République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme de master recherche en informatique

Option : Réseaux et Systèmes Distribués.

Thème

Anonymat et vie privée dans la blockchain

Réalisé par

BELHOUL Lydia

LALAOUI Feriel

Membres du jury :

Présidente : Mme. OUYAHIA Samira.

Examinatrice : Mlle. BOUCHLAGHEM Siham.

Encadrante : Mme. YAICI Malika.

Année universitaire : 2020 - 2021

Remerciements

Nos plus vifs remerciements vont à notre encadrante Mme. YAICI Malika pour sa compréhension, sa disponibilité, son aide et ses conseils qui nous ont été utiles pour l'achèvement de ce travail.

Nous tenons à exprimer notre gratitude aux membres du jury pour avoir accepté de juger ce travail.

Un profond merci à toute personne qui a contribué de près ou de loin à la réalisation de ce travail.

- Feriel & Lydia -

Dédicace

Je dédie ce travail à mes chers parents HEMMANOU et SAIDA pour leur amour, leur soutien et leur patience tout au long de mes études, qu'ils trouvent ici l'expression de ma gratitude et de mon profond amour.

A ma sœur NARIMEL, son mari AMINE et sa fille TANIRT, à mes frères NAZIM et FATAH ainsi que ses deux filles RANA et MIRNA.

A tous les membres de ma famille, à mes grands-mères HOURIA et FATMA. A tous mes oncles et tantes.

A mes amis proches, ou qu'ils soient.

- Feriel -

Dédicace

À mes chers parents ATMANE et DJAHIDA pour leur amour, leur soutien et leur patience tout au long de mes études, qu'ils trouvent ici l'expression de ma gratitude et de mon profond amour.

À l'amour de ma vie, NABIL qui n'a jamais cessé de croire en moi.

A mon frère LYES, à ma sœur SONIA et ses enfants SAMY, SABINE et MAXEN.

À la mémoire de YEMMA DJADJA.

A tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail

- Lydia -

Sommaire

Listes des figures

Liste des tableaux

Introduction Générale

La technologie blockchain introduite en 2009, a connu en l'espace d'une dizaine d'années une évolution spectaculaire. Elle est considérée comme étant une technique révolutionnaire d'effectuer des transactions en se passant d'un tiers de confiance tout en protégeant l'identité des utilisateurs par l'usage de pseudonymes.

De plus en plus d'entreprises et d'organisations sont désireuses de déployer la technologie Blockchain pour la tenue de dossiers et leur gestion commerciale. Cependant la nature publique de la Blockchain, pose un grand problème de préservation de la vie privée des utilisateurs et de confidentialité des données. En effet, de nombreux travaux de recherches ont pu mettre en avant les principales lacunes et faiblesses de cette technologie.

Certaines études sont parvenues à la désanonymisation des utilisateurs, ce qui est une grosse remise en question sur l'intérêt d'utiliser les blockchains. Ces critiques ont justement incité les chercheurs à proposer différentes solutions visant à améliorer la préservation de la vie privée des utilisateurs de la blockchain.

Notre travail est d'étudier la problématique ainsi que les différentes solutions proposées et éventuellement proposer une méthode pour améliorer la protection de la vie privée dans les Blockchains.

Nous avons divisé notre mémoire en quatre chapitres. Dans le premier chapitre nous donnons un aperçu sur la Blockchain et cela en présentant les différentes technologies sur lesquelles elle s'appuie. Nous avons aussi expliqué son fonctionnement ainsi que les différents domaines d'applications.

Dans le second chapitre, nous avons donné une présentation générale du concept de la vie privée, ainsi que les techniques utilisées pour la préserver. Puis nous avons introduit le concept de la vie privée dans la Blockchain, en mettant en avant les techniques utilisées pour l'améliorer.

Dans le troisième chapitre, nous avons réalisé l'étude de différents travaux visant à améliorer la préservation de la vie privée dans les blockchains. Nous avons effectué une comparaison des techniques utilisées par chacun de ces travaux.

Dans le quatrième chapitre, nous présentons notre contribution qui est un modèle de mixage de pièces de monnaies numériques dans un réseau Blockchain et cela en constituant un groupe de mixage constitué de nœuds du réseau. Cette solution vise essentiellement à préserver l'anonymat des utilisateurs de cette Blockchain.

Nous finissons par exposer les différentes améliorations possibles sur le modèle proposé visant à le rendre réalisable sur le terrain.

Chapitre I
Généralités sur les Blockchains

Introduction

Dans ce chapitre, nous allons essayer d'aborder les grandes lignes de la blockchain. Nous allons commencer par définir la blockchain, nous allons énumérer les prérequis technologiques de cette dernière qui sont l'architecture pair à pair (P2P) et la cryptographie asymétrique et expliquer le principe de fonctionnement.

1.1 Concepts de base sur la blockchain

1.1.1 Définition

La blockchain est une technologie de stockage et de transmission d'informations, elle se distingue par le fait qu'elle soit distribuée, infalsifiable, décentralisée, sécurisée et transparente, cela grâce au fait qu'elle soit fondée sur l'échange P2P dans les réseaux.

Nous pouvons dire que c'est une base de données numériques sur laquelle sont inscrits tous les échanges effectués entre ses utilisateurs depuis sa création. C'est parce que les échanges successifs y sont enregistrés sous forme de blocs de transactions que l'on appelle ce registre une "blockchain", ou chaîne de blocs [2].

1.1.2 Prérequis technologiques de la blockchain

1.1.2.1 Architecture pair à pair (P2P)

Dans les recherches réalisées pour entamer ce mémoire, différentes approches ont été trouvées pour définir un réseau pair à pair. Voici une définition parmi beaucoup d'autres,

C'est un modèle de réseau informatique dont les éléments (les nœuds) sont à la fois clients et serveurs lors des échanges. Grâce à ce modèle on a pu décentraliser les réseaux, en opposition aux architectures traditionnelles client/serveur. Ce modèle a pu nous offrir la possibilité des pairs avoir des communications directes, d'égal à égal comme son nom l'indique, entre les différents nœuds du réseau, qui peuvent alors échanger différents types d'informations sans passer par un serveur central [3].

1.1.2.2 Principe de fonctionnement

Les systèmes de partage de fichiers pair-à-pair permettent de rendre les objets d'autant plus disponibles qu'ils sont populaires, et donc répliqués sur un grand nombre de nœuds. Cela permet alors de diminuer la charge (en nombre de requêtes) imposée aux nœuds partageant les fichiers populaires, ce qui facilite l'augmentation du nombre de nœuds et donc de fichiers dans le réseau. C'est ce qu'on appelle le passage à l'échelle. Le modèle pair-à-pair va bien plus loin que les applications de partage de fichiers : il permet en effet de décentraliser des services et de mettre à disposition des ressources dans un réseau, nommées *objets*. Tout nœud d'un réseau pair-à-pair peut alors proposer des objets et en obtenir sur le réseau. Les systèmes pair-à-pair permettent donc de faciliter le partage d'informations. Ils rendent aussi la censure ou les attaques légales ou pirates plus difficiles. Ces atouts font des systèmes pair-à-pair des outils de choix pour décentraliser des services qui doivent assurer une haute disponibilité tout en permettant de faibles coûts d'entretien. Toutefois, ces systèmes sont plus complexes à concevoir que les systèmes client-serveur [4].

Cette architecture présente beaucoup d'avantages mais le plus important c'est le fait qu'il rende le système décentralisé tel que chacun des nœuds est autonome.

1.2 Cryptographie asymétrique

La blockchain utilise le principe de la cryptographie afin de la sécurisé sans passer par une autorité centrale pour veiller à l'application des règles.

La cryptologie est une science clé pour la blockchain. Cependant, il est important de noter que la naissance de la cryptologie est bien antérieure à l'introduction de l'informatique. En effet, le premier document crypté est une tablette en argile retrouvée en Irak datant du XVIème siècle. Un potier y avait inscrit une recette en supprimant des consonnes et en modifiant l'orthographe des mots [6].

1.2.1 Définition

La cryptographie asymétrique, également appelée cryptographie à clé publique, utilise des clés publiques et privées pour chiffrer et déchiffrer des données. Ces clés sont simplement de grands nombres qui sont associés par paires, mais pas identiques

(asymétriques). Une clé de la paire peut être partagée avec tout le monde ; elle est appelée clé publique. L'autre clé de la paire est tenue secrète, c'est la clé privée. L'une ou l'autre de ces clés peut servir à chiffrer un message ; c'est alors la clé opposée à celle ayant servi au chiffrement qui est utilisée pour le déchiffrement [5].

1.2.2 Fonction de hachage

1.2.2.1 Définition

C'est une fonction capable de prendre en entrée n'importe quelle valeur informatique et donner en sortie une valeur d'une taille fixe appelée « **empreinte de hachage** » [6].

Les fonctions de hachage sont :

- Imprédictibles : impossible de prédire à l'avance l'empreinte en sortie.
- Déterministes : si on propose deux fois la même valeur en entrée, alors les deux empreintes en sortie seront identiques.
- Irréversibles : il est impossible de remonter à la valeur d'entrée en possédant la valeur de sortie.

Les fonctions de hachage cryptographique les plus couramment utilisées incluent MD5 (*Message Digest 5)* et la série SHA (Secure Hash Algorithm).

1.2.2.2 Fonction de hachage MD5

MD5 est une fonction de hachage inventée par Ronald Rivest en 1991. Une 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) [8].

1.2.2.3 Fonctions de hachage SHA

- **SHA** ou **SHA-0** est créé par la NSA en 1993. Suite à de premières rapides découvertes de vulnérabilités dans cette fonction, elle est considérée comme obsolète, la NSA publie SHA-1 en 1995, très similaire mais complexifié. Les utilisations des fonctions de la famille SHA sont les mêmes que pour MD5.

Comme toute solution cryptographique, le SHA se doit d'évoluer en même temps que les capacités de calcul de nos ordinateurs et éviter de devenir vulnérable.

- **SHA-1 :** est une fonction de hachage cryptographique qui peut convertir une chaîne de données arbitrairement longue en un condensé d'une taille fixe de 160 bits. Ce résumé est généralement affiché sous la forme d'un nombre hexadécimal de 40 caractères. L'algorithme SHA-1 est considéré comme peu sûr. Les certificats SHA-1 ne sont plus conformes aux exigences de base du forum CA / B (Certification Authority Browser), ni pris en charge par les versions actuelles des principaux navigateurs Web.
- **SHA-2** : est une famille de fonctions de hachage qui ont été conçues sur le modèle des fonctions SHA-1 et SHA-0. Ce sont des fonctions de hachage cryptographiques qui peuvent convertir des chaînes de données arbitrairement longues en résumés de taille fixe (224, 256, 384 ou 512 bits).
- **SHA-256** : elle fait partie de la famille des algorithmes SHA-2, il produit des empreintes de longueur de 256 bits ("0" ou "1" de 64 caractères), Le nombre d'empreintes possibles étant très élevé, le risque de collision (production du même haché) est donc relativement faible. Toute modification du contenu d'un bloc est immédiatement visible même si cette dernière n'est qu'une rupture de casse. L'algorithme SHA-256 est alors qualifié de très fiable [7].
- **SHA-512 :** est une version non réduite de l'algorithme SHA-256 proposant une empreinte de 128 caractères.

Nous retenons que la SHA-256 et SHA-512 sont les plus utilisées dans les blockchains.

1.3 Consensus

1.3.1 Définition

Nous commencerons par la définition littéraire, donnée dans LAROUSSE,

Procédure qui consiste à dégager un accord sans procéder à un vote formel, ce qui évite de faire apparaître les objections et les abstentions données.

Un algorithme de consensus peut être défini comme le mécanisme par lequel un réseau Blockchain parvient à un consensus. Les blockchains publiques (décentralisées) sont construites en tant que systèmes distribués et, puisqu'ils ne dépendent pas d'une autorité centrale, les nœuds distribués doivent se mettre d'accord sur la validité des transactions. C'est là que les algorithmes de consensus entrent en jeu. Ils s'assurent que les règles du protocole soient respectées et que toutes les transactions aient lieu de manière fiable [11].

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

1.3.2 Preuve de travail (Proof of Work)

Appelée aussi preuve de calcul, Il s'agit du traitement cryptographique permettant la validation des blocs de transactions notamment sur Bitcoin. Afin d'éviter qu'une personne puisse valider plusieurs blocs de suites et ainsi autoriser une transaction frauduleuse, le système oblige tous les mineurs à travailler en compétition sur le prochain bloc. Pour valider un bloc, les mineurs doivent trouver le résultat d'une fonction de "hash" qui correspond au bloc. Les mineurs vont, en utilisant la puissance de calcul de leur ordinateur, essayer toutes les combinaisons possibles jusqu'à trouver la bonne. La probabilité d'être celui qui puisse soumettre le bloc dépend ainsi uniquement du ratio entre sa puissance de calcul et celle de l'ensemble des mineurs. Le système PoW (Proof of Work) permet donc d'avoir un validateur aléatoire parmi la masse de mineurs, tout en s'assurant que ce validateur est une machine, impartiale. Effectuer ce traitement requiert du temps de calcul : en général, un seul ordinateur du réseau y parvient en environ dix minutes (Bitcoin). La difficulté est régulièrement adaptée pour maintenir cet intervalle [2].

1.3.3 Preuve d 'enjeu (Proof of stake)

Comme le proof of work, le proof of stake est une méthode utilisée pour atteindre le consensus distribué dans un réseau blockchain. A l'inverse du Proof of work, le Proof of stake ne demande pas aux utilisateurs d'utiliser leur puissance de calcul, mais plutôt de prouver la propriété d'un certain montant de crypto-monnaies. Cependant afin d'éviter

que la concentration de capital ne permette de valider plusieurs blocs à la suite, si je suis désigné "validateur" du prochain bloc, je ne peux participer aux prochains "tirages au sort" pendant un certain temps [2].

1.3.4 Preuve d'autorité (Proof of authority)

Dans un consensus basé sur la PoA, les blocs et les transactions sont validés par des comptes approuvés à l'avance, que l'on appelle en anglais « validator ». Le processus est automatique et mis à part le fait de vérifier que l'ordinateur n'est pas compromis, il n'y a rien d'autre à faire.

Pour devenir un validateur dans le consensus PoA, il faut que votre identité soit formellement vérifiée et affichée sur la blockchain. Car c'est votre identité et votre réputation qui sont mises en jeu, plutôt que votre puissance de calcul ou votre richesse.

Il y a donc 3 piliers sur lesquels ce consensus repose :

- Un moyen de certifier sans aucun doute possible l'identité d'une personne ;
- Un procédé suffisamment difficile à achever pour devenir validateur, afin que la perte de ce titre représente un problème majeur pour le validateur déchu ;
- Un procédé de sélection uniformisé pour tous les validateurs, afin que chacun des validateurs puisse faire confiance aux autres.

