République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Systèmes d'information

Etude de sécurité du Bitcoin
Cas d'étude : gestion de vote

Thème
Présenté Par :

Hadj Amira

Devant le jury :

Mr. T.Mekhazniya	*MCA*	*Univérsité Larbi Tébessi*	*Président*
Mr . S.Tag	*MAA*	*Univérsité Larbi Tébessi*	*Examinateur*
Mr . H.Bendjenna	*Pr*	*Univérsité Larbi Tébessi*	*Encadreur*

Date de soutenance : 14 /09/ 2020


بسم الله الرحمن الرحيم

Remercîments

Nous exprimons notre profonde gratitude à toute personne qui, de près ou de loin, a contribué à la réalisation de ce travail.

Nos remerciements s'adressent plus particulièrement à Mr Hakim Bendjenna qui a bien accepté de diriger ce mémoire. Ses remarques, ses précieux conseils et ses corrections nous ont été d'une grande utilité. Nous lui disons « Merci ».

Nous remercions également les membres de jury d'avoir accepté l'évaluation de ce modeste travail.

Nous aimerions témoigner notre gratitude aux professeurs et enseignants du département des Mathématiques et Informatiques qui ont assuré notre formation universitaire pour les conseils prodigués depuis la première année.

Dédicace

A toute la famille Hadj , Mes parents et Mes amis ...

Hadj Amira

Résumé

Le Bitcoin est une monnaie numérique décentralisée sans banque centrale, qui peut être envoyée d'un utilisateur à un autre via un réseau peer-to-peer sans avoir besoin d'intermédiaires. Les transactions sont vérifiées par des nœuds de réseau via le cryptage et enregistrées dans un registre public distribué appelé blockchain.

La technologie Blockchain est populaire en raison de ses caractéristiques qui coïncident avec l'idéal actuellement requis, et aussi de l'algorithme de preuve de travail (POW).

Dans ce mémoire, nous présentons une étude sur la sécurité du Bitcoin. Dans ce but, nous avons utilisé la blockchain dans un système de vote. Les résultats indiquent que la technologie a donné plus de sécurité au vote électronique, en raison des caractéristiques de transparence et de sécurité.

Mots clés : Bitcoin, Blockchain, POW, Vote électronique, Sécurité, Transparence

Abstract

Bitcoin is a decentralized digital currency without a central bank, which can be sent from one user to another via a peer-to-peer network without the need for intermediaries. Transactions are verified by network nodes through encryption and recorded in a distributed public ledger called a blockchain.

Blockchain technology is popular because of its characteristics which coincide with the currently required ideal, and also the proof of work (POW) algorithm

In this project we present a study on the security of Bitcoin. For this purpose, we used the blockchain in a voting system. The results indicate that technology has given more weight to electronic voting, due to the characteristics of transparency and security.

Keywords: Bitcoin, Blockchain, POW, Electronic voting, Security, Transparency

الملخص

البتكوين هي عملة رقمية لامركزية بدون بنك مركزي، والتي يمكن إرسالها من مستخدم إلى آخر عبر شبكة نظير إلى نظير دون الحاجة إلى وسطاء. يتم التحقق من المعاملات عن طريق عقد الشبكة من خلال التشفير وتسجيلها في دفتر أستاذ عام موزع يسمى البلوكتشين.

تحظى تقنية البلوكتشين بشعبية كبيرة بسبب خصائصها التي تتوافق مع النموذج المثالي المطلوب حاليًا، وكذلك بسبب خوارزمية إثبات العمل

في هذا الموجز، نقدم دراسة حول أمان البتكوين لهذا الغرض، استخدمنا تقنية البلوكتشين في نظام التصويت. وتشير النتائج إلى أن التكنولوجيا أعطت وزناً أكبر للتصويت الإلكتروني، نظراً لخصائص الشفافية والأمن.

الكلمات الرئيسية :البتكوين ، البلوكتشين ، خوارزمية إثبات العمل ، التصويت الإلكتروني ، الأمان ، الشفافية

Table des matières

Table des figures

Table des tableaux

INTRODUCTION GÉNÉRALE

1 Contexte et problématique

Le buzz word technologique de l'année 2017 sera sans doute « blockchain », il succède ainsi à ses illustres ancêtres « Webinar », « Web 2.0 », « Big Data », « Data mining », « Cloud », etc. Depuis son invention en 2008, la Blockchain a su démontrer sa solidité en permettant à la monnaie électronique tel que le Bitcoin de fonctionner avec des enjeux financiers de plus en plus élevés. En effet, Le concept de blockchain ou chaîne de blocs a été conçu pour créer une crypto-monnaie sans tiers de confiance. Cette nouvelle technologie est fondée sur un réseau pair-à-pair dont les membres détiennent un exemplaire de la même chaîne de blocs et la mettent à jour en effectuant des calculs sophistiqués.

