Généralité sur la cryptographie

1.1 Introduction

Une blockchain est une technologie de stockage et de transmission d'informations sans organe de contrôle

Elle s'appuie en grande partie sur la cryptographie pour assurer la sécurité de la transmission et la confidentialité de l'information numérique au sein du réseau. Dans ce chapitre nous présentons les notions de base de la cryptographie utilisées dans la blockchain.Tels que le cryptage asymétrie,signature numérique,fonction de hachage,ect.

1.2 Concepts de base

1.2.1 Définition de cryptographie

La cryptographie est l'art de chiffrer et coder les messages. Elle est devenue aujourd'hui une science à part entière. Au croisement des mathématiques et de l'informatique, elle permet ce dont les civilisations ont besoin, depuis qu'elles existent, pour sécuriser les données[2].

1.2.2 L'usage de cryptographie

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 :

- La confidentialité : consiste à rendre l'information intelligible à d'autres personnes que les acteurs d'une transmission [1].
- 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[1].

1.2.3 Types de cryptographie

On peut distinguer deux types de cryptographies : la cryptographie symétrique et la cryptographie asymétrique.

1.2.3.1 Cryptographie symétrique

Le chiffrement symétrique, que l'on nomme couramment chiffrement conventionnel, basé sur des fonctions mathématiques réversible. Le chiffrement symétrique repose sur un principe de clé unique pour chiffrer et déchiffrer. Cette clé possède plusieurs appellations telles que clé secrète, clé partagée.

On parle de chiffrement conventionnel puisque c'est le premier chiffrement par clé à avoir été découvert et utilisé[1].

Le chiffrement symétrique se déroule (voir la figure.1.1) sur les étapes suivantes [2], sachant que Alice est un utilisateur et bob est un destinataire :

- Génération de la clé secrète par Alice.
- Envoi de cette clé secrète à Bob, de manière sécurisée.
- Chiffrement du message par Alice, avec la clé secrète.
- Envoi de ce message chiffré à Bob.
- Réception du message chiffré par Bob.
- Déchiffrement du message avec la clé secrète reçue auparavant. [2]

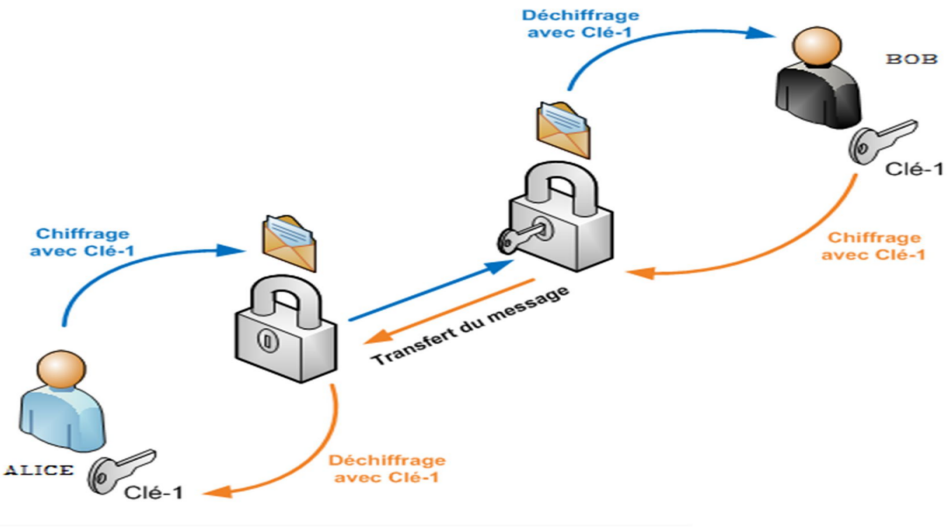

FIGURE 1.1 – Chiffrement Symétrique.
[23]

1.2.3.2 Cryptographie asymétrique

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman [2].

Dans un chiffrement asymétrique (ou cryptographie à clés publiques), les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). A partir de cette clé, ils déduisent la clé publique à l'aide d'un algorithme. Donc les clés existent par paires (le terme de bi-clés est généralement employé). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé [2]. (Voir figure 1.2).

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 détient, 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 !

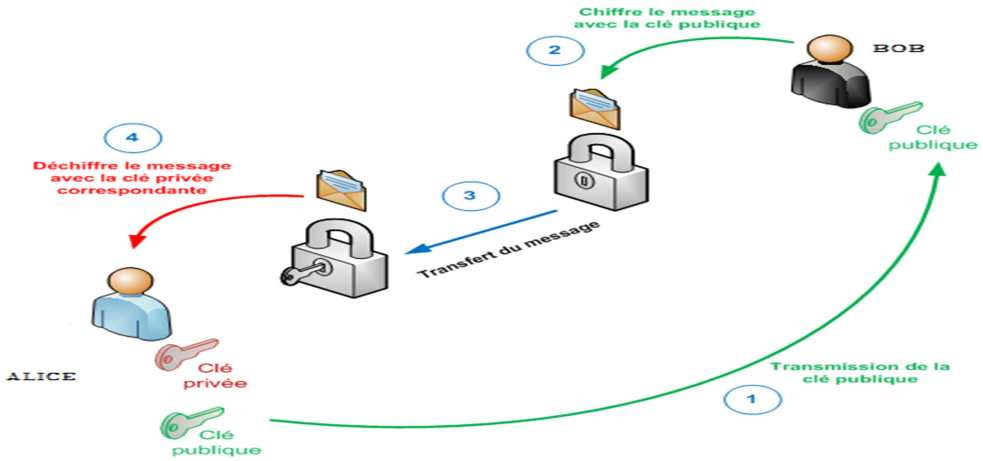

FIGURE 1.2 – Chiffrement Asymétrique [23].

