biométriques

D'autre côté, et dans un algorithme de génération de clef déterministe, chaque clef privée est dérivée, grâce à une fonction a sens-unique, d'une clef précédente, créant ainsi une chaîne de clefs. Il suffit ainsi de connaître la première clef (clef maître) pour recréer la chaîne et générer toutes les clefs.

Notre proposition s'articule sur la réalisation d'un portefeuille déterministe, d'où le détaille de notre proposition est présentés dans les lignes suivantes.

3.3.2.1. Génération de la clé maitre (ou la graine)

Pour ne pas utiliser uniquement les données aléatoires pour générer les clés privées, notre proposition est basée sur l'utilisation des données biométriques en les concaténant avec d'autres données. Pour générer la clé maître (la graine), nous proposons l'utilisation de la formule suivante :

— **Graine= h (B, ts, Nbr).**

B : hachage des données biométriques enregistrées sur la carte intelligente.

Ts : temps universel.

Nbr : nombre aléatoire.

3.3.2.2. Composition des clés de portefeuille déterministe

Comme il est connu, dans un portefeuille déterministe, l'ensemble des clés privées est généré à partir d'une graine.

— **Génération des clés privées**

Dans notre proposition, les clés privées sont générées de la graine concaténée avec un décalage de cette dernière, pour la première clé, et à partir de la clé précédente concaténé avec un décalage de cette dernière pour les autres clés, comme il est présenté avec les formules suivantes :

$$\text{Clé Privé}(1)=h(\text{ Graine . Décalage (Graine)})$$
$$\text{Clé Privé}(i)=h(\text{Clé Privé}(i)\text{-1 . Décalage (Clé Privé}(i)\text{-1))}$$

— **Génération de la clé publique**

La clé publique pour chaque clé privée est générée par la formule suivante :

$$\text{Clé publique} = h\ (\text{ID}, h\ (\text{clé privé}))$$

— **Génération de l'adresse**

L'adresse pour chaque clé publique et définie comme suit :

$$\text{Adresse publique} = h(h(\text{Clé publique}))$$

3.4 Analyse et discutions

Notre proposition permet d'avoir un portefeuille déterministe avec un niveau de sécurité plus élevé. Dans cette section, nous discutons l'intérêt de notre proposition concernant utilisation des données biométriques et supplémentaire, ainsi que génération des clés.

3.4.1 Authentification

3.4.1.1 Utilisation des données biométriques

L'utilisation des données biométrique est plus sécurisée que l'utilisation des mots de passe qui peut être oubliés ou volés. La biométrie peut fournir un niveau élevé d'unicité et de sécurité.

Au lieu d'utiliser un mot de passe pour accéder au portefeuille, l'accès est assuré par une comparaison des données biométriques réelles avec celle enregistrées, en passant par une vérification des données supplémentaires au niveau de serveur d'enregistrement.

3.4.1.2 Utilisation des données supplémentaires (mot de passe, nombre aléatoire)

L'utilisation des données supplémentaires permet de garder la possibilité d'utiliser les données biométriques dans le cas de perte ou vol de la carte. Dans ces deux cas, on peut régénérer une autre carte en modifiant ces données.

3.4.2 Génération des clés

Notre méthode de génération des clés permet de les générer d'une façon déterministe à partir d'une **graine**. Cela signifie qu'on ne doit pas sauvegarder toutes les clés, donc on minimise l'espace de sauvegarde. De plus, la graine utilise les données biométriques (avec un nombre aléatoire et le temps universel) ce qui permet de générer une graine plus solide qu'une autre basée seulement sur l'utilisation d'un nombre aléatoire.

3.5 Implémentation et environnent de développement

Pour développer notre application, nous avons utiliser les outils présentés dans le lignes suivantes.