Par ailleurs, les élections dans le monde sont confrontées à des menaces croissantes pour la sécurité et à des préoccupations concernant l'intégrité des élections. Le vote par bulletin papier reste la forme de vote la plus courante dans le monde. C'est le moins sensible aux cyber attaques mais très sensible aux erreurs humaines et à la fraude. Alors que de nombreux pays passent aux machines à voter électroniques, ils sont vulnérables aux cyberattaques en raison d'une technologie obsolète, mal conçue ou mise en œuvre. Dans certains cas, les pays qui avaient introduit le vote électronique sont revenus au vote papier en raison de problèmes de sécurité**.**

Afin d'étudier la sécurité du Bitcoin, nous avons proposé d'appliquer la technologie derrière le Bitcoin « qui est la Blockchain » à un domaine sensible à la sécurité qui est le vote électronique.

Dans les délits liés aux élections, le rassemblement des voix est souvent exploité par une seule agence centrale ; Où les votes sont falsifiés illégalement ; Ou l'annonce de résultats

Erronés en raison d'erreurs commises dans le processus de comptage manuel.

Le système de vote électronique est devenu une méthode efficace à l'heure actuelle, qui se caractérise par des données distribuées, un vote en temps réel et nécessite également une sécurité élevée.

Avec l'augmentation du piratage et des préoccupations concernant la sécurité et la confidentialité sur Internet, il n'est pas possible de garantir que le vote électronique ne peut pas être truqué uniquement par cryptage.

Le processus de création d'un système de vote électronique plus sûr et plus transparent est devenu un sujet commun en informatique et en sécurité de l'information. Afin d'étudier et d'analyser la sécurité de la technologie de la blockchain, nous présentons une étude basée sur l'exploitation des propriétés de la blockchain pour construire un nouveau système de vote électronique.

Ainsi, l'objectif principal de ce projet de PFE est de répondre à la question suivante :

La technologie derrière Bitcoin est-elle la révolution de la sécurité et de la transparence nécessaire pour permettre le vote électronique ?

Nous travaillons au long de ce projet pour répondre à cette question à travers une proposition d'une architecture qui explique notre contribution, ainsi que le développement de cette contribution vers une application concrète.

LA TECHNOLOGIE BLOCKCHAIN & LE BITCOIN

1.1 Introduction

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

La réputation de la Blockchain ou chaines de blocs grandit de jour en jour et attire de plus en plus d'attention à l'échelle mondiale. Certaines personnes comparent blockchain au début d'Internet dans les années 1970 et certains l'appellent la révolution du web 2.0, et il est parlé par de nombreuses personnes dans différentes disciplines : économistes, programmeurs et autres.

Dans ce chapitre nous allons introduire les principes et les concepts de base de la technologie Blockchain. Dans une première partie, nous allons définir technologie blockchain, son architecture, ses mécanismes et enfin les applications de la technologie aux différentes échelles, la deuxième section présente le protocole Bitcoin.

1.2 Historique

L'architecture derrière la technologie de la Blockchain a été décrite dès 1991 quand les chercheurs Stuart Haber et W. Scott Stornetta ont introduit une solution informatique, permettant l'horodatage des documents numériques et donc que ceux-ci ne soient jamais antidatés ou altérés.

Leur système utilisait une Blockchain sécurisée cryptographique pour stocker des documents horodatés. Par la suite, en 1992, le protocole dit « arbre de Merkle » fut introduit au fonctionnement, rendant ainsi le système plus efficace en permettant à plusieurs documents d'être rassemblés en un seul bloc. Cependant, cette technologie tomba dans l'oubli, et le brevet expire en 2004, quatre ans avant la création du Bitcoin.

En 2004, l'informaticien et activiste cryptographique Hal Finney, lance un système appelé RPoW (« Reusable Proof Of Work » pour résolu le problème de la double dépense en conservant une registre de la propriété des jetons. Le système fonctionnait en recevant un jeton preuve du travail non échangeable et non fongible basé sur le système HashCash, celui-ci créait en retour un jeton possédant une signature RSA qui pouvait ensuite être transféré de personne en personne.