1.2.4 Fonction de hachage

1.2.4.1 Définition

Une fonction de hachage (dite aussi une fonction de contraction, digest, empreinte digital, "hash code") est une fonction à sens unique et sans collision, générant une sortie de taille fixe (appelée condensat ou empreinte)[3], caractéristique des données fournies en entrée (voir figure 1.3).

Une fonction de hachage est dite « à sens unique » car :

- Il est impossible de retrouver les données initiales à partir de l'empreinte.
- Elle est conçue de telle sorte que le hash produit une image ou empreinte de taille fixe créée à partir d'une donnée de taille variable, fournie en entrée soit impossible à inverser. Alors qu'il est simple de produire un hash.
- À partir d'un ensemble de données, il est impossible de remonter à un ensemble de données à partir d'un hash connu, au moins avec les puissances de calcul disponibles aujourd'hui.

Une fonction est dite « sans collision » ou « injective »

- lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat[3].

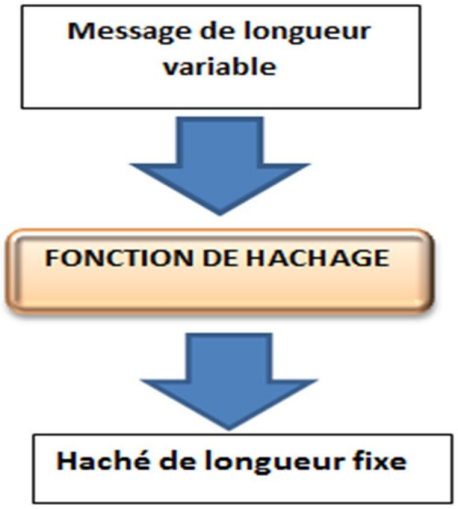

FIGURE 1.3 – Principe de Hachage.

1.2.4.2 Propriété de base d'une fonction de hachage

Une fonction de hachage cryptographique idéale possède les quatre propriétés suivantes :

- La valeur de hachage d'un message se calcule "très rapidement" [4] .
- Il est par définition, impossible, pour une valeur de hachage donnée, de construire un message ayant cette valeur de hachage [3].
- Il est impossible de modifier un message sans changer sa valeur de hachage [4].
- Il est impossible de trouver deux messages différents ayant la même valeur de hachage [4].

L'intégrité des données peuvent être prouvées si les fonctions de hachage remplissent un ensemble d'exigences. Une fonction de hachage est dite avoir des bonnes propriétés cryptographiques si elle est résistante aux préimages, aux secondes préimages et aux collisions.

Les trois problèmes suivants doivent donc être difficiles à résoudre [5] :

- Préimage : étant donné un hache h choisi aléatoirement, trouver un message m tel que : H(m) = h.
- Seconde préimage : étant donné un message m choisi aléatoirement, trouver un message m' tel que H(m) = H(m').
- Collision : trouver deux messages m , m', tels que m déférent que m' et H(m) = H(m'). Selon sa définition, une fonction de hachage est une fonction dont l'ensemble de départ est plus grand que l'ensemble d'arrivée.

1.2.4.3 Exemples des fonctions de hachage

1.2.4.3.1 MD5 MD5 (Message-Digest algorithm 5) : est une fonction de hachage inventée par Ronald Rivest en 1991. Cette fonction de hachage permet de calculer une empreinte de toute donnée numérique (allant d'une simple chaîne de caractères à un fichier de plusieurs giga octets). L'empreinte générée est d'une longueur de 128 octets (soit 32 caractères)[2].

- La fonction de hachage MD5 a été initialement conçue pour être utilisée comme algorithme de hachage cryptographique sécurisé pour authentifier les signatures numériques.
- MD5 comprend 64 blocs de ce type, groupés en quatre tours de 16 opérations similaires basées sur des fonctions non-linéaire(une addition et une rotation vers la gauche)qui varie selon le tour

1.2.4.3.2 SHA256 SHA-256 (Secured Hash Algorithm 256) :est une fonction de hachage qui a été développé par la NSA (United States National Security Agency) en 2001 et continue à être utilisé par de nombreuses institutions financières et de gouvernements pour le cryptage de leurs données grâce à sa complexité. Elle se trouve parmi les plus répandues [2].

- SHA-256 accepte en entrée un message de longueur maximum 264 bits et produit un hash, ou condensé, de 256 bits.
- SHA-256 a ces portes logiques et d'autres opérations vont être appliquées à l'ensemble de données de départ, qui aura été découpé en morceaux de 256 bits. Elles se succèdent suivant une organisation complexe répétée une soixantaine de fois.
- La fonction de compression utilisé par le SHA-256 est basée sur des registres à décalage et des opérations bits à bits. Ces registres nommés de A à H contiennent chacun un mot de 32 bits.
- Sa sécurité est bien plus importante que le Md5, car il propose un bon équilibre entre espace de stockage en ligne et sécurité.