3.5.1 Langages de programmation

Dans notre application, nous avons utilisé les langages suivants :

— **Python version 3.7 :** Python est un langage de programmation interprété, orienté objet et de haut niveau avec une sémantique dynamique. Ses structures de données intégrées de haut niveau, associées à un typage dynamique et à une liaison dynamique, le rendent très attractif pour le développement rapide d'applications, ainsi que pour une utilisation en tant que langage de script ou de collage pour connecter des composants existants entre eux. La syntaxe simple et facile à apprendre de Python met l'accent sur la lisibilité et réduit donc le coût de la maintenance du programme. Python prend en charge les modules et les packages, ce qui encourage la modularité du programme et la réutilisation du code. L'interpréteur Python et la bibliothèque standard étendue sont disponibles sous forme source ou binaire sans frais pour toutes les principales plates-formes, et peuvent être librement distribués.

— **HTML 5 (HyperText Markup Langage 5) :** est une version du HTML (format de données conçu pour représenter les pages web). Cette version a été finalisée le 28 octobre 2014.

— **CSS3 :** est signifie Feuilles de style en cascade, utilisé pour augmenter la fonctionnalité et la polyvalence, et une performance efficace du contenu du site. Il permet la création des sites Web riches en contenu qui ne nécessitent pas beaucoup de poids ou de codes, cela se traduit par des graphiques et des animations plus interactifs, une interface utilisateur supérieure, une organisation beaucoup plus importante et un temps de téléchargement plus rapide.

— **Flask :** est un Framework d'application Web WSGI (Web Server Gateway Interface) léger. Il est conçu pour faciliter et accélérer la mise en route, avec la possibilité de s'adapter à des applications complexes.

3.5.2 IDE

Nous avons utilisé jetBrains PyCharm 2020 (développé par l'entreprise tchèque JetBrains), qui est un environnement de développement intégré utilisé pour programmer en Python. Il permet l'analyse de code et contient un débogueur graphique. Il permet également la gestion des tests unitaires, l'intégration de logiciel de gestion de versions, et supporte le développement web avec Flask.

3.6 Structure de blockchain adopté

Notre application permet de réaliser un portefeuille déterministe. Ce portefeuille est ensuite utilisé pour accéder à une blockchain de crypto-monnaie. Dans cette section nous présentons la structure des transactions et des blocks adaptées.

3.6.1 Structure de transaction

Chaque transaction contient les champs suivants :

— Une clé publique de l'expéditeur

— Adresse publique de l'expéditeur.

— Adresse publique de destinataire.

— Montent a envoyé.

3.6.2 Structure de bloc

Le bloc dans la Blockchain implantée ayant la structure suivante :

— **N° de bloc :** l'ordre de bloc dans la blockchain.

— **Hash**(hachage) : Le hash de bloc.

— **Hash du bloc précédent :** Le hash des données de bloc précédent.

— **Nonce :** est le nombre de cycle pour que le mineur obtient le hachage généré.Dans notre implantation, La solution est la génération d'une hache qui commence par 2 zéros.

— **Temps :** l'horodatage de validation du bloc (date et heure).

— **Minage :** le hash généré commence par un nombre de zéro. Dans notre cas, le nombre de zéro égale à 2.

3.7 Quelques fenêtres de notre application

Nous assurons aussi la gestion des portefeuilles et l'accès à la blockchain en traitant des transactions. Dan cette section, nous présentons quelques fenêtres de notre application.

3.7.1 Enregistrement (Création d'une carte)

Pendant la création de la carte intelligente (smart carte), l'utilisateur fournit les donnés suivantes : :

— ID

— Mot de passe

— Nombre aléatoire

— Données biométriques

Ces informations de la carte sont sauvegardées au niveau de serveur des enregistrements.