En créant un système de réputation lié à une identité, les validateurs sont incités à continuer de valider les transactions de la manière la plus efficace, honnête et transparente possible. S'ils ne le font pas, alors leur identité pourrait être associée à une réputation négative, ce qui leur ferait perdre ainsi leur rôle de validateur difficilement acquis [2].

1.4 Structure d’une blockchain

Comme son nom l’indique la blockchain est constituée d’une chaîne de blocs qui se suivent, chacun d’eux connaît son prédécesseur.

Les transactions effectuées entre les utilisateurs du réseau sont regroupées dans une structure de données appelée **bloc**, ils sont ordonnés et hiérarchisés dans une seule

et unique chaîne. Chaque bloc connaît son prédécesseur **valide**. Cette chaîne est distribuée et répliquée sur tous les nœuds du réseau. [9]

La validation des blocs se fait grâce à certains nœuds du réseau appelés « **mineurs** », ce sont des utilisateurs qui créent et valident les nouveaux blocs assurant ainsi **l'intégrité** de la chaîne.

Chaque nouvelle transaction en attente de validation, est regroupées dans un nouveau bloc, elle est identifiable grâce à son « hash » (empreinte unique) calculé à partir des données qu'elle contient.

Ainsi, un bloc est un regroupement de transactions créées tous les T temps comportant une date de création « horodatage » et une référence pointée à son prédécesseur « hash ».

Une fois le bloc validé la transaction devient visible pour l'ensemble des utilisateurs, qui vont alors l'ajouter à leur bloc [9].

1.5 Caractéristiques de la blockchain

➢ La désintermédiation

La technologie blockchain permet d'échanger sans le contrôle d'un tiers. La validation et l'ajout d'un bloc résultent d'un consensus entre les utilisateurs-validateurs, qui repose sur la possibilité de vérifier leur travail de validation et qui rend inutile le contrôle par une institution de référence. Tout est effectué sans l'intervention d'une autorité centrale, les utilisateurs opèrent la surveillance, et se contrôlent mutuellement, assurant la certification des sauvegardes et leurs cohérences [15].

➢ La transparence

Une fois qu'un document est inscrit sur la blockchain, cela suffit à prouver que ce dernier existe bien à l'instant T et qu'il n'a pas été modifié. La blockchain est qualifiée de transparente car tout le monde peut la télécharger dans son intégralité et vérifier à tout moment son honnêteté. Tous les utilisateurs de la blockchain peuvent ainsi voir les transactions présentes et passées [15].

- **La sécurité**

L'hébergement décentralisé fait également de la blockchain une technologie sûre : elle rend quasi-impossible la suppression de toutes les copies des documents, qui existent sur une multitude de serveurs à travers le monde. La blockchain a une grande résistance, car toutes les données sont copiées dans les différents serveurs. Cela la rend résistante aux cyber-attaques ou au contrôle de l'État. En effet, s'il est possible de s'attaquer à un ou plusieurs ordinateurs, il est plus compliqué de s'attaquer aux blocs d'informations copiés dans l'ensemble des ordinateurs connectés au réseau. Cela offre à la blockchain un haut niveau de sécurité. [15]

- **L'autonomie**

La puissance de calcul et l'espace d'hébergement sont fournis par les nœuds du réseau, c'est-à-dire les utilisateurs eux-mêmes. Il n'y a donc pas besoin d'infrastructures centrales. Au sein d'une blockchain, l'infrastructure n'est plus concentrée dans les mains d'une organisation mais est, au contraire, éclatée dans l'ensemble des points du réseau. Une blockchain est donc autoportante et indépendante de services tiers [15].

- **Open source**

La technologie de la blockchain est formulée de manière à fournir un accès open source à toutes les personnes connectées au réseau. Cette polyvalence inimitable permet à quiconque non seulement de vérifier publiquement les enregistrements, mais également de développer diverses applications. [17]

- **L'anonymat**

Lorsque le transfert de données a lieu entre nœuds, l'identité de l'individu reste anonyme, ce qui en fait un système plus sécurisé et fiable [17].

- **L'immutabilité**

Les enregistrements effectués sur la blockchain sont dits immuables, une fois stockés, ils deviennent archivés pour toujours et ne peuvent pas être modifiés facilement sans le contrôle simultané de plus de 51 % des nœuds du réseau. Le système cryptographique de validation garantit qu'il est quasiment impossible de réécrire une transaction une fois son bloc validé [17].

1.6 Fonctionnement

Pour pouvoir comprendre et assimiler le fonctionnement de la blockchain, nous allons le découper en étapes distinctes, comme l'illustre la figure 1 :

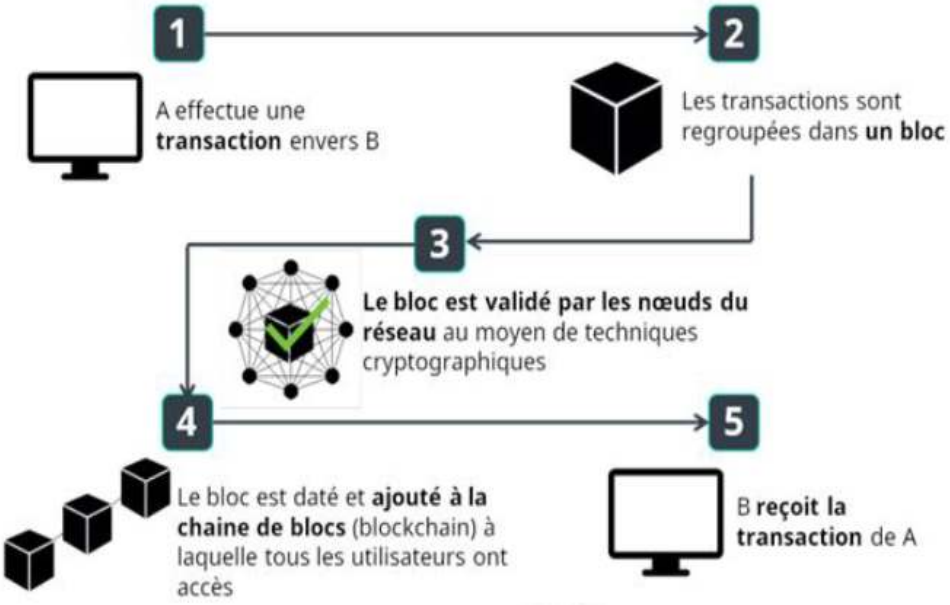

Figure 1 : Fonctionnement d'une blockchain

1. A effectue une transaction vers B,
2. Les transactions sont regroupées dans un bloc,
3. Le bloc est validé par les nœuds du réseau,
4. Le bloc est daté et ajouté à la chaîne de blocs,
5. B reçoit la transaction de A.

Pour être valide, chaque transaction doit être signée, au sens cryptographique du terme en utilisant la cryptographie asymétrique (clé privée, clé publique). Puis les autres nœuds du réseau vérifient la validité de la transaction en utilisant la clé publique de cet utilisateur.

La création des nouveaux blocs est effectuée par les nœuds du réseau qui sont appelés mineurs en analogie avec les chercheurs d'or, qui sont en constante compétition car celui qui pourra ajouter son bloc se verra récompensé, cette étape est appelée minage. Elle consiste en la résolution d'un algorithme de consensus par les différents

mineurs et le premier pourra soumettre son bloc aux autres nœuds pour vérification et validation.

Une fois cette étape effectuée, le bloc est ajouté à la chaîne et les transactions qu'il contient deviennent effectives.

1.6.1 Signature d'une transaction

Chaque transaction a recours à la cryptographie asymétrique proposée pour la première fois par Diffie et Hellman en 1976,elle est très répondue pour sécuriser les échanges d'information, car elle permet d'assurer l'origine des données(identité de l'auteur d'une transaction) tout en préservant leurs confidentialité (génère une signature numérique unique), elle fonctionne pour chaque utilisateur, avec une paire de clés l'une privée et l'autre publique .dans le cas du Bitcoin cette paire permet de signer la transaction [12].

- **La Clé privée**

C'est une suite aléatoire de chiffres créé par un auteur d'une transaction, elle permet de signer la transaction fournissant ainsi une preuve sûre qu'il en est le propriétaire. Toutes modifications de la transaction après son émission sont interdites grâce à la signature. La transaction est ensuite placée dans un nœud quelconque du réseau qui va se charger de sa diffusion de proche en proche sur tous les nœuds du réseau [14].

- **La Clé publique**

Une fois que la transaction est reçue par tous les nœuds, ces derniers possédant la clé publique, ils vont devoir procéder à l'identification de l'auteur de la transaction, nous détaillerons par la suite l'intérêt de l'utilisation des algorithmes (MD5, SHA-256).

- **Horodatage (time stamping)**

L'horodatage est une propriété qui permet à un auteur de prouver qu'il en est bien le propriétaire et que tout autre bloc reprenant son travail et produit après la création de son bloc est par conséquent une copie non autorisée. Grâce au principe d'immutabilité. La date est une preuve qu'une transaction a été effectuée à un instant T.

Les blocs alors constitués de plusieurs transactions signées par clés publiques sont ensuite horodatés par leur auteur, cet aspect est essentiel car il permet de réaliser une datation relative respectant la chronologie dans laquelle les transactions sont classées les unes après les autres [2].

La figure 2 illustre le rôle du hash dans la liaison entre deux blocs successifs.

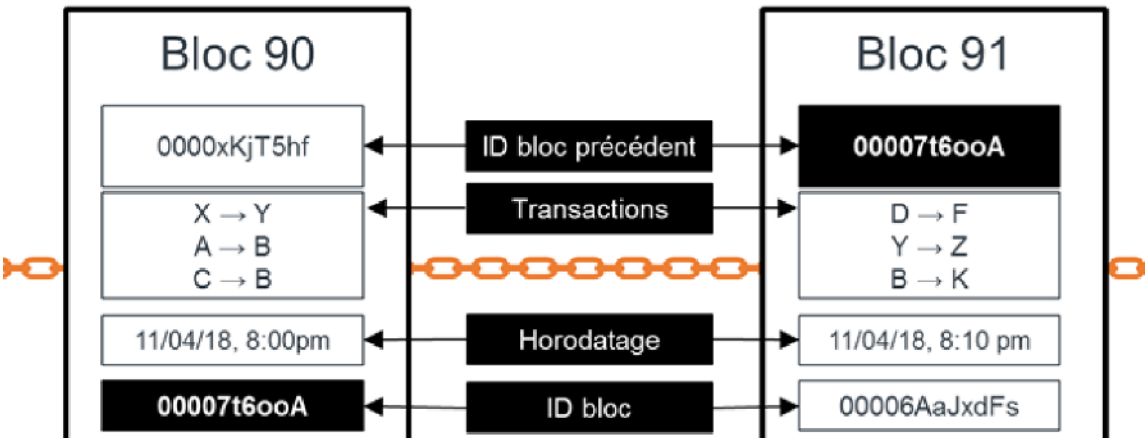

Figure 2 : Structure d'une blockchain et le rôle des hashs

Le fait que la blockchain soit basée sur les fonctions de hachage pour relier les blocs entre eux, limite le risque de production de deux blocs simultanés et assure qu'un bloc valide ait le temps de se diffuser dans l'ensemble du réseau avant qu'un suivant ne soit créé.

1.7 Types de blockchain

Nous avons trois types de blockchain: les blockchains publiques, les blockchains privées et les blockchains de consortium.

- **Blockchain publique**

Ce sont les blockchain qui sont accessibles par n'importe quelle personne dans le monde, donc n'importe qui peut envoyer des transactions qui pourront être ajoutées à la blockchain après vérification et validation bien-sûr, de plus n'importe qui peut participer au minage.

Dans le cadre d'une blockchain publique, tout utilisateur est libre de créer son propre nœud distribué. Ainsi chacun de ces nœuds est anonyme et doit être considéré comme entité non fiable. Un mécanisme de consensus entre ces nœuds, qui sont généralement nombreux, doit être employé afin de pallier efficacement aux attaques. Ce problème a été résolu par toutes les premières plateformes blockchains en exigeant des nœuds qu'ils fournissent une preuve de travail (la Proof of Work ou PoW) difficilement réalisable mais facilement vérifiable. Cette preuve nécessite la dépense d'une quantité significative d'énergie, ce qui garantit la sécurité du mécanisme et endigue le déploiement potentiel de nœuds malveillants visant à manipuler le consensus [13].

Nous pouvons citer la blockchain Bitcoin et Ethereum comme exemple les plus connus.

- **Blockchain privée**

Enfin, il y a les blockchains totalement privées, dont l'accès d'écriture est délivré par une organisation centralisée (par exemple une banque centrale), mais où les autorisations de lecture peuvent être publiques ou restreintes [13].

- **La blockchain de consortium**

Une blockchain de consortium est un type semi-décentralisé où plus d'une organisation gère un réseau blockchain. Ceci est contraire à ce que nous avons vu dans une blockchain privée, qui n'est gérée que par une seule organisation. Plus d'une organisation peut agir en tant que nœud dans ce type de blockchain et échanger des informations ou faire du minage. Les blockchains de consortium sont généralement utilisées par les banques, les organisations gouvernementales, etc... [18].

- **Blockchain hybride**

Une blockchain hybride est une combinaison de la blockchain privée et publique. Il utilise les fonctionnalités des deux types de blockchains, c'est-à-dire que l'on peut avoir un système privé basé sur des autorisations ainsi qu'un système public sans autorisation. Avec un tel réseau hybride, les utilisateurs peuvent contrôler qui a accès à quelles données stockées dans la blockchain [18].

1.8 Exemples de Blockchain

1.8.1 Bitcoin

Le réseau Bitcoin est basé sur l'algorithme de preuve de travail HashCash, mais au lieu d'utiliser une fonction informatique de confiance comme le RPoW, la protection contre la double dépense est assurée par un protocole pair à pair décentralisé afin de suivre et de vérifier les transactions. Les bitcoins sont « minés » en tant que récompense, en utilisant le mécanisme de preuve du travail, par des mineurs individuels et les transactions sont ensuite vérifiées et validées par les nœuds décentralisés dans le réseau [1].

Le 3 janvier 2009, le Bitcoin est né quand le premier bloc de Bitcoin est miné par Satoshi Nakamoto, le bloc offrait une récompense de 50 bitcoins [1].

Il faut savoir que Bitcoin avec un B majuscule fait référence à la Blockchain Bitcoin tandis que bitcoin avec un B minuscule fait référence à la crypto-monnaie qui y est utilisée.

1.8.2 Ethereum

L'Ethereum est né en 2013, le programmeur et cofondateur du Bitcoin Magazine, Vitalik Buterin déclara que le Bitcoin avait besoin d'un langage de script pour construire des applications décentralisées. Mais il n'a pas réussi à trouver un accord au sein de la communauté Bitcoin, alors il lança le développement d'une nouvelle plate-forme informatique distribuée et basée sur la Blockchain : l'Ethereum, dotée d'une fonctionnalité de script appelée « smart contracts » (des contrats intelligents) [1].