1.2.5 Signature numérique

1.2.5.1 Définition

Comme la signature manuscrite, la signature numérique est un terme générique qui indique tout simplement un mécanisme permettant de lier un document à un signataire. Dans les deux cas, les signatures peuvent être vérifiées publiquement. Donc elle permet de garantir l'intégrité d'un document électronique une fois signé et d'en authentifier le signataire [24].

Les schémas de signature électronique sont donc fondamentalement asymétriques : la clé privée du signataire intervient dans l'algorithme de signature, et la clé publique correspondant sert à la vérification.

1.2.5.2 Principe de signature

1. A l'utilisation d'une signature, une empreinte numérique unique se crée (appelée un hache) grâce à un algorithme mathématique. Ce hache est spécifique à ce document, ce qui signifie que la moindre modification créera un hache différent(voir la figure 1.4).

2. Le hache est chiffré avec la clé privée du signataire. Le hache chiffré et la clé publique du signataire sont ensuite réunis dans une signature numérique qui est annexée au document.

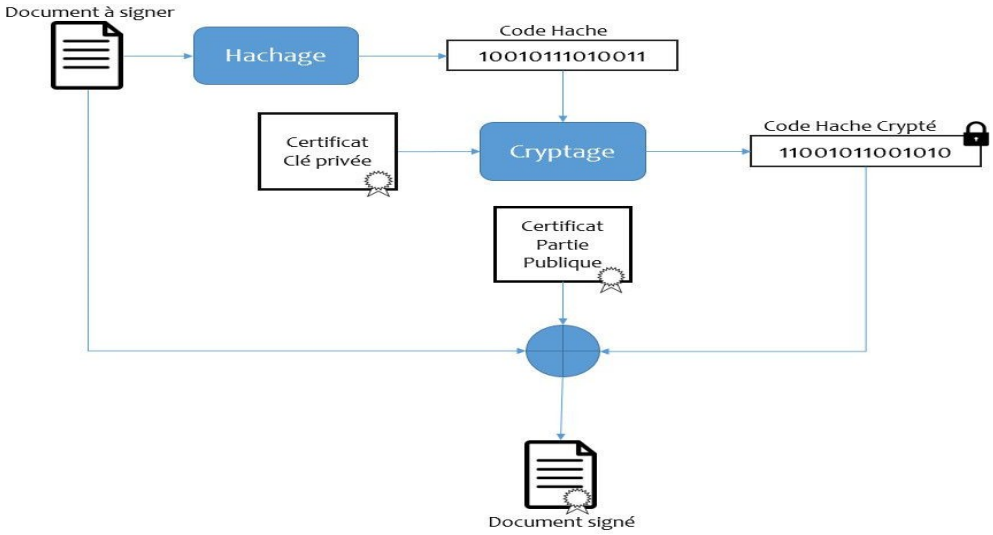

FIGURE 1.4 – Signature numérique.
[25]

Les signatures numériques sont souvent utilisées dans trois objectifs que leurs propriétés permettent d'atteindre : l'intégrité des données, l'authentification et la non-répudiation.

- L'intégrité des données : Bob peut vérifier que le message d'Alice n'a pas été modifié entre l'envoi et la réception. Toute modification du message produirait une signature complètement différente.

- L'authenticité : Tant que la clé privée d'Alice est gardée secrète, Bob peut se servir de sa clé publique pour confirmer que les signatures numériques ont été créées par Alice et personne d'autre.

- Non-répudiation : Une fois la signature générée, Alice ne pourra pas nier l'avoir appliqué à l'avenir, à moins que sa clé privée ne soit compromise d'une quelconque manière.

1.2.6 Arbre de Merkle

Un arbre de Merkle est un arbre de hachage binaire [6]. Il est construit en hachant les données (les transactions au niveau feuille), puis en hachant à nouveau les sorties hachées

jusqu'au noeud racine, appelé racine Merkle (Merkle root). De cette façon, l'intégrité d'une quantité arbitraire de données peut être efficacement assurée.

L'arbre de Merkle est construit de bas en haut. Un arbre Merkle typique peut être représenté comme le diagramme dans la(Figure 1.5). Dans cet exemple l'arbre de Merkle contient quatre feuilles.