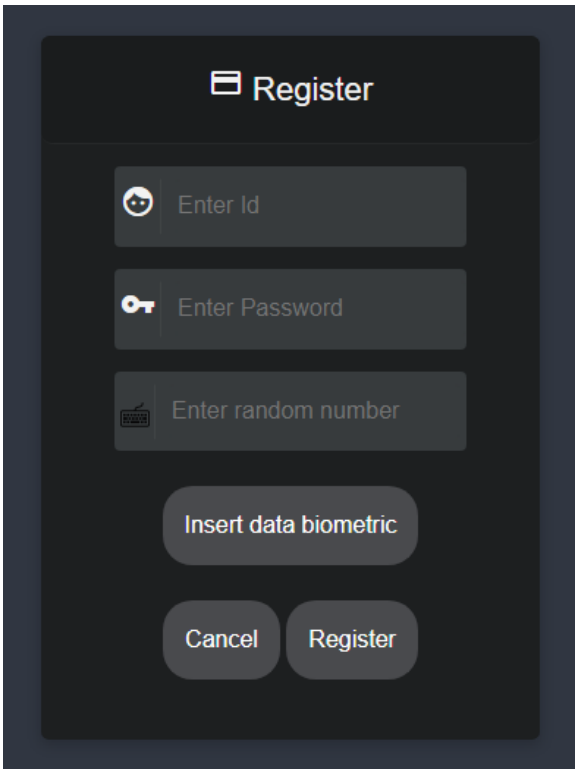

FIGURE 3.3 – Création d'une carte

3.7.2 Accès au compte (login)

Dans cette page, l'utilisateur doit s'authentifier pour accéder à sa propre portefeuille, elle contient les éléments suivants :

— Un champ pour sélectionner la carte d'utilisateur

— Un champ pour sélectionner l'empreinte d'utilisateur

— Login : bouton pour valider les informations remplis. Si les informations sont correctes, autre page sera affiche, sinon une message d'erreur sera affiché.

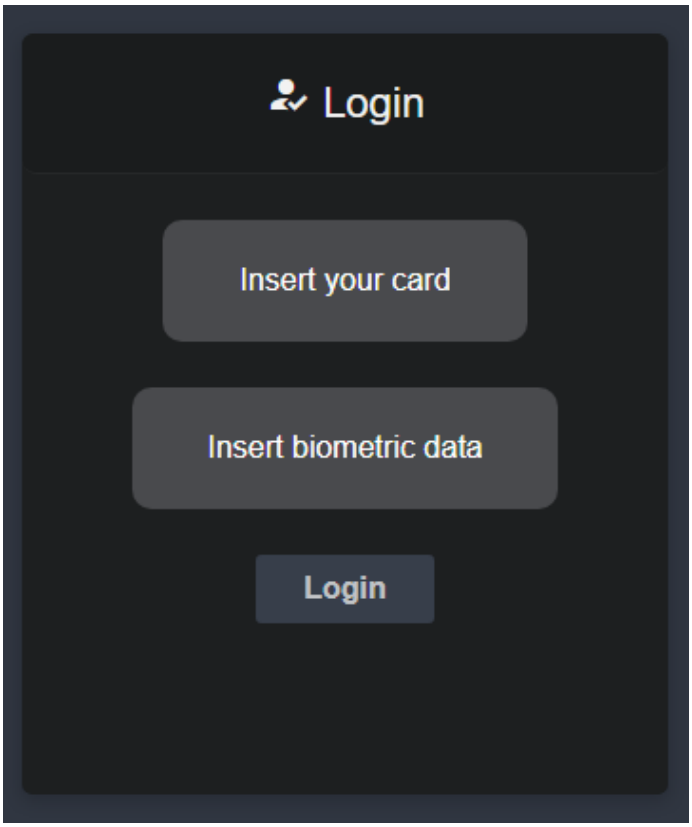

FIGURE 3.4 – Accès au compte

3.7.3 Génération des clés

— Sur cette page, nous devons créer un porte-monnaie déterministe (*deterministic wallet*) pour stocker les clés qui sont dérivés de la graine.

— A partir de chaque clé privée, on génère une clé publique et une adresse publique.