La crypto-monnaie de l'Ethereum s'appelle l'Ether, elle peut être transférée entre des comptes et est utilisée pour payer les frais, engendrés par la puissance de calcul informatique consacrée à l'exécution des smart contrats [1].

1.8.2.1 Contrats intelligents (Smart contracts)

Les smart contrats sont des programmes ou des scripts, utilisés pour faire une transaction si certaines conditions sont réunies. Les smart contrats sont écrits dans des langages de programmation spécifiques et compilés en bytecode, qui est une machine

virtuelle « Turing-complet» décentralisée (EVM pour Ethereum Virtual Machine) pouvant ensuite les lire et les exécuter.

Les développeurs ont aussi la possibilité de créer et de publier des applications fonctionnant sur la blockchain Ethereum. Ces applications sont généralement appelées DApps (Applications décentralisées) et il en existe déjà des centaines, dont des plateformes de réseaux sociaux, des applications de paris sportifs ainsi que des échanges financiers [1].

1.9 Évolution chronologique de la technologie blockchain

Les fonctionnalités de la technologie blockchain ont évolué au fil du temps. On peut aujourd'hui distinguer trois stades : Blockchain 1.0, Blockchain 2.0 et Blockchain 3.0.

- **La Blockchain 1.0**

Le déploiement des cryptographies et architectures distribuées dans les applications liées aux liquidités, telles que le transfert de devises et les systèmes de paiement numérique, ont permis de former la couche technologique supportant la création de la Blockchain 1.0. Le premier type de transactions a été le Bitcoin qui utilise une crypto-monnaie virtuelle. Cette application a connu une forte notoriété dans la sphère publique sans pour autant concurrencer les marchés des changes internationaux. Cette évolution représente une alternative au modèle d'affaires traditionnel des tiers de confiance [16].

- **La Blockchain 2.0**

L'ensemble des applications économiques, commerciales et financières requièrent des fonctionnalités plus larges que de simples transactions monétaires. La Blockchain 2.0 a vu le jour : elle a permis l'utilisation de modèles de « contrats intelligents ». Les contrats intelligents (dits Smart contracts) sont des protocoles numériques capables de reconnaître automatiquement si les conditions prédéfinies de réalisation d'une transaction sont réunies, puis, le cas échéant, d'en appliquer les termes, sans intervention d'un tiers [16].

- **La Blockchain 3.0**

La Blockchain 3.0 est un concept d'application au-delà de la crypto-monnaie. Elle s'appuie sur les contrats intelligents pour développer des organisations décentralisées autonomes qui possèdent leurs propres procédures légales définies en amont par les membres du réseau. Cette Blockchain 3.0 n'en est encore qu'au stade de concept [16].

1.10 Domaines d'application de la blockchain

- **La chaîne d'approvisionnement**

La chaîne d'approvisionnement est un segment très complexe et il est devenu plus difficile d'avoir une visibilité transparente sur l'ensemble de la chaîne d'approvisionnement. Il est devenu plus difficile de suivre le flux de matériel et les canaux de distribution, ce qui a entraîné divers comportements contraires à l'éthique dans les entreprises, allant du commerce illégal aux produits de contrefaçon et aux dommages environnementaux. Tout au bout de la chaîne d'approvisionnement, les consommateurs ne disposent pas des informations selon lesquelles un produit final a été importé tout au long de la chaîne d'approvisionnement. De nos jours, vous pouvez perdre vos colis par la poste. En tirant parti de la convergence du paradigme IoT (internet of thing) et des contrats intelligents, vous pourrez enregistrer la position à tout moment de vos colis grâce à la connexion de capteurs à chaque étape [17].

- **L'identité numérique**

Garantit un moyen plus sûr de vérifier l'authenticité d'une personne et d'éviter et de réduire les fraudes possibles [17].

- **Le 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 [17].

- **Les Soins de santé**

Les établissements de santé doivent faire face à des problèmes de sécurité et de confidentialité lorsqu'ils partagent des données sur plusieurs plates-formes. L'amélioration de la collaboration de données entre fournisseurs signifie l'amélioration de nombreux aspects du domaine de la santé, tels que la précision des diagnostics et l'efficacité des traitements. Blockchain peut créer cet environnement sécurisé pour permettre aux établissements de santé, aux payeurs et aux autres acteurs de ce domaine de partager l'accès à leur réseau avec des garanties d'intégrité des données [17].

La figure ci-dessous regroupe un grand nombre de domaines d'application des blockchains.

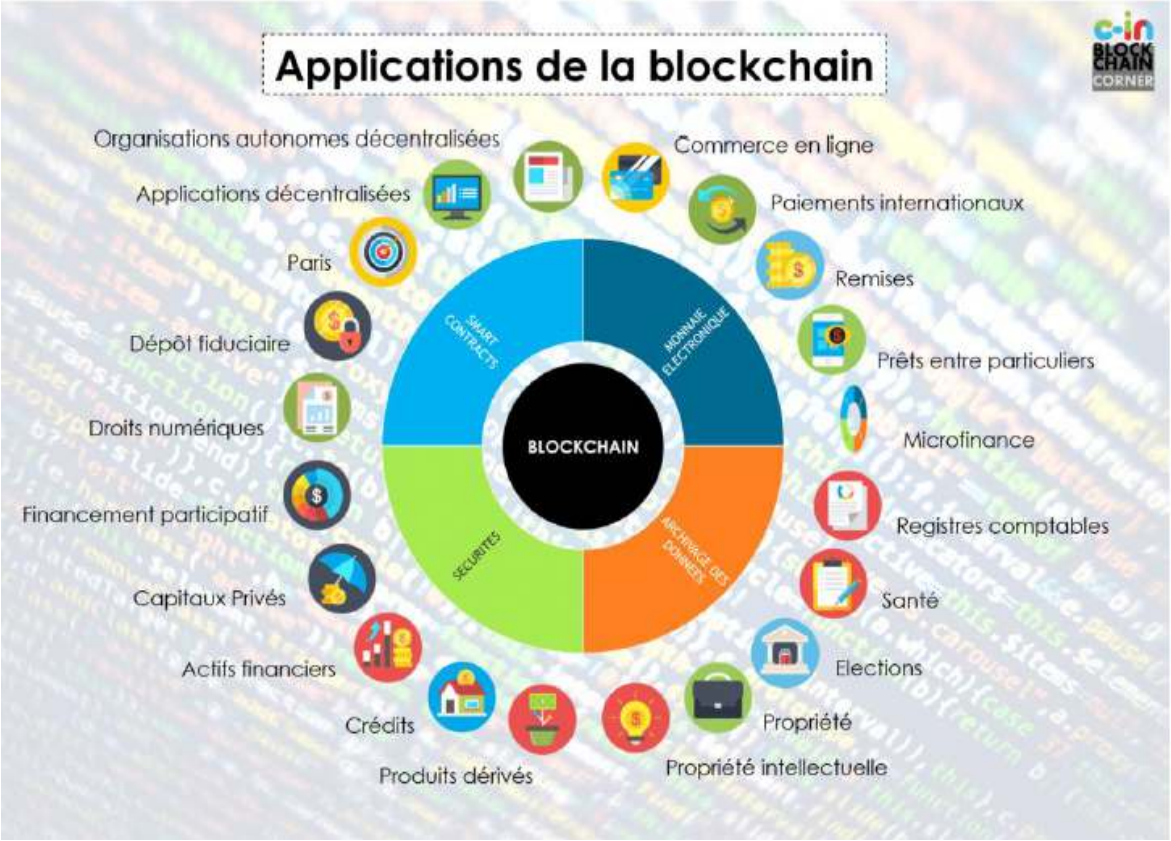

Figure 3 : Les domaines d'application de la blockchain

Conclusion

Au cours de ce chapitre nous avons défini la blockchain, les prérequis technologiques, son principe de fonctionnement.

Nous avons aussi présenté les différents types de blockchains, son évolution et enfin les domaines d'application de celles-ci.

Chapitre II

Vie privée

Introduction

Le concept de "vie privée" (privacy en anglais) est un concept général, qui a des différents sens selon les personnes et varie selon chaque individu et du contexte. Ce concept peut englober plusieurs notions telles que : le droit d'être seul, le droit à la liberté de penser, le droit à une propre vie familiale, le droit de protéger sa réputation, etc. De plus, ces notions peuvent varier d'un contexte à un autre [19].

Sur Internet par exemple, la vie privée englobe toute une gamme de questions touchant à la capacité des utilisateurs d'Internet à assurer le contrôle et la transparence sur l'utilisation de leurs données personnelles lorsqu'elles sont recueillies et utilisées par des entités privées ou publiques. L'objectif de ce chapitre est de donner une vue générale sur certains aspects de cet important concept, les différentes menaces visant à atteindre la vie privée des utilisateurs ainsi que les techniques développées afin de la préserver, et on finira par voir, comment la vie privée est-elle préservée dans les blockchains.

2.1 vie privée

2.1.1 Définition

Étant un concept vaste et ambigu nous allons prendre la définition donnée par [19] pour définir la vie privée comme étant le droit de contrôler l'accès et l'utilisation des informations personnelles et les localisations spatiales, c'est-à-dire, toute information ou acte destinés à être individuels à une personne et à elle seule sont privés au grand public, telles que l'identité de la personne, dossiers médicaux, conversations privées (mails, sms, etc.), photos et vidéos personnelles

2.1.2 Vie privée et législation

L'un des principaux buts de la législation est d'instaurer des lois pour assurer la protection de la vie privée des personnes en protégeant leurs renseignements personnels dont des institutions ont la garde ou le contrôle. La loi protège la vie privée en :

- énonçant les règles qui déterminent quels renseignements personnels peuvent être collectés par les institutions et par quels moyens ;

- énonçant les règles régissant le traitement, la gestion et le partage des renseignements personnels entre les institutions et entre d'autres organismes gouvernementaux ;

- établissant pour les personnes des procédures d'accès à leurs propres renseignements personnels, sous réserve de quelques exemptions nécessaires et clairement définies [41].

2.1.3 Principes de la vie privée

Plusieurs principes fondamentaux peuvent être déployés pour assurer la protection de la vie privée. Ces principes doivent être implémentés dans tout système ou architecture compatible avec la protection de la vie privée. Ils existent des principes relatifs aux données et d'autres à l'identité et aux activités de l'individu.

2.1.4 Protection des données

- La Minimisation des données : Ce principe exige que les données collectées devront être utilisées uniquement pour des finalités déterminées, légitimes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées.
- Le Consentement explicite : Ce principe exige que toute collecte ou traitement de données personnelles ne doive avoir lieu sans l'autorisation explicite et préalable de la part du propriétaire de ces données.
- La Souveraineté des données (droit à l'oubli) : Ce principe donne à un individu le droit d'accès à ses informations personnelles, de les corriger et de les supprimer.
- La Transparence : Ce principe impose que l' utilisateur à le droit d'être informé sur ces informations personnelles collectées, et comment et pourquoi ses données sont utilisées et avec qui elles sont partagées.
- La Sécurité : une organisation qui détient des renseignements personnels doit assurer des mesures de sécurité contre la perte, l'accès non autorisé, l'utilisation abusive ou la divulgation [42].

2.1.5 Protection de l'identité et des activités

- L'anonymat : Ce principe permet à un utilisateur de réaliser une action sans que celle-ci puisse être reliée à son identité.

- Le pseudonymat : Ce principe définit le fait qu'un système offre à ses usagers la possibilité d'agir sous un pseudonyme au lieu de leurs vraies identités.
- La non-chaînabilité : Ce principe définit le fait que dans un système, un attaquant soit incapable de relier deux actions anonymes qui ont été menés par le même individu.
- La non-observabilité : Ce principe définit le fait qu'un attaquant soit incapable de savoir, à un instant donné, si une action particulière a lieu ou non [44].

2.1.6 Menaces sur la vie privée

Toutes les menaces relatives à la vie privée concernent l'utilisation non autorisée ou malveillante des données collectées. Les menaces les plus fréquentes sont :

- Divulgation des données personnelles : trouver et accéder à des informations personnelles est devenu une opération très simple en raison de l'émergence des réseaux sociaux et des services de partages de contenus. Les photos, videos, dates de naissance, préférences musicales ou culinaires ou encore lieux de loisir souvent fréquentés, partagés naïvement sur ces plates-formes augmentent les risques de préjudice, de discrimination et de perte d'autonomie, ce qui est un danger permanent sur l'individu.
- Vol et usurpation d'identité : Le vol d'identité est l'un des crimes qui connaît la plus forte croissance. On peut considérer qu'il s'agit d'un vol d'identité, chaque fois qu'un criminel s'empare d'une partie des données d'une personne et les utilise à son propre profit.
- Profilage : Le profilage désigne le fait de compiler des dossiers d'information sur des individus afin de déduire des intérêts et des caractéristiques par corrélation avec d'autres profils et données. Le profilage est un avantage, s'il est utilisé par exemple dans les systèmes de recommandations qui proposent aux clients des produits et des services qui correspondent à leurs préférences et leurs intérêts, mais devient une menace sur la vie privée dans ces deux cas :

  – si les données sont collectées d'une manière illégale en utilisant les diverses techniques de trackage et de surveillance.

  – si les profils issus après le traitement des données collectées, sont utilisés pour des mauvaises fins, comme : la discrimination par les prix, les publicités non sollicitées et nuisibles et les spams.

2.2 Technologies de protection de la vie privée

2.2.1 Technologies de protection de la vie privée sur internet

2.2.1.1 Les systèmes de gestion des identités et des accès

En anglais Identity and Access Management (IAM), un ensemble de processus relatifs à l'identification des individus au sein d'un système et au contrôle de leur accès à des ressources mises à disposition au sein de ce système, en associant droits et restrictions d'utilisation à l'identité établie [43].

2.2.1.2 Accréditations anonymes

C'est un ensemble de techniques à base cryptographique, permettant à un utilisateur de présenter des preuves de qualification, de compétence ou d'autorisation d'accès émises par une autorité pour un individu sans révéler quoi que ce soit sur lui-même d'autre que la possession de l'accréditation. Pour certifier des attributs ou des messages, des techniques complexes sont utilisées, comme : la signature aveugle, la signature de groupe et la preuve de connaissance à divulgation nulle [46].

2.2.1.2.1 Signature aveugles : (Blind signature)

Ce concept offre la possibilité de faire signer un message, sans que le signataire puisse lire le contenu de ce message. Le principe de base pour réaliser ce type de signature est d'utiliser une fonction d'aveuglement (qui chiffre le contenu d'un message) et son inverse. La signature se déroule en 3 étapes : [44]

- Aveuglement du message msg par le propriétaire en utilisant une fonction de chiffrement et un facteur aléatoire b, appelé facteur d'aveuglement.

$aveugle(msg, b) = msg_{av}$.

- Signature du message aveuglé par un signataire avec sa clé privée Pr_{key}.

$sign(msg_{av}, Pr_{key}) = msg_{sig}$.