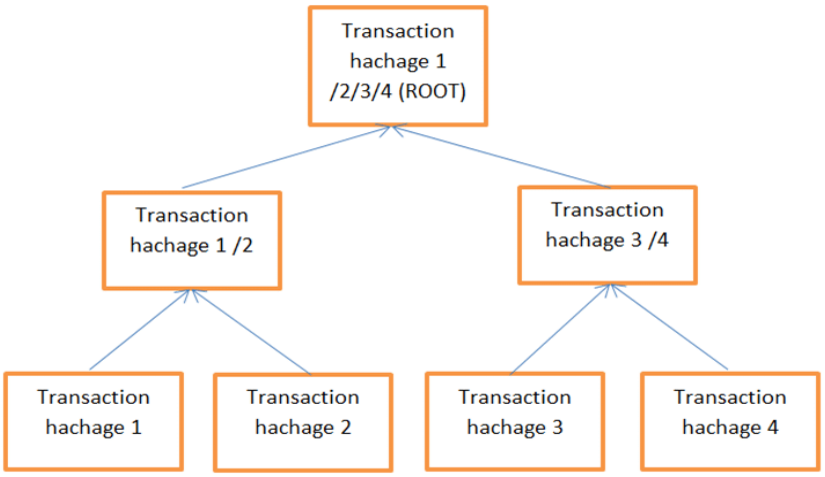

FIGURE 1.5 – Arbre de Merkle.

1.3 Conclusion

Le but traditionnel de la cryptographie est d'élaborer des méthodes permettant d'échanger des données de manière sécurisée. C'est pour ça la cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications.

Dans ce chapitre nous avons présenté une introduction à la cryptographie qui permet de s'assurer à la fois certain nombre de sécurité de base : confidentialité, intégrité et authentification des données transmises, ainsi que l'authentification des tiers et la non répudiation.

Ces techniques cryptographiques ainsi que d'autres théquenologies forment les éléments constitutifs de la technologie blockchain qui seront introduits au chapitre 2 .

Chapitre 2

Blockchain

2.1 Introduction

La protection des données sur internet a toujours été un sujet qui a affolé la toile : il ne se passe pas une journée sans que les médias nous parlent de piratage des coordonnées bancaires ou de géant du e-commerce qui se font hacker. C'est pourquoi les chercheurs se concentrent aujourd'hui sur les technologies de cryptage et de sécurisation des données comme la Blockchain.

Une Blockchain fonctionne sur un réseau pair-à-pair d'ordinateurs qui exécutent tous le protocole et détiennent une copie identique des blocs de transactions, qui sont transmises sans intermédiaire et sans aucune autorité central grâce à un mécanisme appelé consensus. Blockchain est lui -même un registre public et partagé qui enregistre toutes les transactions du bloc de genèse (premier bloc) jusqu'à aujourd'hui.

Dans ce chapitre, nous présentons la nouvelle technologie « Blockchain », qui promet d'assurer cette confiance numérique sans organe central. Nous montrons comment elle peut être utilisée pour partager et contrôler en toute sécurité les informations entre les parties qui ne se font pas nécessairement confiance.

Le présent chapitre couvre : l'histoire de la Blockchain ,sa définition ,ses caractéristiques,son fonctionnement,ses composants et le rôle de l'algorithme de consensus .

2.2 Histoire de Blockchain

La Blockchain a été connue en 2008 avec la monnaie virtuelle bitcoin. Les deux sont donc historiquement liées : la Blockchain est l'infrastructure virtuelle sur laquelle repose le bitcoin [16].

Le terme Bitcoin (B majuscule) renvoie à la fois :

- A une monnaie numérique (le bitcoin avec b minuscule) utilisant des techniques cryptographiques [16].
- Au protocole décrivant le fonctionnement du réseau sur lequel cette monnaie circule.

Ce protocole, c'est la Blockchain, où la création monétaire et la validation des transactions s'effectuent de manière horizontale et transparente. Ce système fonctionne sans autorité centrale ni tiers de confiance, à l'inverse des monnaies contrôlées par des banques ou des gouvernements. L'inventeur de Bitcoin reste à ce jour inconnu, même si certains ont tenté de revendiquer sa paternité, sans réussir toutefois à présenter les preuves nécessaires. On ne connaît que son pseudonyme, Satoshi Nakamoto, sous lequel il a mis en ligne fin 2008 le livre blanc à l'origine de ce qu'il définissait comme un "système de monnaie électronique pair-à-pair" [16].

Il propose un système basé sur des preuves cryptographiques, censées remplacer la confiance accordée aux institutions financières. Ce système a pour objectif de répondre à plusieurs enjeux [7] :

- Une transaction entre deux parties sans tiers de confiance.
- Des vendeurs protégés contre d'éventuelles fraudes grâce à une impossibilité de supprimer ou modifier une transaction.
- Des acheteurs protégés avec un système de comptes captif (indisponibilité d'un bien pendant une courte période)
- Pas de double dépense possible grâce à l'horodatage des transactions.

Ce système est cependant possible uniquement si la puissance de calcul des noeuds honnêtes du réseau est plus importante que celle des noeuds agissant pour réaliser une attaque combinée sur le réseau [7]. Ce concept sera explicité ultérieurement

2.3 Définition

- « Une Blockchain, ou chaîne des blocs, est une technologie de stockage et de transmission d'informations sans organe de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne » [15].
- « Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les noeuds de stockage. Une Blockchain est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti » [16].

  Grâce aux définitions ci-dessus, nous pouvons définir la Blockchain comme une distribution d'un grand livre décentralisé et public composé de nombreux pairs (noeuds), chaque pair a les mêmes enregistrements de données exactes dans son propre appareil, ces enregistrements sont enregistrés dans des blocs là où se trouve un ensemble de transaction sous forme d'une chaîne. (voir la figure 2.1) [8].