Fin 2008, un livre blanc (white paper) introduit un système de paiement électronique décentralisé de pair à pair (peer-to-peer), appelé Bitcoin. Le white paper fut distribué par le biais d'une liste de diffusion e-mail en rapport avec la cryptographie, par une personne ou un groupe de personnes utilisant le pseudonyme de Satoshi Nakamoto.

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 peer-to-peer décentralisé afin de suivre et de vérifier les transactions. En bref, 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.

En 2013, Vitalik Buterin, un programmeur et co-fondateur du Bitcoin Magazine déclara que le Bitcoin avait besoin d'un langage de script pour construire des applications décentralisées. N'arrivant pas à réussir à trouver un accord au sein de la communauté, Vitalik 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 en français).

1.3 Le réseau distribué

La technologie Blockchain repose sur un système de réseau distribué. C'est en cela que réside toute son innovation. Il existe 3 principaux types de réseaux possibles : **Centralisé, décentralisé et distribué.** [9]

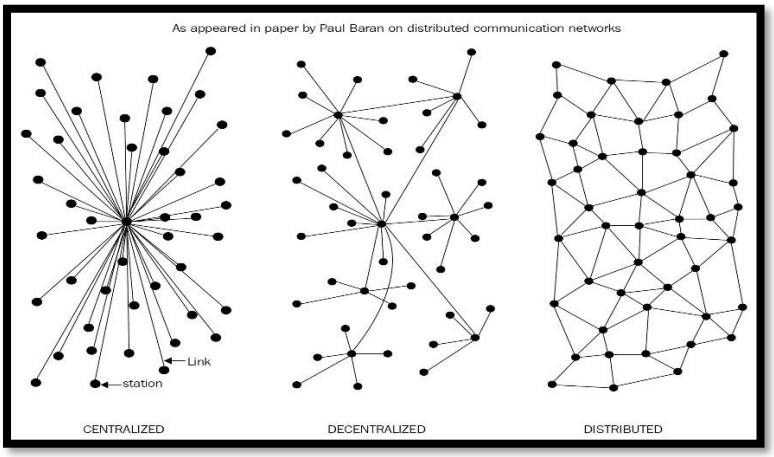


Figure 1.1 **:** différents types de réseaux (Bashir, 2017)

1.4 La chaine des blocs

Une Blockchain est une technologie informatique « open source », de stockage et de transmission de Données numérique fondée sur des échanges P2P, d'une manière chronologique, horizontal, transparente, décentralisée, sans intermédiaire (Casino et al., 2018) et sécurisée grâce aux algorithmes de consensus. Par extension, elle constitue une base de données publique qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création (Casino et al., 2018) décentralisée fiable, inviolable et sans organe central de contrôle , et est organisée en des sous-registres connus sous le nom de "bloc".

Elle peut être assimilée à un grand livre distribue (DLT) de comptes anonymes, Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer "un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible".

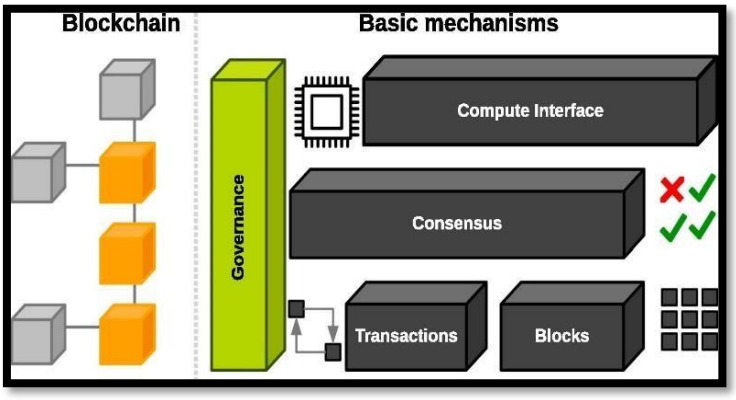


Figure 1.2 : Une chaine de blocs *(*Casino et al., 2018*)*

1.5 Les problèmes adressés

La blockchain constitue en elle-même une innovation car elle permet la résolution de deux problèmes : le problème de la double dépense et le problème des généraux byzantins (Lamport et al. 1982).