- Vérification du message signé par le propriétaire en utilisant la fonction inverse de la fonction d'aveuglement.

$msg : aveugle^{-1}(msg_{sig}, b) = sign(msg, Pr_{key})$.

2.2.1.2.2 Signatures de groupe : (group signature)

Analogue à la signature numérique, cette technique est utilisée généralement pour vérifier l'appartenance d'un individu à un groupe (qui peut avoir un accès à des ressources) sans révéler son identité. C'est-à-dire que chaque personne appartenant au groupe possède une clé privée propre à lui, et une unique clé publique pour tous les membres (clé publique du groupe). La vérification qu'un message ait bien été signé par un membre du groupe se fait avec la clé publique du groupe, sans connaître son identité c'est-à-dire qu'on ne pourra jamais savoir lequel. En parallèle, les utilisateurs ne peuvent pas abuser de cet anonymat puisqu'une autorité est capable de lever l'anonymat des utilisateurs (malveillants) en utilisant une information secrète. La signature de groupe passe par les étapes suivantes : [44]

- L'enregistrement : Pour appartenir à un groupe « G », un individu « i » doit s'enregistrer à ce groupe pour avoir sa clé privée de signature « SK_{gi} ».
- La signature : pour signer un message « *msg* », un individu « *i* » utilise sa clé privée « SK_{gi} » le résultat est un message signé msg_{sig} (sign(msg, SK_{gi}) = msg_{sig}).
- La vérification : pour vérifier la validité de la signature, un vérificateur utilise la clé publique de vérification « VK_g » du groupe « G » et le message signé msg_{sig} (verif(msg_{sig}, VK_g)).

2.2.1.2.3 Signatures d'anneau : (Ring signature)

La signature d'anneau est une technologie couramment utilisée dans le domaine de la protection de la vie privée. Elle a été introduite en 2001 [49], un travail qui consiste à former un anneau par des participants au réseau et créer une signature de groupe simplifiée qui divulgue des secrets de manière anonyme. Cette signature est basée sur la clé privée de l'initiateur de l'anneau, les clés publiques des membres de l'anneau, des nombres aléatoires ainsi que d'autres technologies. Le vérificateur peut juste vérifier que cette signature provient de ce groupe de signataires sans jamais pouvoir savoir qui est l'initiateur. Ainsi l'anonymat est préservé.

2.2.1.2.4 Preuve de connaissance à divulgation nulle : (zero-knowledge proof)

C'est une technique qui permet de prouver la validité d'une déclaration sans avoir à divulguer une quelconque information, cette fonctionnalité permet de garantir la

confidentialité des données et de protéger les informations sensibles. Une autre variante des zk proofs connue sous le NIZK proof (non iterative zero-knowledge) est largement utilisée puisqu'elle réduit drastiquement la complexité de la communication.

2.2.1.2.5 Chiffrement homomorphe : (Homomorphic encryption)

Le chiffrement homomorphe est une technique cryptographique qui permet d'effectuer des calculs directement sur des données cryptées, le résultat du calcul est le même que celui effectué sur les données originales [51]. Ce qui permet de préserver la confidentialité des données manipulées. Il peut aussi être vu comme une extension de cryptographie symétrique ou à clé publique.

2.2.1.2.6 Calcul multipartie sécurisé : (Multi-party computation)

Noté MPC ou parfois SMPC (Security Multi-Party Computation) est un protocole cryptographique qui permet à des parties distribuées mutuellement méfiantes les unes des autres de calculer conjointement une fonctionnalité arbitraire sans avoir à révéler leurs propres entrées et sorties privées [50]. Ce qui permet la préservation de la vie privée car aucune autre information n'a été échangée.

2.2.1.3 Réseaux de communication anonymes

C'est une technologie de protection de la vie privée, permettant de communiquer de manière anonyme dans un réseau, c'est à dire en protégeant l'identité de l'émetteur et/ou du récepteur du message parmi un groupe (ou l'ensemble de la population), en assurant la non-chaînabilité et la non-observabilité.

2.2.1.3.1 Réseau de mixage : (Mix network)

Mix network (Mix-nets) est une famille de modes de routage favorisant l'anonymat en empêchant l'analyse du trafic, en cachant le lien entre les messages entrants et sortants par un mécanisme de chiffrement et de permutation des messages, autrement dit, Le mixeur reçoit en entrée plusieurs paires du type (message ; adresse du destinataire) qui ont été préalablement chiffrées puis déchiffre une couche de chiffrement et relaie le message jusqu'au destinataire.

2.2.1.3.2 TOR : (The Onion Router)

C'est un réseau mondial décentralisé, anonyme organisé en couches autour de routeurs qui jouent le rôle de nœud, il Permet d'anonymiser tout type de communication faite sur Internet. Le réseau Tor est constitué d'un groupe de serveurs (routeurs onion), son principe de fonctionnement est très semblable à celui des Mix-nets, à part l'étape de mixage qui n'existe pas, d'ailleurs, c'est l'une des raisons qui rend Tor plus efficace et plus rapide qu'un réseau Mix-net. La sécurité dans Tor est basée principalement sur le choix des routes difficiles à prédire par un adversaire. Cependant, et contrairement aux mix networks, Tor est incapable de résister contre une attaque d'un adversaire capable de voir le chemin entier des serveurs Onion [45].

2.2.1.3.3 Crowds

Protocole de communication anonyme qui protège l'anonymat de l'envoyeur d'un message en le routant de manière aléatoire, vers des groupes d'utilisateurs similaires. L'idée principale est de cacher l'origine d'un message en le dispersant. Les nœuds sont groupés dans des "Crowds". Seuls les nœuds d'un même Crowd peuvent se connecter entre eux pour relayer le trafic. Chaque nœud d'un crowd est nommé "jondo". Tout utilisateur qui rejoint le réseau devient un jondo. Un serveur nommé "blender" administre les nœuds du réseau. Un utilisateur rejoint un Crowd en s'enregistrant auprès du blender. Celui-ci avertit tous les nœuds du Crowd de l'arrivée du nouveau nœud. Lorsque l'utilisateur veut accéder à un site web, il va sélectionner un jondo au hasard et lui transfère la requête. Celui-ci va choisir aléatoirement s'il transfère le paquet à un autre jondo (qui sera toujours choisi au hasard) ou s'il l'envoie directement au serveur web. Le processus est répété jusqu'à ce que la requête arrive à destination. La réponse du serveur est renvoyée en sens inverse. Un jondo ne peut pas savoir si les paquets qu'il reçoit proviennent de la source ou d'un jondo intermédiaire [47].

2.2.2 Technologies de protection de la vie privée dans le Bigdata

Aujourd'hui, les méga-données sont utilisées dans tous les domaines de la science, de la technologie et des activités socio-économiques, la protection de ces données est alors primordiale pour conserver la vie privée des individus, les techniques clés utilisées pour les protéger sont :

2.2.2.1 Pseudonymisation

Le pseudonymat est utile pour protéger les données stockées, dans la mesure où il n'est pas toujours possible de rendre les données anonymes. Elle est également utile pour conserver les informations nécessaires à des fins de traitement : scientifiques, statistiques ou même historiques. Le chiffrement est couramment utilisé afin de réaliser ces objectifs. Le pseudonymat par chiffrement remplace les attributs identifiants (ID) et quasi-identifiants (QID) par d'autres chiffrés ce qui signifie que l'identité est cachée, mais en même temps la possibilité de la ré-identifier reste possible. Le plus grand avantage des pseudonymes est qu'il n'y a aucune restriction sur le traitement ultérieur des données. Tant que nous ne pouvons pas identifier directement les champs que nous traitons, nous pouvons effectuer exactement les mêmes calculs que dans les bases de données non anonymes [48].

2.2.2.2 K-anonymat

Une publication de données est dite anonyme, si les informations relatives à chaque personne contenue dans la publication ne peuvent être perçues par au moins k-1 personnes dont les informations figurent dans la publication. Dans le contexte des problèmes de k-anonymat, une base de données est une table qui se compose de n lignes et m colonnes, où chaque ligne de la table représente un enregistrement relatif à un individu particulier d'une population, il existe deux techniques courantes pour réaliser le k-anonymat pour une certaine valeur de k dans une table [48].

2.2.2.2.1 Suppression

Cette technique génère une table anonyme où toutes les données de la table originale sources d'un risque de réidentification sont retirées. Une suppression peut concerner aussi bien la suppression de tuples dans leur totalité que la suppression de quelques données de tuples (remplacement par la valeur nulle). Dans le premier cas, on parle de suppression globale. Le second cas est nommé suppression locale [26].

2.2.2.2.2 Généralisation

La généralisation consiste à diluer une information afin qu'elle ne puisse plus être attachée à une personne ou un faible groupe de personnes (par exemple, tous les noms de ville sont remplacés par le nom du pays, la date de naissance est remplacée par l'année de naissance, …).

2.2.2.2.3 L-diversité

Elle vient renforcer le k-anonymat en évitant, dans le cas où le QIT d'une victime est connu, de cibler un enregistrement d'une table publiée et donc, de ce fait, de révéler de façon directe des données sensibles de la victime. Une classe d'équivalence respecte la contrainte de l-diversité, si elle contient au moins ℓ valeurs "représentatives" pour l'attribut sensible [25].

2.2.2.2.4 T-proximité

Bien que la l-diversité protège les tables, il est tout de même possible pour un adversaire d'obtenir des informations au sujet d'un attribut sensible dès lors qu'il dispose d'informations sur la distribution globale de cet attribut. Pour contrer cela, la t-proximité a été proposée. Ce modèle fait en sorte que la distribution de l'attribut sensible au sein de n'importe quelle classe d'équivalence soit proche de la distribution globale de l'attribut. En d'autres termes, il introduit le concept de distance entre ces deux distributions et propose que cette distance ne dépasse pas un seuil t. Ainsi, plus t est petit, plus la possibilité d'inférence de l'adversaire est réduite [25].

2.2.2.2.5 Confidentialité différentielle

La confidentialité différentielle (differential Privacy) est une méthode très en vogue dans les milieux de la recherche en informatique depuis quelques années, car contrairement aux méthodes précédentes, elle est la seule à donner des garanties formelles, c'est-à-dire des preuves mathématiques, sur la possibilité de borner les informations qu'on peut apprendre sur les individus. Elle permet d'obtenir des informations utiles à partir des bases de données qui contiennent des données personnelles, sans révéler l'identité personnelle des individus [25,48].

2.3 Vie privée et la blockchain

La protection de la vie privée a été largement étudiée dans les blockchains, en tant que type de base de données distribuée, la technologie blockchain a des avantages significatifs en matière de protection de la vie privée, tels que l'inviolabilité des données et l'anonymat des utilisateurs, Cependant, le mécanisme d'architecture décentralisée et le stockage des données adopté par la technologie blockchain apportent également certains effets négatifs sur la protection de la vie privée. Les deux principaux problèmes sont le défi de la confidentialité de l'identité (anonymat) et le défi de la confidentialité des transactions (des données) de l'utilisateur.

2.3.1 Vie privée de l'utilisateur (anonymat)

La vie privée des utilisateurs (anonymat) est la capacité de convertir l'identité réelle d'un utilisateur de blockchain en quelque chose qui ne peut pas être identifié, et en veillant en outre à ce que l'identité d'origine reste également impossible à obtenir [10]. L'anonymat cache l'identité réelle de l'utilisateur en masquant l'adresse réseau réelle des utilisateurs avec une adresse générée par ordinateur [51].

2.3.2 Vie privée des données (confidentialité)

La vie privée des données dans la blockchain consiste à cacher le contenu d'une transaction. La vie privée des données est également appelée confidentialité. Au niveau le plus élémentaire, le contenu des données d'une transaction est généralement crypté pour maintenir la confidentialité dans le réseau. Le maintien de la confidentialité des données garantit que le contenu de la transaction est exempt d'accès, d'ingérence et de modification non autorisés [51].

Dans les blockchains, bien que les utilisateurs échangent des transactions directement en utilisant des pseudonymes, n'importe qui peut suivre ces transactions, voir le montant exact des échanges et par quels pseudonymes ces échanges ont été effectués. Ce qui a entraîné des tentatives réussies de lier ces pseudonymes aux entités du monde réel comme montré dans [53]. Par conséquent, de nombreuses d'études tentant d'améliorer la préservation de la vie privée dans les blockchains ont été menées

et basées sur deux techniques distinctes, à savoir des techniques de mixage et des primitives cryptographiques, que nous allons voir au chapitre 3.

Conclusion

Dans ce chapitre nous avons présenté une vue générale sur la vie privée. En particulier, nous avons introduit une définition relative à la vie privée, un bref aperçu du rôle de la législation dans ce domaine, ainsi que les principales menaces et attaques sur la vie privée des utilisateurs, et enfin quelques exemples de technologies et approches de lutte contre ces attaques dans une première partie, d'une manière générale ensuite dans les blockchains.

Bien évidemment, aucune solution de protection n'est parfaite. Les Solutions à base des techniques cryptographiques, comme les systèmes d'accréditations anonymes et les réseaux de communication anonyme, sont efficaces en termes de protection d'un côté, mais coûteuses en consommation de ressources et en temps d'exécution d'un autre côté, ce qui pose des problèmes de scalabilité et de temps de réponse. Enfin, nous notons que le domaine de la vie privée est un domaine très vaste et très complexe, et loin d'être englober dans sa totalité dans le cadre d'un modeste mémoire de master.

Dans le chapitre qui suit, nous allons présenter un état de l'art de certains travaux réalisés pour améliorer la protection de la vie privée et l'anonymat depuis la création des blockchains.

Chapitre III

Etat de l'art sur les techniques d'anonymat dans la Blockchain

Introduction

Dans le but de proposer une solution améliorant la préservation de l'anonymat dans les Blockchain, nous avons commencé par l'étude des travaux ayant traité ce sujet.

Dans [21], les auteurs ont discuté des problèmes de confidentialité liés à l'identité de l'utilisateur et à la confidentialité des transactions dans les systèmes Blockchain, cette étude a couvert les techniques de protection de la vie privée dans la technologie Blockchain entre autres, le mécanisme de mixage, la preuve à connaissance nulle, la signature en anneau, adresse cachée, le chiffrement homomorphe, l'adresse furtive, la mise en gage, Le calcul multipartite sécurisé et l'environnement d'exécution de confiance. Ils ont aussi effectué une analyse comparative détaillée de ces dernières du côté technique et anonymat. Les auteurs ont conclu que les mécanismes du mixage centralisé et d'adresse cachée ont la plus faible confidentialité suivie du mixage décentralisé et signature en anneau, tandis que les quatre autres techniques ont une meilleure confidentialité et améliorant l'anonymat dans les blockchains.