FIGURE 2.1 – Structure d'une Blockchain .

2.4 Caractéristiques de Blockchain

La technologie Blockchain repose sur les principales caractéristiques suivantes [26]

- La décentralisation : un réseau pair à pair où chaque noeud du réseau remplit une ou plusieurs fonctions ;
- La transparence : l'historique des transactions est consultable en permanence par n'importe qui via une connexion internet et un explorateur de Blockchain, le code source d'une Blockchain publique est ouvert et consultable par tous ;
- La fiabilité : la Blockchain repose sur des mécanismes de cryptographie éprouvés et extrêmement robustes, tels que la gestion de binômes clés publiques/clés privées et des fonctions de hachage. De plus, les transactions sont toutes validées par des algorithmes (que l'on appelle consensus) avant d'être partagées au sein de blocs de données ;
- L'immuabilité : une fois insérée dans la Blockchain, une transaction est infalsifiable, y compris par des acteurs malveillants qui participeraient au réseau ;

2.5 Fonctionnement d'une Blockchain

La particularité de la Blockchain est qu'elle fonctionne sans organe central de contrôle. Au lieu d'être regroupées à un seul endroit ou de passer par un seul intermédiaire, les transactions (achat ou transfert d'argent par exemple, dans le cas de blockchaine de crypto-monnaie) sont distribuées entre tous les membres d'un réseau via leur ordinateur.

2.5.1 Fonctionnement

Pour une première approche du fonctionnement des blockchain, le plus facile est de raisonner avec une blockchain purement monétaire. On peut prendre l'exemple de Bitcoin, ou d'une blockchain avec des jetons "simples", en commençant par la création d'une transaction peut être décrit en quelques étapes (voir la figure 2.2) :

1. Un compte (ou portefeuille, portemonnaie, wallet) doit être créé 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.

2. A la réception de la transaction, chaque mineur authentifie la transaction à l'aide de la clé publique de **A**. Cette transaction avec d'autres transactions récentes sont regroupées en bloc, et chaque transaction sera vérifiée et validée par les mineurs. Lors de la vérification de la transaction, l'historique des transactions de **A** est remonté pour vérifier que l'argent qu'il a reçu précédemment n'a pas été réutilisé depuis. On vérifie en fait tout simplement qu'il n'essaye pas de dépenser deux fois l'argent qu'il a reçu.

3. Une fois les vérifications effectuées, le bloc dans lequel se trouve la transaction entre **A** et **B** est validé par les mineurs, selon des techniques de consensus qui dépendent du type de blockchain, et qui permettent d'atteindre le consensus distribué, c'est-à-dire le consensus des noeuds sur l'état du réseau [10]. Pour cela, les mineurs doivent lancer un procédé cryptographique : le calcul du hache du bloc. Dont chaque bloc possède un identifiant qui prend la forme d'un hache permettant de relier les blocs les uns aux autres. Cet hache est toujours le résultat du hachage du bloc précédent.

4. Quand le bloc est validé, il est daté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs ont accès.

5. Enfin, "B" reçoit la transaction de **A**.

FIGURE 2.2 – Principe Général d'une Blockchain [26].

2.5.2 Rôle de hache

Dans le cas d'une chaîne de bloc, le hachage est effectué à partir du contenu du bloc : le hache du bloc précédent, un certain nombre de transactions et un horodatage (voir la figure 2.3).

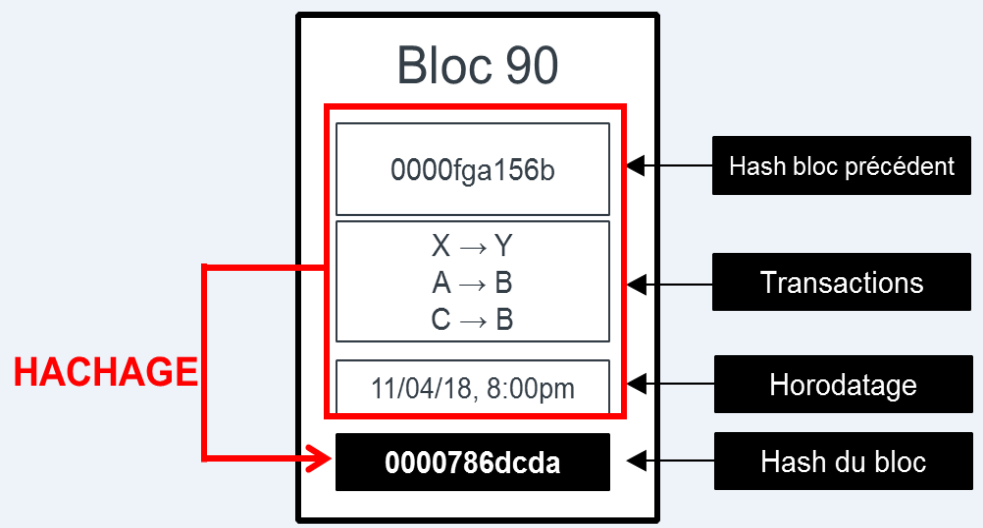

FIGURE 2.3 – Rôle des hashs dans les blocs[26].