1.6 Architecture de blockchain

Les transactions sont regroupées dans des blocs de la façon suivant :

- Les blocs sont ajoutés un par un, à intervalle régulier et liés au bloc précédent.
- Le chaînage se fait en incorporant dans le bloc en cours le hash du bloc précédent.
- La modification d'un seul bloc détruirait l'intégrité de toute la chaîne.

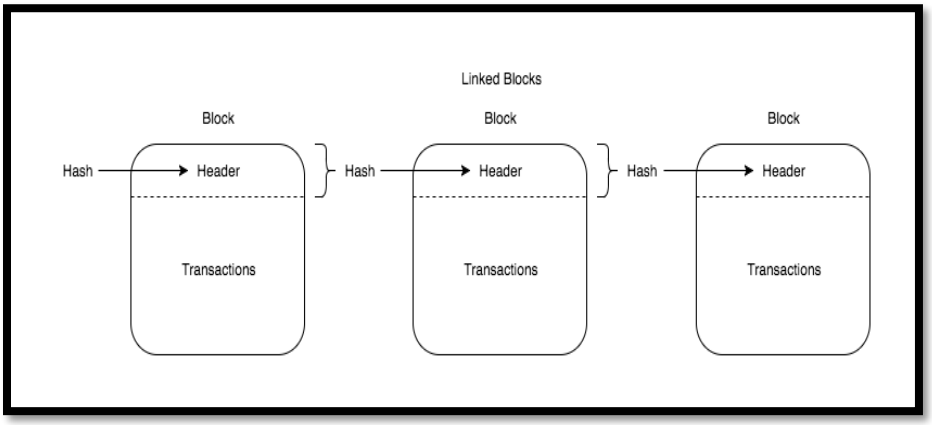


FIGURE 1.3 Structure du blokchain (Zheng et al., 2017)

1.7 Caractéristiques de blockchain

Selon (Casino et al., 2018), la blockchain présente les caractéristiques clés suivantes :

1.7.1 **Décentralisation :** Il n'existe pas de tiers de confiance. Deux personnes peuvent réaliser une transaction en comptant sur le système lui-même pour confirmer l'échange. De plus, le réseau entier a accès à la base de données et aux opérations qui y sont effectuées.

1.7.2 **Transparence :** Bien que les participants intervient sous des pseudonymes, mais leur transactions sont traçable. L'historique des transactions est consultable à tout moment par toutes les membres de réseaux, rendre le système transparent.

1.7.3 **Sécurisation :** La Blockchain est conçue pour stocker les données de manière **immuable et inviolable**. La nature décentralisée de la blockchain et les algorithmes de cryptage rend trop difficile de tirer parti du système par des personnes mal intentionnées utilisateurs.

1.7.4 **Immutabilité :** Étant donné que chacune des transactions réparties sur le réseau doit être confirmée et enregistrée sous forme de blocs répartis dans tout le réseau, il est presque impossible de falsifier. De plus, chaque bloc diffusé serait validé par d'autres nœuds et les transactions seraient vérifiées. Ainsi, toute falsification pourrait être facilement détectée.

1.7.5 **Authenticité :** Chaque transfert d'objet, d'actif, de document, de propriété, de contrat est authentique étant donné que la blockchain l'enregistre dans la base de données. De plus, il est possible d'ajouter à chaque transfert l'heure, le jour, l'année et le propriétaire.

1.7.6 **Automatisé** : Les règles préétablies par les membres de la blockchain sont effectuées par des programmes informatiques. Des « contrats intelligents » seront auto-exécutants

1.8 Les catégories de blockchain

1.7.1. Blockchain publique

C'est le modèle le plus connu*) (historique)*, est un registre ouvert accessibles à n'importe qui dans le monde, aucune permission d'autorisation ni d'être authentifiés demander pour effectuer des transactions ou de participer au processus de consensus.

1.7.2. Blockchain privée

Il y a les blockchains totalement fermé (*permissioned*), 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 privée. D'une façon générale les nœuds du réseau sont authentifiés et autorisés selon des critères prédéfinis.