Bien que chacun des travaux étudiés présente un mélange de différentes technologies pour atteindre la préservation de la vie privée tant recherchée, on pourrait essayer de les distinguer. la figure suivante résume cette classification à laquelle nous sommes parvenu à établir

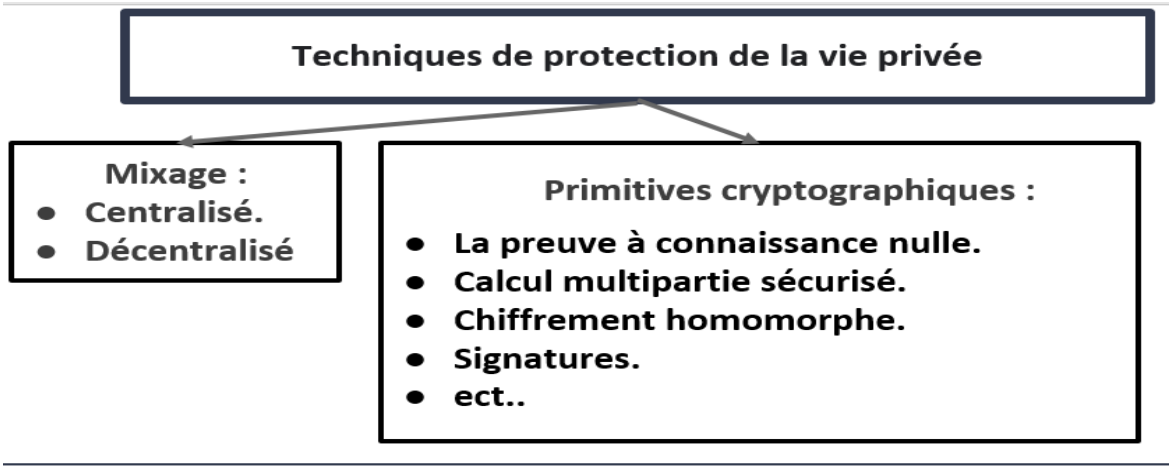

Figure 4 : Techniques de protection de la vie privée.

3.1 Solutions cryptographiques

3.1.1 Signatures

1. PriWatt

Inspiré et construit à partir du protocole Bitcoin, les auteurs dans [20] présentent un système P2P décentralisé privé basé sur des jetons nommé PriWatt. Le but de PriWatt est d'assurer la sécurité des transactions ainsi que la confidentialité des identités des utilisateurs dans les systèmes de réseau intelligent dans le domaine énergétique. Ce système se compose de contrats intelligents distribués assistés par la blockchain, de multi-signatures et de flux de messagerie cryptés anonymes. Suivant les accords écrits dans le contrat intelligent, PriWatt permet aux vendeurs et acheteurs d'enchérir et de négocier en toute sécurité les prix de l'énergie. Pour se faire de manière anonyme, la technique de flux de messagerie anonyme est utilisée. Le schéma multi-signature est déployé pour assurer la protection contre le vol, tandis que pour valider une transaction, un minimum M des N parties doivent signer la transaction pour pouvoir la terminer. La signature se fait grâce un algorithme de signature numérique à clé publique Elliptic Curve Digital Signature Algorithm (ECDSA). Dans le cas où il y aurait des problèmes lors d'une transaction, le Gestionnaire du Réseau de Distribution (GRD) se charge de résoudre le problème. De plus, pour le consensus, la PoW est utilisée pour éviter certaines attaques, entre autres, l'attaque à fautes byzantines et l'attaque à doubles dépenses. Au terme de ce travail, les auteurs estiment que la combinaison technologie blockchain, multi-signatures et flux de messagerie cryptée et anonymes dans une structure décentralisée présente une orientation beaucoup plus fiable et performante que les solutions centralisées traditionnelles.

2. La preuve à connaissance nulle

La recommandation du protocole Bitcoin était d'utiliser un Laudry service qui se traduit par un service de blanchisserie et qui consiste à échanger les utilisateurs, mais cela revient à avoir un tiers de confiance, ce qui est une altération du principe de la blockchain.

❖ Zerocoin

Dans Zerocoin [55], les auteurs ont étendu Bitcoin pour améliorer l'anonymat des utilisateurs et protéger leurs vies privées. Le principe de [55] est de casser les liens entre les transactions Bitcoin et de masquer l'origine de ces dernières, cela en remplaçant une pièce par une nouvelle qui a la valeur de la première plus les frais en bitcoins générés par cette opération. La pièce qui résulte doit avoir une valeur correspondante à une transaction et être correctement construite. Ce protocole s'appuie sur la zero-knowledge proof pour certifier que les pièces générées appartiennent à une liste de pièces valides.

❖ Zerocash

Zerocash [56], les auteurs critiquent les fonctionnalités de [60] en mettant en avant ses faiblesses et en se basant dessus pour apporter une amélioration et cela en s'appuyant essentiellement sur les avancés de la zero-knowledge proof et plus précisément la zk-SNARK. Il est considéré comme étant un système de paiement électronique décentralisé plus connu par DAP (Decentralized Anonymous Paiement) qui permet d'effectuer des paiements anonymes de n'importe quel montant. Tout comme [55], le principe de remplacement d'une par une nouvelle est adopté aussi, sauf que les valeurs ne sont pas fixes.

❖ Hawk

Hawk [57], Conçu en 2016 et s'appuyant sur le concept des smart contracts introduits par Ethereum, HAWK permet d'assurer la préservation de la vie privée qui manquait jusqu'à lors à la technologie blockchain, vue que dans la blockchain toute la séquence d'actions prise dans un smart contract y compris le flux d'argent est exposé à l'ensemble des nœuds.

Hawk est proposé aux utilisateurs même s'ils ne maîtrisent ni la programmation ni la cryptographie car c'est lui qui compile le programme en un protocole cryptographique en utilisant des primitives cryptographiques tel que zero-knowledge proof et secure multi-party computation SMPC.

Il est constitué de deux parties une partie privée notée Φ_{priv} qui prends en compte la contribution des parties du contrat et une autre publique notée Φ_{pub} qui ne touche ni à l'argent ni aux données privées.

Il garantit deux choses primordiales :

- On-chain privacy : la préservation de la confidentialité des transactions est garantie contre le public.
- Contractual security : qui assure la préservation de l'anonymat des membres d'un même contrat les uns des autres.

L'exécution des contrats HAWK est facilitée par une partie spéciale appelée manager, il peut connaître les entrées des utilisateurs et est digne de confiance pour ne pas divulguer les données privées des utilisateurs. Et en cas d'interruption du protocole par le manager, il peut être pénalisé financièrement et les parties du smart contract peuvent obtenir compensation.

3.2 Solutions de mixage

Ce mécanisme est couramment utilisé dans les blockchains, avec ses deux méthodes centralisées et décentralisées, il permet d'améliorer l'anonymat des transactions, l'objectif consiste à ajouter des informations de transit intermédiaires permettant de cacher le lien entre l'adresse d'entrée et l'adresse de sortie d'une transaction, assurant ainsi la confidentialité des transactions. De ce fait de nombreux travaux ont été effectués ; nous allons citer les plus importants et les plus récents :

3.2.1 Mixage centralisé (Centralized coin mixing)

Cette méthode consiste a utilisé un nœud intermédiaire (serveur) pour jouer le rôle d'une tierce de confiance et effectuer le mixage des fonds grâce un algorithme de mixage adéquat, l'objectif est de brouiller les adresses et le lien entre l'entrée et la sortie d'une transaction, les travaux importants qu'on peut citer sont :

- **Mixcoin**

MixCoin [22] est un protocole proposé pour faciliter les paiements anonymes en utilisant le système monétaire Bitcoin, il utilise un serveur central de mixage pour mixer

les adresses de transaction et offrir des services de mixage aux utilisateurs. Les liens entre les adresses d'entrées et de sorties sont alors masqués, ce qui rend l'analyse du contenu des transactions difficile pour un attaquant, le résultat étant une protection importante de la vie privée des utilisateurs. Pour améliorer l'anonymat, MixCoin oblige l' utilisateur à choisir le même montant à mixer simultanément et ils ne sont pas autorisés à choisir le nombre de transactions correspondantes, aussi, le serveur de mixage doit être assez honnête pour enregistrer les identités et les informations contenues dans les transactions, dans le cas contraire, il faut prévoir un mécanisme antivol.

- **BlindCoin**

L'idée du BlindCoin [23] est d'ajouter au MixCoin une signature aveugle (blind signature) et la propriété d'ajouter uniquement (append-only) associé à un journal d'accès qui surveille le serveur de mixage, c'est-à-dire que les données et les transactions manipulés par le serveur de mixage sont ajoutées et enregistrées sur le journal mais ne peuvent être ni écrasées ni supprimées, ce qui rend le serveur de mixage responsable et ses tentatives de vol détectables. Les signatures aveugles quant à elles, ont été développées pour signer des messages préalablement cryptés, l'objectif est donc de masquer le contenu des messages au signataire [24]. La signature aveugle dans BlindCoin permet de masquer la relation entre l'adresse de l'entrée et l'adresse de sortie d'une transaction au serveur de mixage lui-même. Cependant, il est encore impossible de prouver l'honnêteté du journal et devient une cible d'éventuelles attaques, ce qui affaiblit l'anonymat de BlindCoin.

- **Blind-Mixing**

les auteurs de [25] ont essayé d'améliorer protocole BlindCoin avec un algorithme de mixage à signatures aveugles basé sur une courbe elliptique qui empêche les serveurs de mixage de lier une adresse d'entrée à un adresse de sortie, Blind-Mixing offre une meilleure protection de l'anonymat que BlindCoin et une performance de vitesse de calcul globale des signatures aveugles très élevée.

- **LockMix**

LockMix [26] propose aussi une amélioration du protocole BlindCoin, en effet, c'est un protocole qui utilise un algorithme de signature aveugle pour cacher le lien entre

l'adresse d'entrée et l'adresse de sortie d'une transaction au serveur de mixage ainsi qu'un schéma multi-signature qui permet de lutter contre les vols de fond de la part du serveur de mixage pour assurer la protection des données dans les couches IP du réseau le protocole Tor[30] a été adapté. Le protocole LockMix fonctionne en deux phases : phase de dépôt de paiement et phase de mixage incluant des frais de mixage.

3.2.2 Mixage décentralisé (Decentralized coin mixing)

Le mixage décentralisé utilise des techniques qui ne nécessitent pas de tiers de confiance, éliminant ainsi le problème du point de défaillance unique. De plus, ils peuvent empêcher le vol et supprimer les frais de mixage dans la plupart des techniques proposées, nous allons citer quelques-unes :

- **CoinJoin**

CoinJoin [27] est le plus ancien des protocoles de mixage décentralisés, publié sur le forum bitcoin, CoinJoin fait recours à un serveur central à zéro frais. Dans le système CoinJoin, il est nécessaire que plusieurs utilisateurs du réseau établissent la décision d'utiliser cette méthode, puis chaque utilisateur, signe et envoie sa requête au serveur central individuellement et simultanément, lors de la réception de toutes les requêtes, le serveur se charge alors du changement des adresses d'entrées, effectue le mixage des fonds, rassemble les transactions et génère une transaction de type plusieurs à plusieurs, puis transfert les fonds vers les adresses de sorties correspondantes. De cette manière, les destinataires reçoivent leur fonds mais ne pourront jamais retrouver les adresses de sorties ayant effectuées le transfert des fonds, mais pas seulement, un tiers ne pourra jamais déterminer quel destinataire a reçu quelle sortie, car les fonds ne sont pas directement liés à une adresse elle-même, mais à une transaction à entrées multiples, toutes indépendantes. Il est à noter que pour un anonymat fort il faut avoir un nombre de participants important, sinon, retracer l'émetteur devient plus facile pour un attaquant.

- **CoinShuffle**

CoinShuffle [28] est considéré comme un protocole de mixage décentralisé complet, qui permet d'utiliser Bitcoin d'une manière anonyme, il est inspiré par les deux protocoles CoinJoin et Dissent, qui est le premier protocole de messagerie générale qui offre un anonymat prouvable avec responsabilité pour des groupes de taille moyenne et

gère les charges déséquilibrés ou peu de membres souhaitent transmettre des données dans un tour précis [29].

Dans le cas des blockchains, Dissent est utilisé pour que les nœuds d'un groupe réprimandent un nœud qui ne suit pas correctement un protocole donné, ce qui renforce l'anonymat et rend CoinShuffle plus robuste contre les attaques. Le schéma multi-signatures est utilisé pour chiffrer l'adresse de sortie de chaque transaction avec les clés publiques des autres membres du groupe, si les nœuds du groupe suspecte un nœuds d'être malhonnête, ils n'ont qu'a ne pas signer sa transaction et sera exclu du groupe, le protocole sera ré exécuté à nouveau. Le recours à un tiers de confiance est supprimé ce qui n'entraîne pas des frais de mixage.

Ce protocole a été amélioré en 2017 et a donné naissance à CoinShuffle++ [33] qui intègre DiceMix [33], pour effectuer des mixages en parallèle et non en séquentiel comme le fait CoinShuffle, une transaction de mixage avec 50 utilisateurs avec CoinShuffle++ peut être exécuté en huit secondes au lieu de trois minutes avec CoinShuffle, ce qui est une grande évolution dans les délais de mixage qui sont généralement très longs.

- **Xim**

Xim [31] est une approche proposée pour résister aux attaques connues contre le mixage notamment, les attaques Sybil, DOS et par inférence (analyse des données pour extraire des informations). Xim est un protocole biparti multi-tours, il inclut un système décentralisé anonyme de recherche de partenaire pour effectuer le mixage en utilisant FairExchange [32] qui est un protocole permettant à deux utilisateurs d'échanger des fonds en permutant leurs adresses de sorties. Il peut supporter jusqu'à quatre transactions en même temps contrairement à CoinJoin qui en supporte qu'une seule. Aucune partie externe ne peut confirmer ou trouver des preuves concernant les partenaires qui se jumellent. Les mineurs se chargent des demandes de partenariat en échange de frais payés par le demandeur et le répondeur. La transaction est alors validée et exécutée, si et seulement si, les deux partenaires se jumellent.

❖ ValueShuffle

ValueShuffle [34] est une extension de CoinShuffle++, il combine les protocoles CoinJoin, Confidential Transaction CT (transaction confidentielle) [35] et Stealth Adresses SA (adresses furtives) [36], ainsi, lors d'une transaction avec ValueShuffle l'anonymat du payeur, l'anonymat du bénéficiaire et la confidentialité du montant à transférer sont nettement améliorés par rapport aux autres protocoles. En effet, CT définit un format de transaction qui garantit la confidentialité de la valeur du paiement, SA permet au payeur de générer une adresse unique du destinataire ce qui renforce son anonymat car les autres utilisateurs du groupe ne peuvent pas la connaître, de plus, il ne nécessite aucune communication directe entre le payeur et le bénéficiaire, il fournit alors ; un anonymat solide au payeur aussi lors du mixage.