La modification étant visible dans l'ensemble des blocs suivants car les blocs sont tous liés entre eux cryptographiquement. En conséquence, modifier le contenu d'un bloc suppose de recalculer les hachs de tous les blocs qui le suivent (voir figure 2.4).

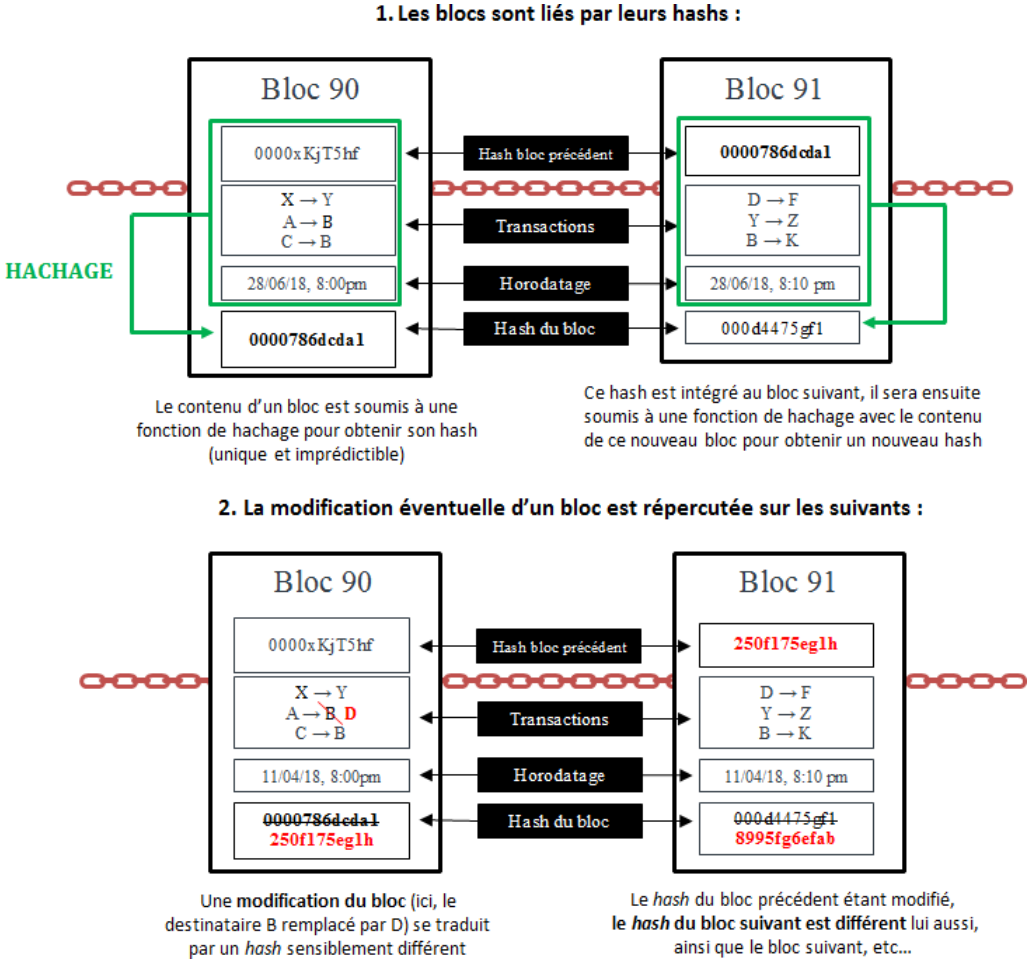

FIGURE 2.4 – Rôle du hachage dans l'intégrité de la chaîne de blocs [26].

2.6 Composants de Blockchain

La technologie de blockchain se base sur plusieurs concepts tels que transaction, bloc, consensus,.. Dans cette section, nous présentons ces différents composants.

2.6.1 Compte ou porte-monnaie (wallet)

Le porte-monnaie est un logiciel pour la sauvegarde de la clé privé et clé publique d'un utilisateur de blockchain, ce logiciel peut être une application sur le web, téléphone mobile ou ordinateur. Il permet à cet utilisateur de contrôler son compte de crypto-monnaie, voir son montant et exécuter des transactions[**?**].

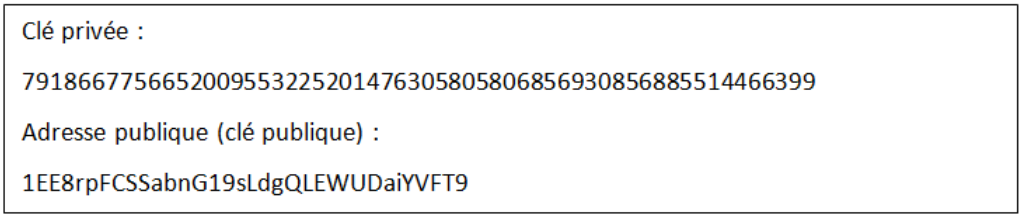

FIGURE 2.5 – Exemple de couple clé privée et clé publique [**?**].

2.6.2 Transaction

Pour une première approche du fonctionnement des blockchains, le plus facile est de raisonner avec un blockchain purement monétaire.