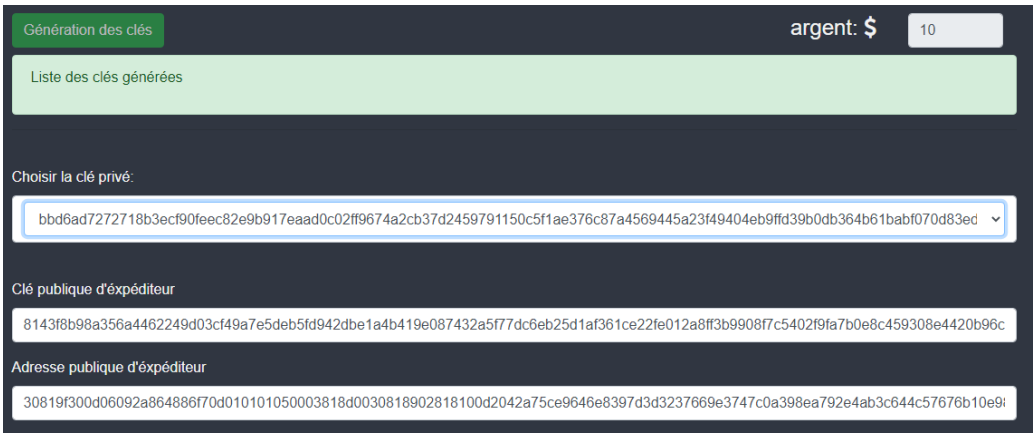

FIGURE 3.5 – Création d'un portemonnaie déterministe

3.7.4 Transaction

Pour générer une transaction et l'envoyer, il faut avoir :

— La clé publique du récepteur de monnaie.

— Le montant de l'argent à envoyer.

— Sans oublier de choisir une adresse publique parmi celles générées auparavant.

FIGURE 3.6 – Fenêtre transaction

3.7.5 Fenêtre Bloc

Nous avons testé notre solution localement sur une seule machine.
Sur le local host, nous avons utilisé 4 Noeud, en changeant à chaque fois le numéro de port. Par exemple :

— Adresse du 1èr nœud : http ://127.0.0.1 :5000/ port :5000

— Adresse du 2ème nœud : http ://127.0.0.1 :5002/ port :5002

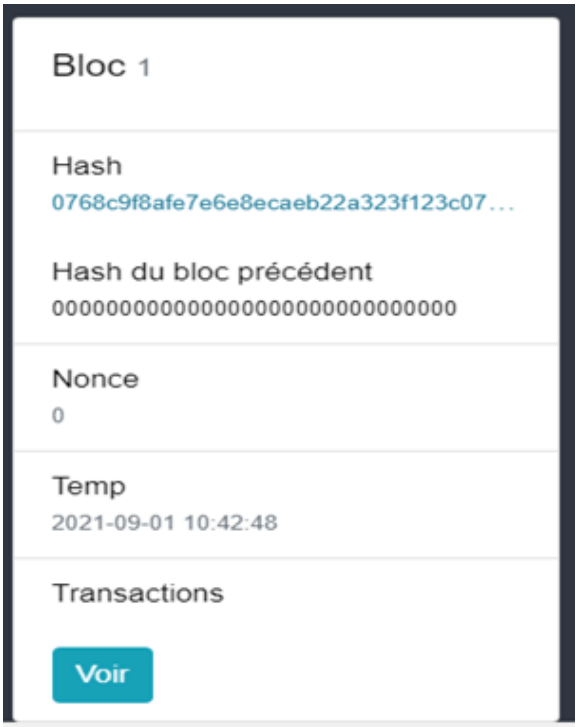

FIGURE 3.7 – Exemple d'un bloc.

3.7.6 Fenêtre Blockchain

— Liste des transactions : tableau de transactions et le Bouton Mine (seront affiché chez le mineur).

— Bouton Mise à Jour Blockchain : mise à jour de la liste des Bloc.

— Liste des Blocs : Chaque bloc affiche ses propres informations.

— Bouton Voir : affiche la liste de transaction dans ce Bloc.