1.7.3. Blockchain de consortium

Est une combinaison hybride de blockchains publics et privés Bien qu'elle partage le même niveau d'évolutivité et de protection de la confidentialité avec la chaîne de blocs privée, leur différence principale réside dans le fait qu'un ensemble de nœuds, nommés nœuds leaders, est sélectionné à la place d'une seule entité pour vérifier les processus de transaction. Cela permet une conception partiellement décentralisée où les nœuds leaders peuvent accorder des autorisations à d'autres utilisateurs. (Casino et al., 2018)

Propriétés	**Blockchain Public**	**Blockchain hybride**	**Blockchain prive**
détermination du consensus	Tous les mineurs	Ensemble de nœuds	Une organisation
autorisation de lecture	Publique	Public ou restreint	Public ou restreint
immutabilité	Impossible de falsifier	pourrait être altéré	Pourrait être altéré
Efficacité	Faible	Haute	Haute
centralisé	Non	Partielle	Oui
processus de consensus	Sans permission	Autorisée	Autorisée

Tableau 1.1 : classification de blockchain (Casino et al., 2018)

1.9 Le fonctionnement de blockchain

Tout d'abord, il s'agit de bien mettre en contexte les composantes les plus importantes de la blockchain :

1) Le nœud

Un nœud est un ordinateur qui est relié au réseau blockchain. Chaque nœud représente donc un utilisateur. Celui-ci conserve à tout moment une copie du registre blockchain et peut être réparti partout dans le monde.

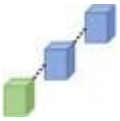
2) Le réseau P2P

La blockchain repose sur un réseau pair-à-pair composé d'un ensemble de nœuds qui sont interconnectés entre eux. Ce réseau ne possède aucune autorité centrale et est donc entièrement décentralisé. L'entièreté de ce réseau a accès au registre blockchain.

3) Le bloc

Un bloc enregistre les transactions récentes émises par le réseau. Une fois rempli, un nouveau bloc est créé pour enregistrer les nouvelles transactions et le bloc rempli va se faire valider par le réseau.

4) Le registre blockchain



Le registre est la chaîne de blocs (qui contiennent toutes les transactions) qui est partagée à l'ensemble des utilisateurs du réseau. En d'autres mots, le registre est une base de données qui classe toutes les transactions de manière chronologique et qui est accessible par tous les membres du réseau.

Chaque nouvelle transaction et/ou Smart Contract, « en attente », sont groupés dans un nouveau bloc. Pour que ce bloc puisse être ajouté à la Blockchain, il faut qu'il soit validé par certains nœuds spécifiques du réseau appelés « mineurs », Leur rôle consiste à répondre à un casse-tête crypto mathématique complexe. Chaque réponse trouvée est propre à un et à un seul bloc interdisant ainsi, sa réutilisation pour la validation d'un nouveau bloc.

Le problème mathématique, propre à chaque bloc, est très difficile à résoudre (demande d'importantes ressources de calcul). Pour encourager les mineurs, essentiels au bon fonctionnement et à la viabilité du réseau, une rémunération leur est attribuée en récompense de leur travail.

La complexité du problème de validation est liée à une difficulté associée au bloc. Afin de maintenir constant, le temps de production d'un bloc, le niveau de difficulté est automatiquement ajusté par le réseau.

Extrêmement difficile à calculer, la validation de la solution est, à l'inverse, très facile. Il existe plusieurs solutions valides pour un bloc donné. Il suffit d'en trouver au moins une pour que le bloc soit validé au travers du processus de consensus.

Une fois que le bloc est validé par un « miner » et approuvé par les autres nœuds du réseau, il est horodaté et ajouté, en tête de la chaîne de blocs et tous les nœuds du réseau l'ajoutent dans leurs copies de la chaine.

La figure ci-dessous illustre les différentes étapes par lesquelles passe la technologie et qui permettent à un utilisateur A d'effectuer une transaction vers un utilisateur B: (Hannesse et al.)

.