- Pour une simple définition, une transaction se résume à trois informations : qui donne quoi à qui.[7]
- Le concept des transactions repose en réalité sur la cryptographie asymétrique. Lorsque quelqu'un se lance dans le processus de création d'une transaction, il génère, à l'aide de son porte-monnaie, une clé publique et une clé privée. La clé privée n'est transmise à personne et la clé publique est, quant à elle, disponible pour tout le monde. Les deux clés (privée et publique) permettent de garantir l'intégrité des données transmises en chiffrant les données envoyées, ainsi que l'authentification de l'origine de la transaction
- Les transactions sont composées d'une liste d'entrées de transactions et d'une liste de sorties de transaction.

Chaque sortie de transaction contient deux données :

- Donnée : La donnée qu'il vas envoyer.
- Adresse du destinataire : ce dernier est dérivé de la clé publique du destinataire.

Les entrées de transaction contiennent :

- Référence à une sortie de transaction précédente.
- Signature qui prouve l'authenticité de transaction [11].

2.6.3 Bloc

Un bloc est un enregistrement dans la blockchain, qui contient et confirme plusieurs données ou transactions en attente. Toutes les 10 minutes en moyenne (dans le cas de Bitcoin), un nouveau bloc contenant des transactions est ajouté à la chaine de blocs par le minage [13].

Chaque bloc est constitué de plusieurs champs :

- Bloc : l'indice de bloc.
- Hash du bloc précedent : champ contient l'empreinte de bloc précedant (bloc d'indice numero 91 dans notre exemple).
- Transaction : la partie qui contient la liste des transactions.
- Horodatage : temps de la création de bloc.
- Hash : l'identifiant du bloc actuel .

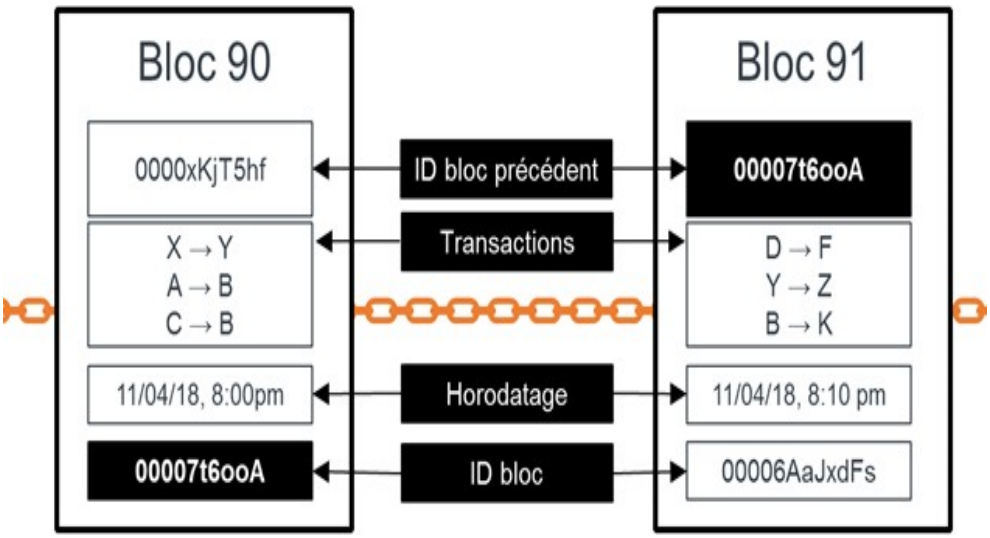

FIGURE 2.6 – Structure des blocs de la chaine[26].

2.6.4 Minage

Le minage est un processus très importent dans une blockchaine. [14]

- Mineur : est le noeud qui s'occupe de miner (effectuer le processus de minage) en fournissant de la puissance de calcul pour valider les transactions.

- Minage (mining) : C'est le processus qui permet la validation des blocks des transactions. Cette opération, très coûteuse en puissance de calcul informatique, est motivée par l'obtention d'une récompense par le mineur gagnant.

2.6.5 Algorithme de consensus

L'algorithme de consensus joue un rôle important dans le contexte de la Blockchain. Le but est d'obtenir tous les participants s'accordent sur un seul état de la blockchain.

Puisqu'il n'y a pas de centralisation pour décider quels nouveaux blocs sont valides, chaque noeud doit décider s'il accepte un nouveau bloc reçu ou non. étant donné que tous les noeuds du réseau ont leur propre copie des données complètes de la chaîne de blocs et ils utilisent la signature numérique pour vérifier l'authenticité de toutes les transactions.[15]

Le mécanisme de consensus a les objectifs suivants :

- S'assurer d'avoir un bloc valide dans la chaîne de blocs.
- Parvenir à un accord équitable pour toutes les parties concernées
- Il faut s'assurer qu'il n'y aura pas d'adversaires puissants pour réussir à bifurquer la chaîne.
- Rendre le réseau plus solide face aux divers types d'attaques.

Les algorithmes de consensus sont constitués une partie très importante des plateformes blockchain. Sans eux, il ne nous restera qu'une base de données stupide et immuable. Nous listons ici quelques algorithmes de consensus les plus utiliser qu'on va évaluer et analyser dans le prochain chapitre.