❖ Möbius

Möbius [37] a été le tout premier mixeur de pièces de monnaies sans confiance basé sur un contrat intelligent Ethereum. Les auteurs de Möbius ont fourni des définitions formelles de diverses notions de sécurité telles que l'anonymat, la prévention du vol et la disponibilité du mixeur. Ces propriétés pourraient être utilisées pour évaluer et comparer des propositions futures du point de vue de la sécurité c'est ce qui a été fait par MixEth que nous allons aborder juste après. Möbius utilise la signature en anneau et les adresses furtives, il est relativement résistant aux attaques DOS.

❖ Miximus

Miximus [38] est un mélangeur basé sur zk-SNARK pour Ethereum. Il utilise des zk-SNARK pour cacher la correspondance entre les émetteurs et les destinataires. Un émetteur crée une feuille dans un arbre de Merkle. L'émetteur doit échanger la pré-image de la feuille avec le destinataire. Plus tard, un destinataire pourrait prouver au contrat Miximus qu'il connaît l'une des pré-images d'une certaine feuille non divulguée, appelées annulateurs, elles permettent aux destinataires de retirer des fonds une et une seule fois. Cependant, Miximus ne fournit que l'anonymat contre les étrangers, car si A paie B via Maximus, A saura lorsque B a effectué la transaction de retrait. Une autre limitation plus sévère de Miximus est la configuration de confiance requise pour générer la clé de vérification pour le zkSNARK. Si cette configuration de confiance est

compromise, celui qui déploie le contrat et qui a généré la clé de preuve pourrait potentiellement voler des fonds au mixeur.

❖ MixEth

MixEth [39] est un protocole décentralisé multi-tours qui utilise les mélanges vérifiables de Neff [40] dans le contexte des mixages de pièces de monnaies Ethereum. Les utilisateurs de MixEth, mixent les clés publiques à tour de rôle en utilisant un multiplicateur secret qui n'est connu que par le mixeur, dans le but de rompre les liens entre les clés publiques de l'émetteur et du récepteur.

Ensuite, un tour de défi est imposé au mixeur pour générer une ZK-proof vérifiable publiquement pour convaincre les autres participants au mixage que le mélange a bien été effectué correctement, sans divulguer le multiplicateur secret. A chaque tour, les sorties mixées et quelques paramètres du protocole sont ensuite transférés au MixEth, permettant la vérification en ligne de l'exactitude du mélange ou encore le mixage par d'autres participants.

Ces derniers sont continuellement suggérés de vérifier la sortie du mélangeur et déclencher un mélange supplémentaire jusqu'à ce qu'un certain niveau d'anonymat soit établi. Le protocole nécessite trois transactions en chaîne et une transaction hors chaîne à échanger par le mixage d'un seul participant. La nature multi-tours du protocole et l'exigence de publication en chaîne de la sortie de mélange peuvent introduire des retards imprévisibles jusqu'à l'achèvement du protocole.

MixEth a été implémenté dans un canal d'état pour tirer partie de l'évolutivité et de l'instante finalité des solutions de mise à l'échelle hors chaîne, de plus, MixEth peut être utilisé dans n'importe quelle application à canal d'état pour mixer les fonds avant de revenir en chaîne. MixEth assure :

- L'anonymat : il est atteint si un adversaire ne peut pas déterminer qui est l'émetteur sincère qui a envoyé les fonds. Supposons qu'on ne peut pas distinguer les dépôts des émetteurs honnêtes, l'anonymat des récepteurs est assuré, si les transactions de retraits des dentinaires honnêtes sont indiscernables.

- La disponibilité : il est essentiel pour le mixeur d'assurer la disponibilité, ce qui signifie que des destinataires peuvent toujours retirer leurs fonds du mixeur, même si les émetteurs et tous les récepteurs sauf un, sont compromis. Un adversaire A gagne le jeu de la sécurité de disponibilité, s'il parvient à mettre le mixeur dans un état ou le bénéficiaire honnête ne peut pas retirer ses fonds.
- Prévention des vols : en assurant qu'aucune pièce ne peut être utilisée deux fois, ni retirée par qui que ce soit d'autre que le destinataire prévu.

3.2.3 Tableau comparatif des différentes techniques de protection de la vie privée

Le tableau suivant résume les différents protocoles étudiés dans ce chapitre, en effectuant une comparaison des techniques de protection de la vie privée dans les blockchains utilisées, les types de protection qu'ils assurent, le recours ou pas au tiers de confiance, engendrement de frais supplémentaire, les types d'attaques auxquelles ils résistent et la pénalité ou pas des comportements malveillants.

Protocole utilisés	Technologies utilisées	Type de protection	Tiers de confiance	Frais supplémentaires	Résistance aux attaques	Pénalité des comportements malveillants
Mixcoin	Mixage centralisé	Donnée	Oui	Oui	Résistant aux vols et aux attaques DOS et Sybil	Non
BlindCoin	Mixage centralisé	Identité	Oui	Oui	Résistant aux attaques DOS	Non
BlindMixing	Mixage centralisé	Identité	Oui	Oui	Anonymat élevé	Non
LockMixing	Mixage centralisé	Identité	Oui	Oui	Résistant aux vols et aux attaques DOS	Non
CoinJoin	Mixage décentralisé	Identité	Non	Non	Résistant aux vols	Non
CoinShuffle	Mixage décentralisé	Identité	Non	Non	Résistant aux vols	Oui
CoinShuffle++	Mixage décentralisé	Identité	Non	Non	Résistant aux vols et aux attaques DOS	Oui
ValueShuffle	Mixage décentralisé	Identité	Non	Non	Résistant aux vols et aux attaques DOS et anonymat élevé	Non
Xim	Mixage décentralisé	Identité	Oui	Oui	Résistant aux vols et aux attaques DOS et Sybil	Non
Möbius	Mixage décentralisé	Identité	Non	Non	Résistant aux vols et aux attaques DOS et anonyma	Non

					t élevé	
Hawk	Contrat intelligent/ SMPC/ Zero-knowledge SNARK	Identité et données	Oui	Oui	Résistant aux vols et aux attaques DOS	Oui
ZeroCoin	Zero-knowledge proof	Identité	Non	Oui	Résistant aux vols et aux attaques DOS et anonymat élevé	Non
ZeroCash	Zero-knowledge SNARK	Identité	Oui	Oui	Résistant aux vols et aux attaques DOS et Sybil	Non
Miximus	Zero-knowledge proof/ mixage décentralisé	Identité	Non	Non	Faible	Non
MixEth	mixage décentralisé / mélanges vérifiables	Identité et données	Non	Non	Résistant aux vols et aux attaques DOS et Sybil	Non

Tableau 1 : tableau comparatif des différents protocoles

Les services de mixage sont des méthodes relativement simples pour la protection de la vie privée dans la blockchain. La plupart sont compatibles avec les protocoles blockchain existants et nécessitent peu de ressources pour être mis en œuvre. La protection de la vie privée qu'ils proposent est acceptable et reste un domaine de recherche intéressant pour de futurs travaux notamment pour améliorer :

- Les délais d'attente : l'attente de l'utilisateur d'autres participants pour participer au mixage entraîne un délai d'attente élevé pour qu'une transaction soit validée.

- Serveurs de mixage malveillants : Bien que les serveurs de mixage

- Masque la relation entre les entrées et les sorties d'une transaction, cependant, le serveur lui-même peut être malhonnête et par conséquent, la confidentialité devient sujette aux violations.

- Frais de mixage : les services de mixage entraînent généralement des frais et peuvent être très coûteux.

Les services de mixage et les signatures en anneau peuvent assurer la confidentialité de l'identité de l'utilisateur mais ne garantissent pas la confidentialité des données de transaction. De même, les solutions cryptographiques visent à assurer la confidentialité des données de transaction mais n'assurent pas la confidentialité de l'identité de l'utilisateur. De plus, bien que les ZKP fournissent les deux types de confidentialité dans les blockchains, cela se fait au détriment des performances du système et des coûts élevés.

Ces technologies sont appliquées à diverses monnaies numériques et d'autres applications, telles que Zerocoin, Zerocash et Hawk. Une caractéristique commune les réunit, la décentralisation, qui évite l'attaque les nœuds tiers malveillants ainsi que l'analyse des transactions. Par conséquent, la protection de la vie privée dans la blockchain doit être améliorée, d'autant plus que beaucoup d'utilisateurs et de secteurs l'adaptent à leurs systèmes.

Conclusion

Nous avons fait un survol sur l'état de l'art qui consiste à présenter les différentes technologies utilisées pour la protection de la vie privée dans les blockhaus, nous avons aussi fait une étude comparative de ces dernières. Afin de montrer l'intérêt de notre travail, dans le quatrième chapitre, nous allons présenter notre approche proposée qui est basée sur le mixage et les signatures de groupe.

Chapitre IV

Contribution

Introduction

Dans le but de renforcer la protection de la vie privée dans les Blockchain, le mixage de pièces de monnaies peut être un moyen efficace surtout s'il est renforcé par d'autres moyens cryptographiques, tel que nous l'avons fait pour réaliser notre modèle.

En effet ce dernier est basé sur la création d'un groupe de mixage, d'une signature de groupe pour réaliser des opérations de mixage pour améliorer l'anonymat des utilisateurs et la confidentialité de leurs transactions.

4.1 Contribution

4.1.1 Environnement

- Un réseau Blockchain constitué de n nœuds.
- Un bulletin de bord (bulletin board).
- Un nœud voulant effectuer un mixage publie une demande de constitution de groupe de mixage sur le bulletin de bord.
- Notre étude se limitera au traitement d'une demande de création de groupe à la fois.

4.1.2 Idée générale

Nous proposons un modèle de mixage permettant à un nœud du réseau Blockchain, d'effectuer des mixages de pièces de monnaies avec d'autres nœuds du réseau en formant un groupe de mixage temporaire qui assurerait l'anonymat des membres et la confidentialité des transactions.

Notre modèle s'appuie sur :

- Une demande de mixage publiée sur un bulletin de bord.
- Un processus de création de groupe éphémère.
- La génération d'une transaction finale.
- La vérification de la validité de la transaction finale par les membres du groupe.
- L'exécution de la transaction finale.
- L'enregistrement de la transaction sur la Blockchain.

La figure suivante montre un schéma du fonctionnement du modèle.

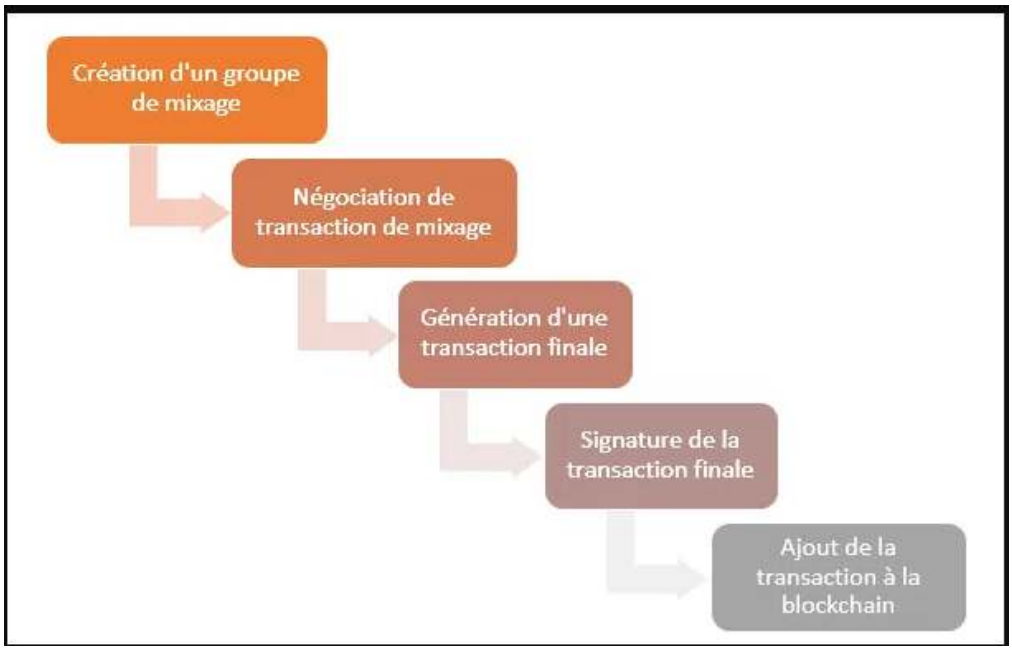

Figure 5 : Etapes de fonctionnement du modèle

4.1.3 Fonctionnement du modèle

Le fonctionnement de notre modèle est détaillé dans les étapes suivantes :

1. Création du groupe de mixage

- Un nœud A du réseau Blockchain publie une requête de création d'un groupe de mixage de pièces de monnaie, ReqGr, sur le bulletin de bord. Cette requête inclut les champs suivants :

- L'ancienne adresse des transactions du nœud A.
- Un nonce : Nonce.
- Un nombre minimal de membres du groupe : MembreMin, de type entier.
- Une demande de mixage.
- Une estampille$_A$ instantanée de l'horloge de A.
- Un délai maximal de création du groupe : Délais, de type minute.
- Un nombre de tours autorisé pour la création du groupe Tr de type entier.
- Une signature SIGN$_A$.

- La requête ReqGr est ensuite diffusée par le bulletin de bord dans le réseau.

- Les nœuds du réseau, $nœud_i$, désirants participer au groupe de mixage de pièces de monnaie, répondent à la requête ReqGr, par des requêtes de réponse ReqRep, contenant les champs suivants :

  - L'adresse des anciennes transactions du $nœud_I$.
  - Une $estampille_i$ instantanée de l'horloge du $nœud_I$.
  - Le Nonce de ReqGr.
  - Une demande de mixage.
  - Une signature $SIGN_I$.

- à la fin du Délais, le nœud A effectue les vérifications suivantes sur le nombre de participants m :

  - Si m ≥ MembreMin alors, le nombre de tour Tr est décrémenté et il continue vers l'étape 2.
  - Si m < MembreMin alors, Tr est décrémenté et vérifie, si Tr>0 alors il refait une tentative de création de groupe depuis l'étape 1, sinon, le groupe est dissous.

2. Négociation d'une transaction de mixage

- Le nœud A du groupe constitué dans l'étape précédente, génère des adresses de sorties : $AdresSort_{Ai}$ à qui il veut envoyer des montants : $montant_{Ai}$, puis choisit un nombre h aléatoirement, tel que : 1 ≤ h ≤ m, et h nœuds aléatoires du groupe pour leurs envoyer h sous-requêtes $ReqMix_{Ah}$, qui contiennent : $AdresSort_{Ai}$ et une division des montants $Montant_{Ai}$: $Montant_{Ah}$.