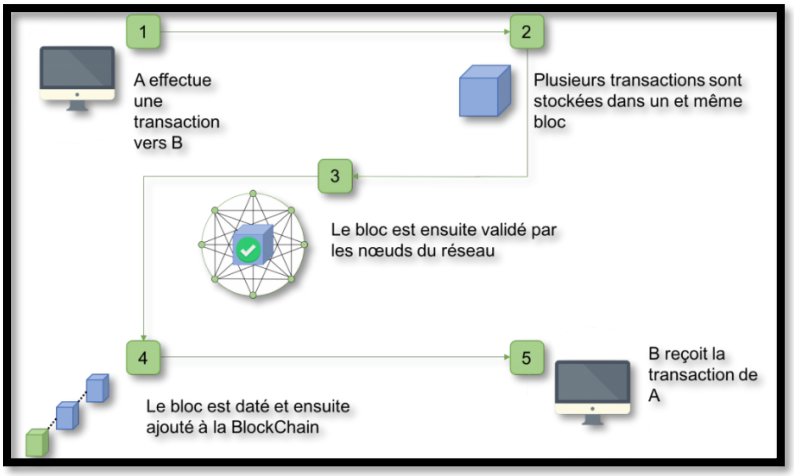


Figure 1.4 : Fonctionnement général de la blockchain

1.10 Les méthodes de consensus

Un consensus se définit par l'accord généralisé et unanime entre des personnes pour décider de la marche à suivre. Pour la technologie blockchain, il s'agit d'un consensus informatique où les utilisateurs se mettent d'accord sur un processus pour valider des transactions et mettre à jour la base de données (Leloup, 2017). Ce consensus a lieu à chaque fois qu'un bloc est ajouté au reste de la chaîne. Le cas échéant, le bloc ne pourra plus être retiré de la chaîne et l'entièreté du réseau aura accès aux informations contenues dans celui-ci (Wright & De Filippi, 2015).

1.9.1. La preuve de travail

C'est un protocole dont le but principal est de prévenir les cyber-attaques, tel qu'une attaque par déni de service distribué (DDoS), qui a pour objectif d'épuiser les ressources d'un système informatique en envoyant plusieurs fausses demandes.

Dans ce mécanisme de consensus, certains utilisateurs de la blockchain, appelés mineurs, mettent à contribution leur puissance de calcul informatique dans le but de "vérifier, enregistrer et sécuriser les transactions dans la blockchain" (Leloup, 2017).

Pour chaque transaction, des milliers de mineurs effectuent des calculs mathématiques (algorithme de hachage), mais à la fin il n'y a qu'un seul d'entre eux qui trouve la solution. La probabilité de trouver cette solution augmente proportionnellement avec la puissance de calcul informatique CPU. Par exemple, un utilisateur A ayant un CPU élevé a plus de chance qu'un utilisateur B avec un CPU faible. Le mineur qui trouve la solution se voit ensuite récompensé par une certaine somme de cryptomonnaie. La preuve de travail fonctionne donc selon le principe du "winner takes all" (Leloup, 2017): les mineurs sont en compétition l'un avec l'autre. Trouver la preuve de travail prend du temps, mais il est ensuite facile d'en vérifier la solution. Enfin, la difficulté de la tâche augmente au fur et à mesure que la blockchain grandit.
Pour le Bitcoin par exemple, la difficulté augmente à chaque 2016 blocs validés (Antonopoulos, 2014).

1.9.2. Preuve d'enjeu

Preuve d'enjeu (proof of stake ou POS) désigne une méthode permettant de valider les blocs et de les inscrire dans une blockchain, contrairement au POW le POS est beaucoup moins énergivore. C'est un « minage virtuel » car il n'y a pas besoin d'acheter du matériel informatique puissant !

Pour participer à un Proof-of-Stake il faut
possèder une certaine quantité de crypto-monnaie (tokens) pour la création et validation de nouveaux blocs investir dans l'achat de la crypto-monnaie ensuite les stocker dans le wallet officiel de la crypto-monnaie, fait donc patie de réseau.
Sur la base du dernier bloc de la blockchain, l'algorithme sélectionne aléatoirement un « validateur » qui aura le droit de créer et valider le prochain bloc. Plus cette somme est grande, plus l'utilisateur a des chances de valider le bloc.

Dans ce cas, le terme de minage est remplacé par celui de minting. Si le bloc n'est pas créé dans un intervalle de temps donné, une deuxième personne est sélectionnée et ainsi de suite. Une fois le bloc est valide vous ganier les récompense correspond aux frais de transactions qui sont contenues dans un bloc.