- Preuve de travail (Proof of Work).
- Preuve d'enjeu (Proof of Stake).
- Preuve d'enjeu délégué (Delegated Proof of Stake).
- Preuve d'importance (Proof of Importance).
- Preuve du temps écoulé (Proof of Elapsed Time).

2.7 Conclusion

Dans ce chapitre, nous avons étudier le mécanisme et le concept sur lequel repose la blockchain, qui est une nouvelle technologie révolutionnaire qui a captivé l'attention des chercheurs et des innovateurs dans le monde de la technologie. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau distribué, assurant une sécurisation

des données par chiffrement, et faisant participer les noeuds du réseau pour la création de nouveaux blocs de la chaîne.

Le principe de base d'une blockchain repose sur la notion de consensus, qui sera le but de prochain chapitre, là où nous allons discuter de quelques algorithmes de consensus en détails.

Chapitre 3

Algorithmes de consencus

3.1 Introduction

Après avoir compris les principes de la blockchain et découvert son architecture, nous mettrons l'accent sur le consensus dans la blockchain : son utilité, son mode de fonctionnement ou encore les différentes formes de consensus qui peuvent exister.

L'enjeu n'est pas de rentrer à un niveau de détail technique mais bien d'évaluer et de vulgariser ce processus clé d'une blockchain. Alors, dans ce chapitre après avoir connaitre les critères de l'efficacité d'un bon algorithme de consensus blockchain. Nous présentons en détail quelques algorithmes de consensus les plus utiliser dans la blockchain et listons leurs différents avantages et inconvénient.

3.2 Critères de l'efficacité d'un mécanisme de consensus

Parvenir à un consensus au sein d'un réseau de noeuds distribues ne semble pas chose aisée. Les algorithmes de consensus doivent [16] :

- Être résilients aux pannes de noeuds, aux retards de transmission, aux messages égarés ou corrompus .
- Faire face aux noeuds malveillants tentant de manipuler le consensus ou de le retarder.

Pour ce faire, une pluralité de mécanismes existent (PoW, PoS, DPoS, PoET, PoI, etc). Chacun d'entre eux dispose de ses propres caractéristiques en matière de synchronisation, d'émission de message (fréquence, taille), de tolérance aux pannes, de prévention contre les noeuds malveillants, de performance et de sécurité des messages échangés.

Ainsi, Le système blockchain, parvenir à un consensus garantit que l'ensemble des noeuds du réseau s'accordent sur un même état du registre et des données qui y sont stockées. Pour déterminer plus précisément l'efficacité d'un mécanisme de consensus, on évalue ce dernier selon trois critères principaux [16] :

- Terminaison (Liveness) : Tous les noeuds opérationnels participant au consensus doivent finalement produire une valeur.
- Sûreté / Consistance (Safety) : Tous les noeuds opérationnels doivent s'accorder en temps réel sur l'une des valeurs proposées par l'un des noeuds. Cette valeur doit être valide selon les règles définies par le mécanisme.
- Tolérance aux fautes (Fault Tolerance) : Le mécanisme doit être capable de fonctionner même si un ou plusieurs noeuds sont défaillants.

Il est crucial de pouvoir satisfaire les trois propriétés listées ci-dessus si on souhaite résoudre, dans son intégralité, le problème du consensus. Malheureusement, Fischer, Lynch et Patterson, trois chercheurs en informatique, ont montré en 1985 qu'aucun algorithme déterministe de consensus ne permettait de garantir en même temps ces trois propriétés au sein d'un système asynchrone tel qu'un réseau de noeuds distribués (FLP Impossibility).

Ainsi, en règle générale, puisque la tolérance aux fautes est absolument vitale dans le cadre d'un réseau de noeuds distribués, les mécanismes de consensus doivent choisir entre la sûreté et la terminaison en fonction des exigences de l'application pour laquelle a été conçue la plateforme décentralisée [16].

En matière de tolérance aux fautes, les mécanismes de consensus traditionnels opérant dans un réseau de noeuds distribués et connus se sont d'abord évertués à faire face aux fautes "fail-stop" où un noeud ne répond plus à la suite d'un problème matériel ou logiciel[18].

La section suivante, présente un ensemble des algorithmes de consensus, les plus connus dans la littérature, en expliquant leur principe et en mettant l'accent sur leurs avantages et inconvénients.

3.3 Algorithmes de consensus

Parmi les algorithmes de consensus existent, on peut citer : preuve de travail, preuve d'enjeu , preuve d'enjeu délégué,ect.Dans cette section,nous détaillant le principe de chaque algorithme.

3.3.1 Preuve de travail (POW : proof of work)

Faisant sa première apparition en 1993, le concept de preuve de travail a été développé pour prévenir les attaques d'altération de service et autres abus de service tels que le spam, sur un réseau en imposant du travail à l'utilisateur du service, généralement en se servant de la puissance de calcul de son ordinateur. [20]

En 2009, Bitcoin a introduit une manière innovante d'utiliser la preuve de travail, comme algorithme de consensus. Dans ce cas, PoW est utilisé pour valider les transactions qui sont regroupées en blocs, qui sont liés entre eux pour former une blockchain. Depuis lors, PoW