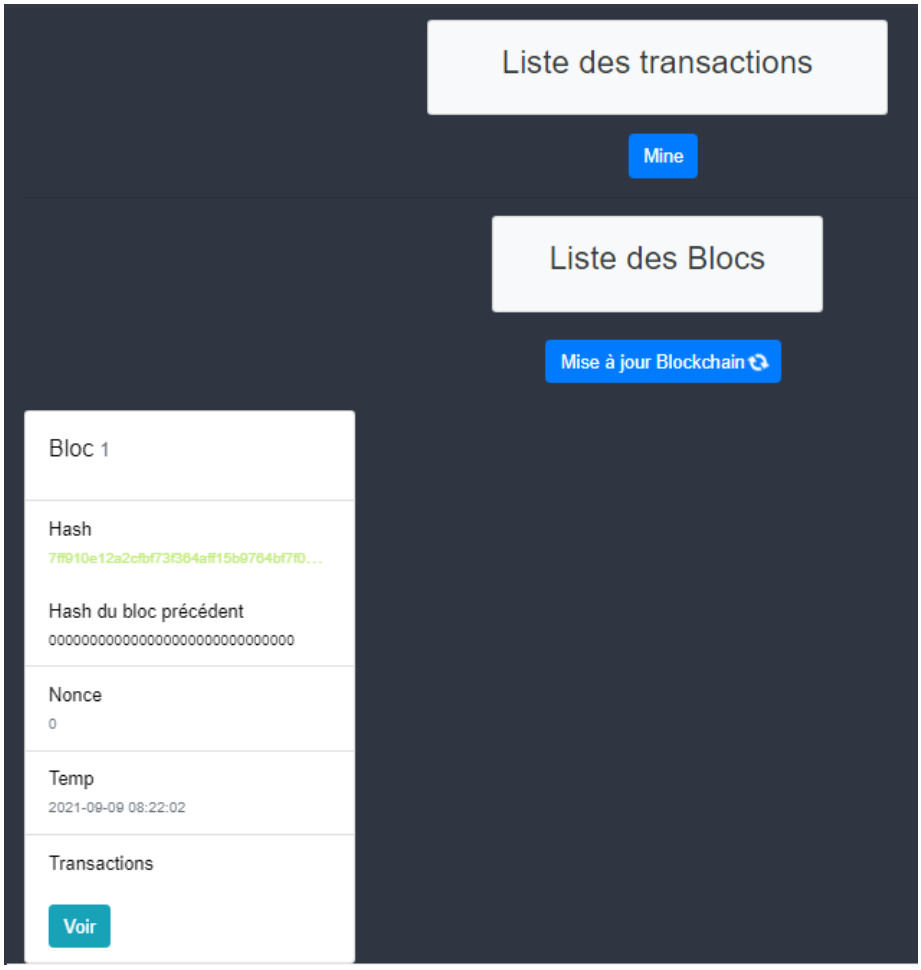

FIGURE 3.8 – Fenêtre Blockchain

3.7.7 Fenêtre Mining

Cette fenêtre affiche les blocs ajoutés à la blockchain et les transactions dans ces blocs.