1.11 Blockchain vs traditionnel BDD

Avantages de la technologie blockchain	• Blockchain peut prouver l'autorité et la validité de sa propre transaction au lieu de faire appel à un administrateur central qui doit valider et assumer la responsabilité (Swan, 2015). • La Blockchain, comme tout autre bdd, doit être exécutée sur du matériel physique. Cependant, contrairement à d'autres systèmes, il n'existe aucun propriétaire car il est physiquement impossible pour une Blockchain de s'exécuter sur un seul nœud alors aucune entité n'à le pouvoir de modifier les informations stockées. Moins sensible à la corruption ou à la fraude • Les informations stockées dans une Blockchain sont transparentes pour tous les nœuds. Il existe tjrs un moyen de vérifier l'historique de Tx. ((Atzori, 2015); (Swan, 2015)). • Les données ne sont pas stockées dans un seul emplacement. Il n'y a donc pas une personne responsable de la sécurité. ((Ølnes, 2016); (Gervais et al., 2016)). • Le risque de défaillance du système est très faible. La robustesse de Blockchain est bien supérieure à celle d'un système de bdd traditionnel car elle est exécutée sur plusieurs systèmes et à plusieurs endroits. Si un nœud tombe en panne, les autres nœuds prendront le relais instantanément. Aucune configuration ou action supplémentaire n'est requise car chaque nœud possède une copie de la chaîne de blocs complète.. (Ølnes et al., 2017)

Désavantages de la technologie	• La Blockchain est toujours plus lente qu'un système de bdd traditionnel. Cela coûte plus cher, car il coûte plus d'énergie, de matériel et de capacité d'infrastructure(Eyal et al., 2016). • Chaque nouvelle connexion d'égal à égal, une preuve de la validité et de l'intégrité de la source doit également être fournie. Cela se fait par une signature numérique signifie alors il faudra plus de temps et de puissance de calcul par rapport aux systèmes traditionnels dans lesquels vous pouvez envoyer des informations instantanément (Gaetani et al., 2017). • Une transaction ne sera autorisée que si au moins 50% des nœuds la valident. Ce processus prend du temps car chaque nœud doit communiquer avec les autres nœuds. Un système traditionnel ne nécessite pas une telle échelle (Gaetani et al., 2017). • Blockchain doit valider et autoriser chaque transaction, mais pour chaque transaction, les calculs sont compliqués car elle chiffre toutes les informations. Avec un système traditionnel, il est possible de l'ignorer et de gagner beaucoup de vitesse avec moins de puissance matérielle. • Il est très difficile d'élargir la capacité d'une blockchain existante (Ølnes, 2016).

1.12 Les domaines des applications

La plupart des applications son classe en applications financières et non financières, en revanche, Blockchain est adopté dans de nombreux domaines :

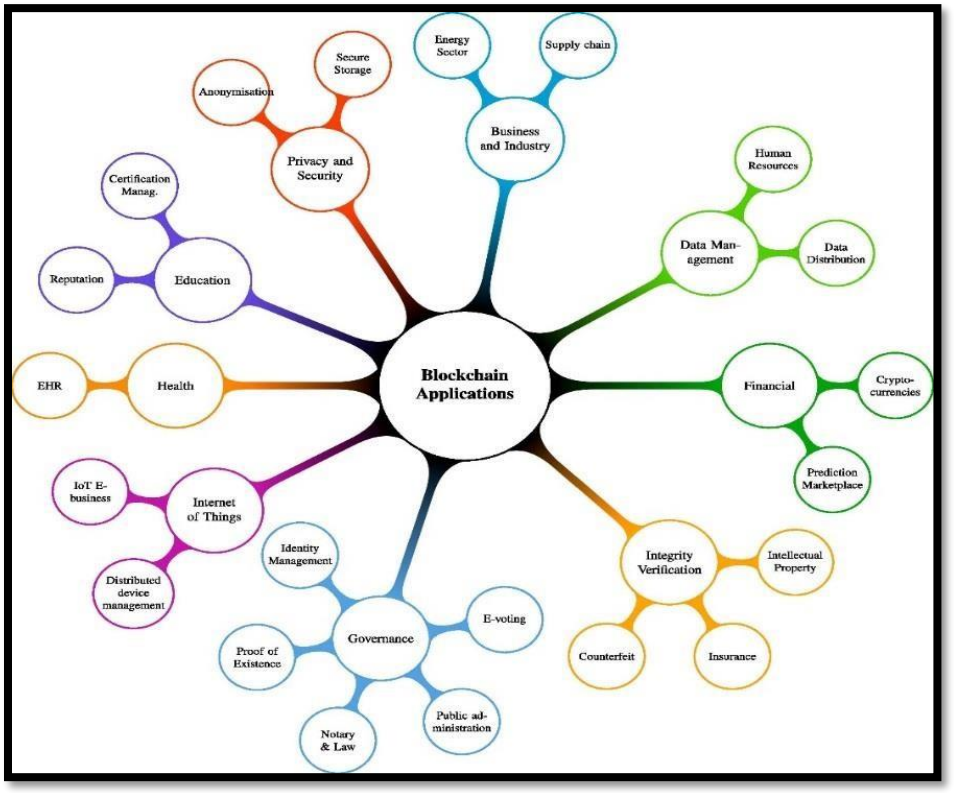


Figure 1.5 : Les domaines d'application de la blockchain (Casino et al., 2018)

1.12.1 Applications financières : la blockchain par le secteur financier entraînera à terme des économies de coûts dans des domaines tels que les rapports financiers centraux.