- A la réception d'une requête $ReqMix_{Ah}$ par un nœud j parmi les h nœuds choisis, il évalue s'il dispose d'assez de pièces de monnaies pour la satisfaire. Là on distingue trois cas :

  - Cas 1 : j ne dispose d'aucune pièce, alors il relaie la requête reçue à un autre nœud du groupe.
  - Cas 2 : le nœud j peut satisfaire la requête reçue, alors il répond par un message de satisfaction $MessageSat_j$ qui contient : l'ancienne adresse de transaction de j, $AdresSort_{Ah}$, $Montant_{Ah}$, puis le diffuse dans le groupe.
  - Cas 3 : le nœud j ne peut satisfaire qu'une partie de la requête, alors il répond par un message de satisfaction partielle $MessageSatPart_j$ qui contient : l'ancienne adresse de

transaction, $AdresSort_{Ah}$, $Montant_j$. Puis il génère une nouvelle requête $ReqMix'_{Ah}$ qui contient $AdresSort_{Ai}$ et $Montant'_{Ah}$ tel que :

$Montant'_{Ah} = Montant_{Ai} - Montant_j$, qu'il envoie à d'autres membres du groupe pour satisfaire le montant qui manque à la requête $ReqMix_{Ah}$.

- Tous les membres du groupe ayant répondu par un message de satisfaction ou de satisfaction partielle mettent à jour leurs montants.

3. Génération de la transaction finale

Chaque nœud du groupe, regroupe l'ensemble des messages reçus et vérifie si chaque adresse de sortie peut recevoir les montants adéquats c'est-à-dire : $AdresSort_{Ai}$ peut recevoir en moins $montant_{Ai}$. Si c'est le cas la transaction finale TransFinale qui contient : toutes les adresses d'entrée, toutes les adresses de sortie, la nouvelle division de pièces de monnaies et le hash de TransFinale, est générée et diffusée sur le groupe. Sinon, Tr est décrémenté et vérifie, si Tr>0 alors il refait une tentative de création de groupe depuis l'étape 1, sinon, le groupe est dissous.

La figure suivante montre le déroulement de cette étape.

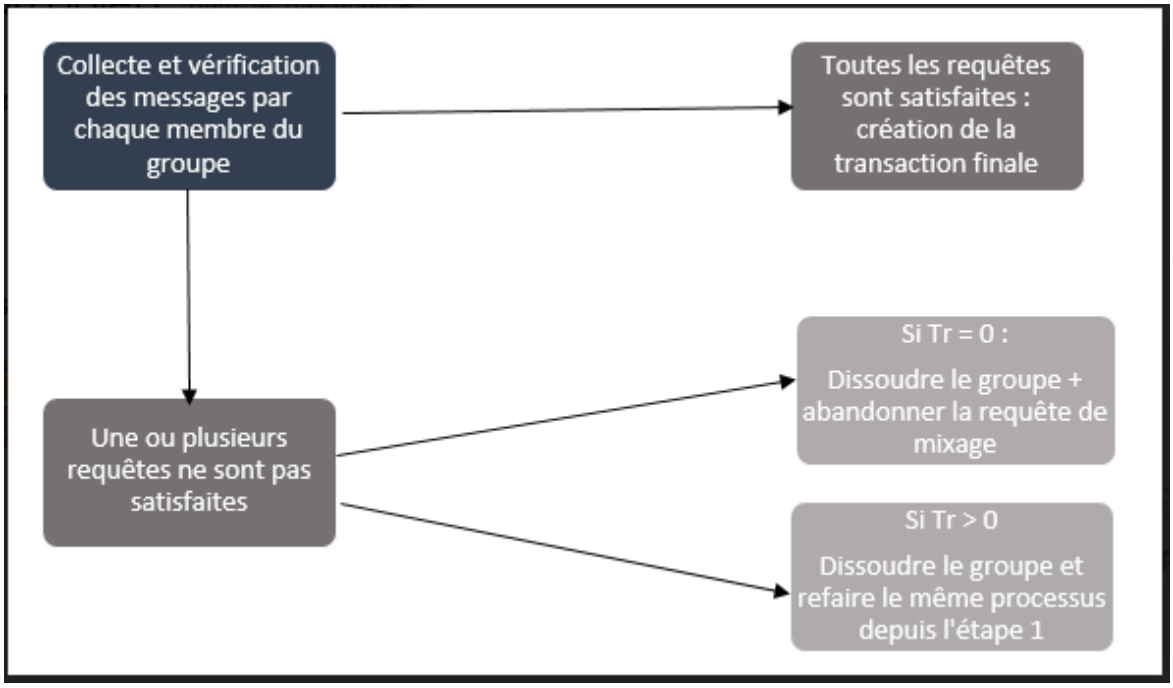

Figure 6 : Étape de génération de la transaction finale

4. Signature de la transaction finale

Chaque nœud du groupe signe TransFinale et diffuse le résultat dans le groupe, si elle est signée par tous les membres du groupe alors la transaction est valide et ajoutée à la Blockchain, sinon, la transaction est annulée et le groupe sera dissous.

4.1.4 Exemple illustratif

Supposons qu'un groupe de mixage soit créé par un nœud A désirant mixer des pièces de monnaie tel que : m=10,

Le nœud A génère trois adresses de sortie $AdresSort_{Ai}$: X, Y et Z, auxquelles il veut envoyer respectivement 1,2 et 3 pièces.

A choisi aléatoirement un nombre h tel que 1 ≤h ≤ 10, et h nœuds du groupe. Soit h=4, et 1,2, 3 et 4 des nœuds du groupe. A génère les requêtes suivantes : $ReqMix_{A1}$ (X,1), $ReqMix_{A2}$(Y,2), $ReqMix_{A3}$(Z,1) et $ReqMix_{A4}$(Z,2).

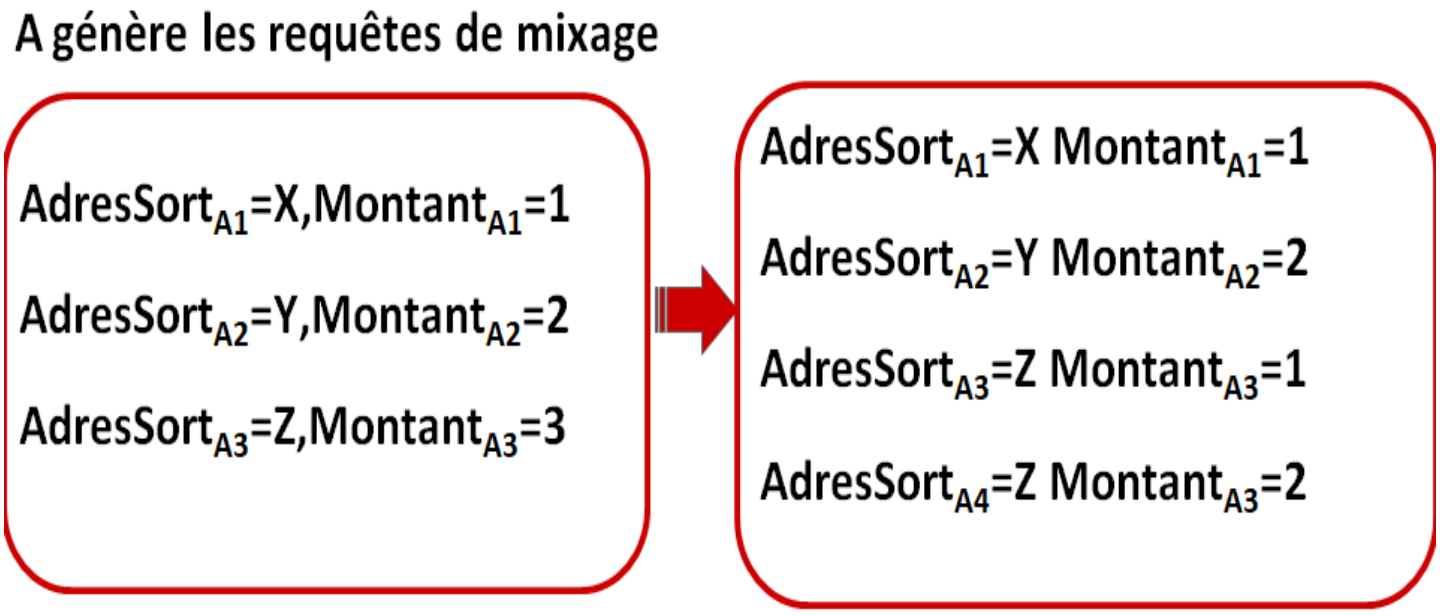

Figure 7 générations des requêtes.

Supposons que les nœuds 1, 2, 3, 4 répondent respectivement par les messages suivants :

$MessageSat_1$(hash(1),X,1),$MessageSat_2$(hash(2),Y,2), $MessageSatPart_3$(hash(3),Z,0.4) et $MessageSat_4$(hash(4),Z,2).

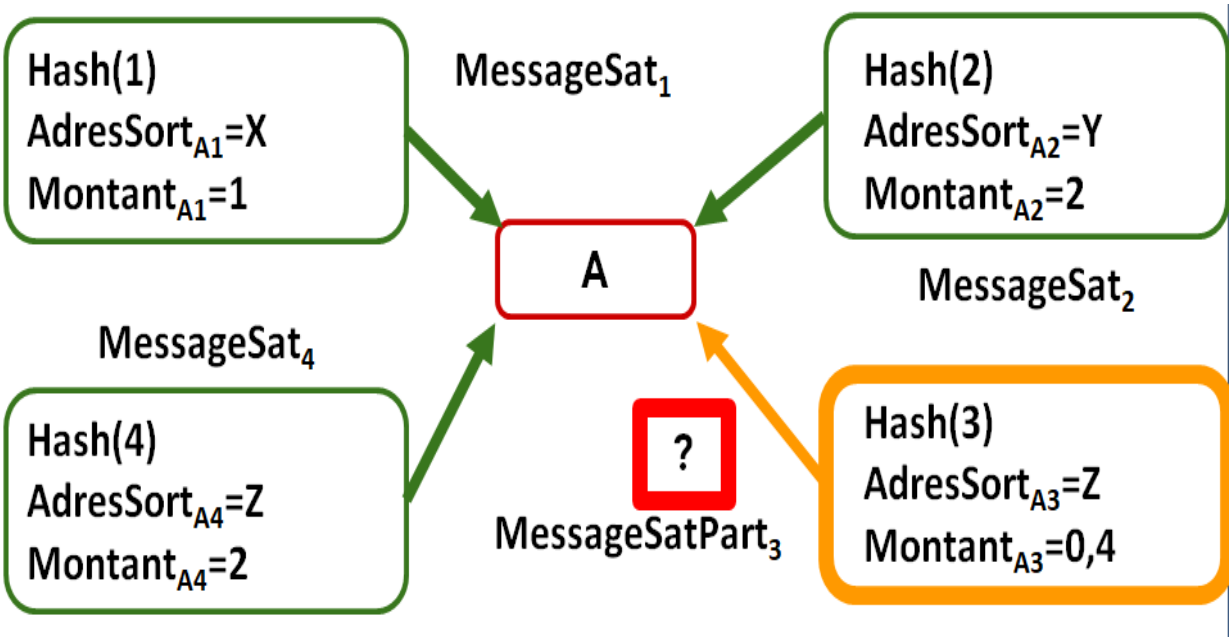

Figure 8 réponses des nœuds

Puisque le nœud 3 a répondu par un message de satisfaction partielle, alors il génère une autre requête ReqMix'$_{A3}$(Z,0.6) qu'il envoie à un autre nœud du groupe soit 5, il répond à son tour par un message, $MessageSat_G$(hash(5), Z, O.6) à Z.

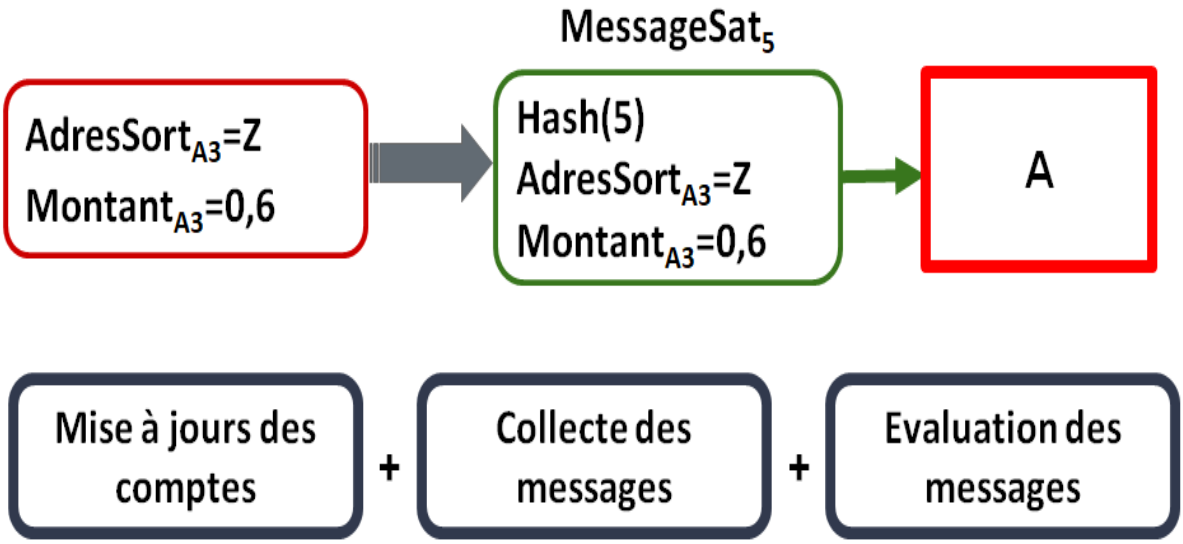

Figure 9 générations des sous-requêtes

Chacun des nœuds 1, 2, 3, 4 et 5, met à jour leurs montants, récolte l'ensemble des messages reçus et vérifie que les requêtes sont satisfaites, ce qui est le cas dans cet exemple car X, Y et Z peuvent recevoir les montants demandés par le nœud A.

Ce n'est qu'à ce moment qu'une transaction finale peut être générée et diffusée dans le groupe pour être signée par tous les membres du groupe. À la fin de cette étape, la transaction finale est validée et ajoutée par le nœud A dans la Blockchain.

4.1.5 Objectifs du modèle

Le fait que la transaction finale ne soit générée qu'après signature de tous les membres du groupe, notre proposition satisfait les critères suivants :

- Un schéma de mixage décentralisé sans tiers de confiance ni de serveur de mixage.
- Pas de frais de mixage.
- Anonymat des utilisateurs.
- Protection contre le vol.
- Protection du contenu de la transaction.

4.2 Comparaison avec quelques protocoles existants

Le tableau suivant compare notre modèle avec les deux protocoles MixCoin et CoinJoin :

Protocole	Protection de l'identité	Protection des transactions	Pas de tiers de confiance	Pas de frais de mixage	Protection contre les vols
MixCoin	✓	✓	×	×	×
CoinJoin	×	✓	×	✓	×
Notre modèle	✓	✓	✓	✓	✓

Tableau 2 : comparaison de notre modèle avec MixCoin et CoinJoin

4.3 Améliorations possibles de la proposition

- Limitation du nombre maximal de membres de groupe afin de réduire la complexité surtout pour des petites transactions.
- Choisir les membres du groupe selon des paramètres prédéfinis (niveau de confiance, fiabilité, etc.) par le demandeur de mixage.
- Définir un critère d'arrêt d'émission de requêtes pour éviter l'inondation du réseau dans le cas où le montant n'est jamais satisfait.
- Définir un critère pour le choix des montants à accepter en cas ou on le montant demandé est dépassé.
- Définir un système de pénalisation pour les membres qui ne signent pas la transaction finale.