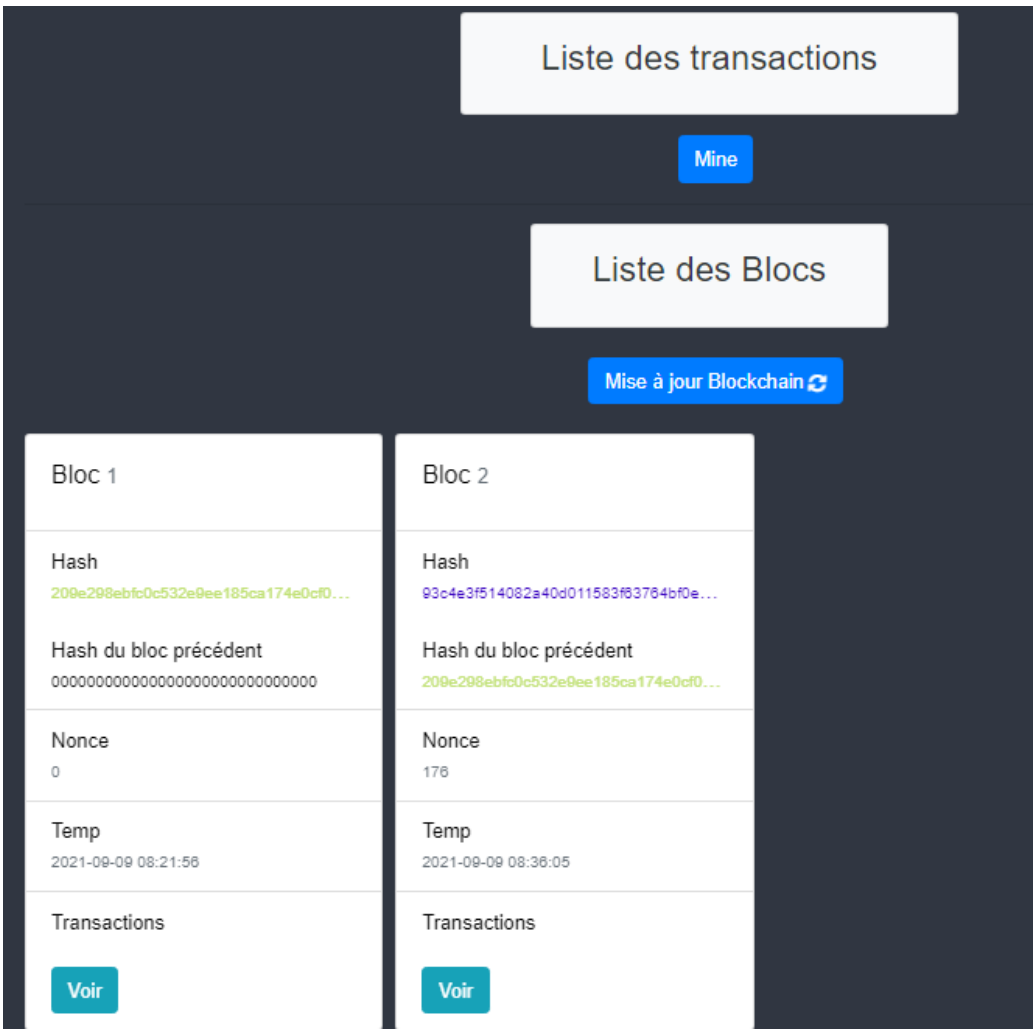

FIGURE 3.9 – Mining

3.8 Conclusion

Le portefeuille est le point d'accès d'une blockchain de crypto-monnaie, tel que bitcoin. Il permet de générer les clés privées, publiques et adresses publiques. Un portefeuille est généralement sécurisé par un mot de passe. Une telle sécurisation peut être cassée, et par conséquent, le propriétaire perde l'accès à son portefeuille. Ce chapitre expose notre proposition pour gérer un portefeuille en basant sur les données biométriques et des données supplémentaires. Nous avons ciblé deux problèmes : la sécurisation de portemonnaie et la génération des clés. Notre solution permet de réaliser un portefeuille sécurisé et déterministe. Cette proposition offre une possibilité de surmonter les problèmes de sécurité basée uniquement sur les données biométriques ou uniquement sur les mots de passe. D'autre part, notre proposition de génération des clés ajoute une valeur par rapport à celle basée uniquement sur les nombres aléatoires.

CONCLUSION GÉNÉRALE

Une blockchain qui peut fonctionner sur n'importe quel réseau peer-to-peer décentralisé et distribué, sans garanti de sécurité, permet d'effectuer des transactions en toute sécurité et sans interférence de tiers. Cette sécurisation est assurée par plusieurs techniques cryptographiques telles que la cryptographie asymétrique, la signature numérique et le hachage. Ces techniques sont aussi utilisées pour gérer et sécuriser les portefeuilles, qui sont des conteneurs des clés, et qui sont considérés comme des points d'entrée d'une blockchain crypto-monnaie.

Dans ce mémoire, nous avons étudié l'applicabilité des primitives cryptographiques dans la technologie blockchain. Nous avons visé le contexte de la sécurité et l'anonymat, plus précisément la sécurisation des utilisateurs de blockchain dans les deux niveaux :

— l'accès aux portefeuilles.

— la génération des clés privées, publiques et adresses publiques.

Dans notre proposition, l'accès à notre portefeuille est assuré après une vérification d'identité à base des données biométriques et d'autres données supplémentaires. Notre proposition permet aussi d'avoir un portefeuille déterministe, dont la génération des clés est commencée à partir d'une graine, et suive un processus qui permet d'avoir toutes les clés à partir de cette graine.

Notre application *Blockchain crypto-monnaie*, dont le backend est une page web, dédiée à être utilisé par les utilisateurs pour créer, gérer les portefeuilles, et générer les clés y associés. L'application permet aussi d'envoyer des transactions sécurisées sur une blockchaine crypto-monnaie, tout en assurant plus d'anonymat aux utilisateurs grâce à l'utilisation d'ensembles des clés (privées et publiques) et adresses (publiques).

Au cours de la réalisation de ce projet, nous avons découvert la technologie blockchain et son fonctionnement et conception plus près. Nous avons traité cette nouvelle technologie, ce qui nous a rendus plus expérimentés et mieux informés dans le domaine. Cependant, nous pensons n'avoir fait qu'un pas dans ce vaste domaine parce que, nous avons répondu sur une seule question et en avons eu beaucoup d'autres.

Nous proposons comme des travaux futurs et perspectifs les points suivants :

— Proposition d'utilisation d'autres générateurs de clés, qui combinent d'autres types des données.

— Adaptation de cette solution pour accès au portefeuille à partir d'une application mobile.

— Étendre la solution à autres domaine d'application de blockchain.

BIBLIOGRAPHIE

[1] M. PIGNEL and D. STOKKINK, "La technologie blockchain une opportunité pour l'économie sociale ?," 2018.

[2] A. M. Antonopoulos, *Mastering Bitcoin : unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[3] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," *arXiv preprint arXiv :1802.04351*, 2018.

[4] O. Desplebin, G. Lux, and N. Petit, "Comprendre la blockchain : quels impacts pour la comptabilité et ses métiers ?," *ACCRA*, no. 2, pp. 5–23, 2019.

[5] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld, "Digging into browser-based crypto mining," in *Proceedings of the Internet Measurement Conference 2018*, pp. 70–76, 2018.

[6] L. Lopes, "L'iran légalise officiellement le minage de cryptomonnaies," 2019 . https://theblockchainland.com/fr/2019/07/29/liran-legalise-officiellement-le-minage-de-cryptomonnaies/. Page consultée le 1 juillet 2021.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology : Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, IEEE, 2017.

[8] I. Bashir, *Mastering blockchain*. Packt Publishing Ltd, 2017.

[9] G. C. https://cryptoast.fr/bitcoin/, "Tout savoir sur les nœuds bitcoin," 2019. Page consultée le 6 juillet 2021, mis à jour le 12 septembre 2020.

[10] "Que fait la banque de france ?." La Banque de France. https://abc-economie.banque-france.fr/. Page consultée le 6 juillet 2021, 2011.

[11] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms : A survey," *arXiv preprint arXiv :2001.07091*, 2020.

[12] J.-G. Dumas and P. Lafourcade, "Les crypto-monnaies, une réalité virtuelle," 2020.

[13] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain : A Beginner's guide to building Blockchain solutions*. Springer, 2018.

[14] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[15] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies : Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[16] J. Bergquist, "Blockchain technology and smart contracts : Privacy-preserving tools," 2017.

[17] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT express*, vol. 6, no. 2, pp. 93–97, 2020.

[18] S. Seibold and G. Samman, "Consensus : Immutable agreement for the internet of value," *KPMG< https ://assets. kpmg. com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism. pdf*, 2016. Page consultée le 17 juillet 2021.

[19] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade : A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[20] T. Laurence, *Introduction to blockchain technology*. Van Haren, 2019.

[21] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, *et al.*, "Blockchain technology : Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[22] S. A. Bennanni, *Implémentation d'un smart contract sous la plateforme ethereum : vote électronique*. PhD thesis, Université du Sad Dahlab de Blida 1, 2019.