Conclusion

Nous avons proposé un modèle de mixage avec une phase de création de groupe qui assure la protection de l'anonymat des utilisateurs et des transactions, cette phase

spécifique permet de contourner le besoin d'un tiers de confiance ainsi que des frais de mixage. Le modèle offre un vaste champ d'améliorations possibles dans des travaux futurs.

Conclusion Générale

L'objectif de notre travail consiste à la réalisation d'un modèle qui puisse parvenir à améliorer la protection de la vie privée dans les réseaux Blockchain.

Pour ce faire nous avons commencé par l'introduction du concept Blockchain , puis nous avons exposé les différentes technologies qui ont permis à la Blockchain de voir le jour et nous avons fini par donner des exemples de Blockchain.

Ensuite, nous avons introduit une définition générale de la vie privée et les techniques de protection de cette dernière. En effet, nous avons introduit beaucoup de généralités en faisant le lien avec les Blockchains.

Dans un second temps, nous avons réalisé l'étude de plusieurs travaux qui nous ont permis d'orienter nos recherches d'une part et d'avoir une idée sur la proposition de notre modèle.

L'élaboration d'un tableau récapitulatif de notre étude est considérée comme étant la synthèse de nos recherches.

Enfin, nous avons proposé un modèle de mixage de pièces de monnaies qui permet de protéger l'identité des utilisateurs ainsi que le contenu des transactions et cela grâce à l'utilisation d'un moyen qui permet de créer des groupes de mixage temporaires. Une étude pratique pourrait mettre la lumière sur ces faiblesses, ce qui nous permettrait d'apporter les ajustements nécessaires afin d'arriver au but ultime, qui est d'atteindre un fort anonymat dans les réseaux Blockchain.

Références

Références

[1]. https://academy.binance.com/fr/articles/history-of-blockchain , (consulté le 20 avril 2021)

[2]. Blockchain France, « La Blockchain décryptée Les clefs d'une révolution », Observatoire Netexplo, Mai 2016, disponible : http://www.netexplo.org/ .

[3]. P. MARLIER, « Sécurité du Peer-to-Peer », disponible : https://academy.binance.com/fr/articles/history-of-blockchaihttps://docplayer.fr/3422712-Labo-www-labo-asso-com-patrick-marlier-securite-du-peer-to-peer.html 2007, (consulté le 22 avril 2021).

[4]. R. AL KING, « localisation des sources des données et optimisation de requêtes réparties en environnement pair à pair », thèse de doctorat, université de Toulouse, France, 2010.

[5]. La rédaction TechTarget, disponible : https://whatis.techtarget.com/fr/definition/cryptographie-asymetrique-cryptographie-a-cle-publique , (consulté le 22 avril 2021).

[6]. S. TESSIER, « Fonctionnement de la blockchain et son intérêt pour le monde pharmaceutique », thèse de doctorat, université de Bordeaux, France, mai 2019.

[7]. Qu'est-ce qu'une fonction de hachage cryptographique ?, publié le 10 novembre 2015, disponible : https://www.ssl.com/ (consulté le 22 avril 2021).

[8]. I. SIDI AISSA, S. KEDDAR, *« Proposition d'un système à base de blockchain pour la gestion des opérations sur les véhicules au niveau national », diplôme de master, université de Tlemcène, Algérie, 2018.*

[9]. T. ROSSETTI, diplôme de bachelor, « Pertinence de l'utilisation des Blockchains dans l'industrie de la mode », Haute École de Gestion de Genève, Genève, le 26 novembre 2019.

[10]. LA ROUSSE , disponible : https://www.larousse.fr/dictionnaires/francais/consensus/1 (consulté le 21 /04/2021)

[11]. BINANCE ACADEMY, disponible : https://academy.binance.com/fr/articles/what-is-a-blockchain-consensus-algorithm (consulté le 22 avril 2021).

[12]. V. FAURE-MUNTIAN, M. CLAUDE DE GANAY, M. RONAN LE GLEUT, « les enjeux technologiques des blockchains (chaînes de blocs) », rapport, office parlementaire d'évaluation des choix scientifiques et technologiques, senat, france, le 20 juin 2018.

[13]. L. Le Loup, La révolution de la confiance, éditions EYROLLE, 2017.

[14]. SMILE, « Blockchain la révolution de l'économie de partage », disponible : https://www.leslivresblancs.fr/livre/informatique-et-logiciels/blockchain/blockchain-la-revolution-de-leconomie-du-partage, 2017.

[15]. M. PIGNEL, « LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale ? », www.pourlasolidarite.eu**,** juin 2019.

[16]. https://www.smartgrids-cre.fr/encyclopedie/la-blockchain-appliquee-a-lenergie/une-grande-variete-de-blockchain, (consulté le 25/04/2021).

[17]. A. O. AYADI, « Etat de l'art de la Blockchain dans : Analyse et étude de la sécurité des données médicales dans l'Internet des objets à partir d'une approche technologique Blockchain, mémoire de master Professionnel en Informatique, Réseaux et Systèmes Distribués, université Constantine 2, 2019.

[18]. Data flair **:** https://data-flair.training/blogs/types-of-blockchain/ (consulté le 26/04/2021) .

[19]. A. D. MOORE, ''privacy'', Library Hi Tech, ResearchGates, disponible: https://www.researchgate.net/publication/280292851_Privacy (consulté le 30/05/2021).

[20]. N. Z. AITZHAN et D. SVELTINOVIC, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, " IEEE Transactions on Dependable and Secure Computing, vol.15, no.5, pages 840–852, 2016.

[21]. Z. WANG, D.ZHAO, J. WANG, "A survey on privacy protection of Blockchain: The technology and application", IEEE Access 8, pages: 108766–108781, 2020.

[22]. J. BONNEAU, A. NARAYANAN, A. MILLER, J. CLARK, J. A. KROLL, and E.W. FELTEN, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes, " *Lecture Notes in Computer Science*, pages : 486–504, 2014.

[23]. L. VALANTA, B. ROWAN, "Blindcoin: blinded, accountable mixes for bitcoin," *International Conference on Financial Cryptography and Data Security.Springer*, Berlin, Heidelberg, pages: 112-126, 2015.

[24]. D. CHAUM, "Blind Signatures for Untraceable Payments, " *Advances in Cryptology Crypto'82*, springer, pages: 199-203, 1982.

[25]. Q. SHENTU, J. YU, "A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm", CoRR, 2015.

[26]. Z. BAO, W.SHI, S.KUMARI, Z.Y.KONG, C.M.CHEN, "Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity", International Journal of Information Security, pages: 1–11, 2019.

[27]. G. MAXWELL, "CoinJoin: bitcoin privacy for the real world", 2018, https://bitcointalk.org/index.php, (consulté le 08/08/2021).

[28]. T. RUFFING, P. MORENO-SANCHEZ, A. KATE, "CoinShuffle: practical decentralized coin mixing for Bitcoin," *European Symposium on Research in Computer Security*, Springer, pages: 345-364, 2014.

[29]. H. CORRIGAN-GIBBS, B .FORD, "Dissent: Accountable anonymous group messaging ", Proceedings of the 17th Conference on Computer and Communications Security CCS'10, USA, pages: 340–350, 2010.

[30]. P. SYVERSON, R.DINGLEDINE, N. MATHEWSON, "Tor: The second generation onion route", Researchgate, 2004,
disponible :https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router .

[31]. G. BISSIAS, A. P. OZISIK, B. N. LEVINE, and M. LIBERATORY, “Sybil resistant mixing for Bitcoin”, the *2015ACM Workshop on Privacy in the Electronic Society Scottsdale*, USA, New York: ACM Press, pages: 149-158, 2014.

[32]. S. BARBER, X. BOYEN, S.SHE, E .UZUN, “Bitter to better—how to make bitcoin a better currency“, International conference on financial cryptography and data security, Springer, Pages: 399–414, 2012.

[33]. T. RUFFING, P.MORENO-SANCHEZ, A.KATE, “P2P mixing and unlinkable bitcoin transactions“, NDSS, pages 1–15, 2017, disponible: https://eprint.iacr.org/2016/824.pdf .

[34]. T.RUFFING, M.S.PEDRO, “Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin“, 2017, disponible: https://eprint.iacr.org/2017/238 .

[35]. G. MAXWELL, “Confidential Transactions“, 2015, disponible: https://web.archive.org/web/20200502151159/https://people.xiph.org/~greg/confidential_values.txt, consulté le: (03/09/2021).

[36]. P. TODD, “[Bitcoin-development] Stealth addresses“, 2014, disponible: http://www.mailarchive.com/bitcoindevelopment@lists.sourceforge.net/msg03613.html, consulté le :(03 /09/2021).

[37]. S. MEIKLEJOHN, R.MERCER, “Möbius: Trustless tumbling for transaction privacy“, *Proceedings on Privacy Enhancing Technologies*, pages: 105–121, 2018.

[38]. B.WHITEHAT, “Miximus“, 2018, disponible: https://github.com/barryWhiteHat/miximus (consulté le 20/10/2021).

[39]. I.A.SERES, D.A.NAGY, P.BURCSI, C.BUCKLAND, "MixEth: efficient, trustless coin mixing service for Ethereum", Conférence (Tokenomics), 2019.

[40]. C.A. NEFF, "A verifiable secret shuffle and its application to e-voting", In *Proceedings of the 8thACM conference on Computer and Communications Security*, pages 116–125, 2001.

[41]. Ontario , ‘’Principes fondamentaux de la protection de la vie privée’’, 2019, https://www.ontario.ca/fr/document/manuel-sur-lacces-linformation-et-la-protection

de-la-vie-privee/chapitre-7-principes-fondamentaux-de-la-protection-de-la-vie-privee , (consulté le : 06/06/2021).

[42]. B. GERBER, ''OECD Privacy Principles'', 2010, disponible : **http://oecdprivacy.org/**, (consulté le 07/06/2021).

[43]. La Rédaction TechTarget, ''Gestion des identités '', 2014, disponible : https://www.lemagit.fr/definition/Gestion-des-identites , (consulté le 24 /05/2021) .

[44]. A. BELABED, ''La protection de la vie privée sur Internet'', thèse de doctorat, université de TLEMCEN, 2018.

[45]. S.GAMBS, ''Réseaux de communication anonyme'', 2015, disponible : https://www.irisa.fr/prive/sgambs/cours2_pvp.pdf , (consulté le : 22/05/2021).

[46]. S.GAMBS, '' Accreditations anonymes'', 2015, disponible : https://www.irisa.fr/prive/sgambs/cours6 pvp.pdf , (consulté le : 23/05/2021).

[47]. G. PILLOT, '' Anonymat et vie privée sur internet'', Mémoire de master, université LAVAL, 2018, disponible : https://corpus.ulaval.ca/jspui/retrieve/b80b8e47-882b-402b9ebb-e21440e1e0bd , (consulté : 21/05/2021).

[48]. A. BELKHAMSA, M. YAHIAOUI, '' La protection de la vie privée dans le BigData", Mémoire de master, Université de BOUIRA, 2020.

[49]. R. L. RIVEST, A. SHAMIR, Y. TAUMAN, ``How to Leak a Secret, '' in *Proc.ASICRYPT*. New York, NY, USA: Springer-Verlag, 2001, pages: 552_565.

[50]. ZHAO, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Li, H.; Tan, Y.A. Secure Multi-Party Computation: Theory, practice and applications. Inf. Sci. **2019**, 476, pages: 357–372.

[51]. X. YAN, Q. WU, Y. SUN, "Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing", 2020, 8832341, disponible : https://www.hindawi.com/journals/wcmc/2020/8832341 ,/

[52]. A. Z. JUNEJO, M. A. HASHMANI, and M. MEMON Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges.

[53]. R. SOLOMON, G. ALMASHAQBEH," smartFHE : Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption : https://eprint.iacr.org /2021/133 , (consulté le 25/09/ 2021).

[55]. I. MIERS, C. GARMAN, M. GREEN, A. D. RUBIN, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin", 2013 IEEE Symposium on Security and Privacy.

[56]. E. BEN-SASSON, A. CHIESA, C. GARMAN, M. GREEN, I. MIERS, E. TROMER, M. VIRZA. Zerocash: Decentralized anonymous payments from Bitcoin. In S&P, 2014.

[57]. A. KOSBA, A. MILLER, E. SHI, Z. WEN, and C. PAPAMANTHOU "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts"

[58]. R. SOLOMON and G. ALMASHAQBEH," smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption", disponible: https://eprint.iacr.org/2021/133 (consulté le 25/09/2021).

Résumé

En tant que nouvelle technologie distribuée point à point (P2P), la blockchain est devenue un domaine de recherche très vaste, relevant divers défis notamment la protection de la vie privée comme c'est le cas dans toutes les autres technologies. Dans ce mémoire nous allons commencer par définir quelques généralités sur les blockchains ainsi que les principes de son fonctionnement pour pouvoir faire une étude des solutions existantes aux problèmes liés à la vie privée d'une manière générale et dans les blockchains en particulier, en effet, l'anonymat des utilisateurs et la confidentialité des transactions sont les deux principaux défis à relever. Les mécanismes de mixage et les solutions cryptographiques répondent à cette problématique mais restent sujets à des attaques et souffrent de lacunes. Compte tenu de ces imperfections et de la synthèse de notre étude nous présentons un modèle de mixage sans tiers de confiance, basé sur des signatures de groupe permettant de renforcer l'anonymat des utilisateurs, la confidentialité des transactions sans frais de mixage en un délai d'exécution minimale. Théoriquement, notre modèle répond aux attentes de protection de la vie privée, cependant sa validation formelle est un de nos futurs objectifs.

Mots clés : Blockchain, anonymat, vie privée, mixage.

Abstract

As a new distributed point-to-point (P2P) technology, blockchain has become a very broad field of research, addressing various challenges including privacy preserving as is the case in all other technologies. In this work, we will start by defining some generalities in blockchains as well as the principles of its operation in order to be able to make a study of the existing solutions to the problems related to private life in general and in blockchains in particular, indeed, User anonymity and transaction confidentiality are the two main challenges for the protection of privacy in blockchains. Mixing mechanisms and cryptographic solutions respond to this problem but remain subject to attacks and suffer from shortcomings. Taking into account these imperfections and the summary of our study, we present a mixing model without trusted third parties, based on group signatures allowing to reinforce the anonymity of the users, the confidentiality of the transactions and without mixing costs with minimal turnaround time. Theoretically, our model meets the expectations of privacy preserving , formal validation will be one of our future goals.

Key words : Blockchain, anonymity, privacy, mixing.