[23] P. M. Nik Roby Dylan Yaga and K. S. https://bitcoin.org/bitcoin.pdf, "Blockchain technology overview," 2018. Page consultée le 18 may 2021.

[24] S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.

[25] B. France, "La blockchain décryptée," *Les clefs d'une révolution. Paris, Netexplo*, 2016.

[26] O. Ayadi, *Analyse et étude de la sécurité des données médicales dans l'Internet des objets à partir d'une approche technologique Blockchain*. PhD thesis, Université de Constantine 2, 2019.

[27] B. E. K. GHOGGALI, "Systeme des credits bancaire base sur la technologie blockchain,"

[28] G. E. H. Mammeri Ilham, *Cryptographie homomorphe pour les réseaux « Vehicular Cloud Computing »*. PhD thesis, Université Abou bakr Belkaïd – Tlemcen – Faculté de TE, 2017.

[29] T. Ebrahimi, F. Leprévost, and B. Warusfel, "Cryptographie et sécurité des systèmes et réseaux," 2006.

[30] F. Burnel, "Les clés asymétriques. https://www.it-connect.fr/les-cles-asymetriques/," 2012. (Page consultée le218 may 2021.

[31] D. Grellety, "La signature électronique avec .nethttps://stormimon.developpez.com/dotnet/signature-electronique/," 2009. Page consultée le 01 juin 2021.,Mis à jour le 29 mars 2020.

[32] Guilieb, "Illustration de signature et vérification d'un message," 2015.

[33] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies," *Curso elaborado pela*, 2019.

[34] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*, pp. 369–378, Springer, 1987.

[35] Victor, "Introduction to cryptography in blockchain technology. https://crushcrypto.com/cryptography-in-blockchain/," 2018. Page consultée le 03 juin 2021.

[36] K. Raj, *Foundations of blockchain : the pathway to cryptocurrencies and decentralized blockchain applications*. Packt Publishing Ltd, 2019.

[37] M. Musumeci, "How digital signature works.https://www.massmux.com/how-digital-signature-works/," 2020. Page consultée le 06 juin 2021.

[38] M. Raikwar, D. Gligoroski, and K. Kralevska, "Sok of used cryptography in blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.

[39] S. Brunet, *Conception de mécanismes d'accréditations anonymes et d'anonymisation de données*. PhD thesis, Rennes 1, 2017.

[40] G. Greenspan, "Multichain private blockchain-white paper," *URl :http ://www.multichain.com/download/MultiChain-White-Paper.pdf*, pp. 57–60, 2015. (accede : 04.08. 2021).

[41] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 435–464, Springer, 2018.

[42] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts : Anonymous on-blockchain and off-blockchain bitcoin transactions," in *International conference on financial cryptography and data security*, pp. 43–60, Springer, 2016.

[43] S. Meiklejohn and R. Mercer, "Möbius : Trustless tumbling for transaction privacy," 2018.

[44] O. Shlomovits and I. A. Seres, "Sharelock : Mixing for cryptocurrencies from multiparty ecdsa.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 563, 2019.

[45] M. C. VILLANI and M. G. LONGUET, "Les enjeux technologiques des blockchains (chaînes de blocs)," tech. rep., 2018.

[46] T. Tore, "How to generate a bitcoin address — technical address generation explanation and online coursehttps://medium.com/@tunatore/," 2020. Page consultée le 01 juillet 2021.

[47] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *Journal of Network and Computer Applications*, vol. 127, pp. 43–58, 2019.

[48] P. Franco, *Understanding Bitcoin : Cryptography, engineering and economics*. John Wiley & Sons, 2014.

[49] V. Odelu, "Imbua : identity management on blockchain for biometrics-based user authentication," in *International Congress on Blockchain and Applications*, pp. 1–10, Springer, 2019.

[50] N. Li, F. Guo, Y. Mu, W. Susilo, and S. Nepal, "Fuzzy extractors for biometric identification," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 667–677, IEEE, 2017.