1.12.2 Vérification d'intégrité : Les chaînes de caractères activées par la blockchain ont permis d'automatiser plusieurs processus dans le secteur des assurances.

1.12.3 La gouvernance : La responsabilité, l'automatisation et la sécurité offertes par Blockchain pourraient à terme entraver la corruption. Par exemple l'attestation, l'identification, les contrats de mariage, les taxes et le vote.

1.12.4 Internet des objets : L'idée principale est de fournir un échange de données sécurisé et vérifiable dans des scénarios hétérogènes tenant compte du contexte avec de nombreux dispositifs intelligents interconnectés.

1.12.5 Confidentialité et sécurité : Les organisations centralisées - publiques et privées - collectent de grandes quantités d'informations personnelles et sensibles. La Blockchain est considérée comme une occasion d'améliorer les aspects de sécurité de la donnée.

1.12.6 Gestion de la chaîne logistique : La blockchain accroître la transparence et la responsabilité dans les réseaux de supply chain, permettant ainsi des chaînes de valeur plus flexibles. Elle améliore en particulier la visibilité, l'optimisation et la demande.

1.12.7 Secteur énergétique

La blockchain peut réduire les coûts et créer de nouveaux modèles commerciaux, mieux gérer la complexité, la sécurité des données, renforcer la transparence et la confiance du système de marché de l'énergie, garantir la responsabilité tout en préservant les exigences de confidentialité, renforcer les échanges directs entre utilisateurs.

1.12.8 Éducation : La blockchain peut résoudre les problèmes de vulnérabilité, de sécurité et de confidentialité dans le cas d'environnements d'apprentissage comme la gestion des certificats éducatifs et dans le cas de l'édition savante, blockchain peut être utilisé pour mieux traiter les soumissions de manuscrits.

1.12.9 Applications diverses : Les applications de blockchain peuvent être trouvées dans le secteur humanitaire, en particulier pour lutter contre la pauvreté. Aussi pour construire des systèmes de transport intelligents dans des contextes de villes intelligentes. La blockchain devrait jouer un rôle central dans la gestion de l'environnement. Une autre application intéressante peut être trouvée dans le contexte des médias sociaux. Certaines autres applications telles que, le calcul de périphérie et la mise en place de systèmes de partage de ressources informatiques.

1.13 Le protocole Bitcoin

Bitcoin est la crypto-monnaie la plus connue. Dans cette partie nous expliquerons les algorithmes utilisés et leur fonctionnent, comment la blockchain est appliquée dans Bitcoin et comment l'exploration de blocs fonctionne. Nous discuterons enfin des attaques possibles et des limitations de Bitcoin.

1.13.1 Définition

Bitcoin peut être défini de différentes manières. C'est un protocole, une monnaie numérique et une plateforme. Il s'agit d'une combinaison de réseau peer-to-peer, de protocoles et de logiciels facilitant la création et l'utilisation de la monnaie numérique nommée bitcoin. Notez que Bitcoin avec une B majuscule est utilisé pour faire référence au protocole Bitcoin, alors que bitcoin avec une b minuscule est utilisé pour faire référence à la devise Bitcoin. Les nœuds de ce réseau d'égal à égal se parlent via le protocole Bitcoin. (Bashir, 2017)

1.13.2 Algorithmes de signature

L'algorithme spécifique utilisé par Bitcoin est l'algorithme ECDSA. Les signatures dans cet algorithme sont très importantes pour valider les transactions et de cette manière, seul le propriétaire des bitcoins peut envoyer ces bitcoins à une autre adresse.

- **ECDSA**

Pour générer des clés, nous avons besoin d'une courbe elliptique et d'un point de base. En tant que courbe, secp256k1 avec la forme $y^2 = x^3 + 7$ est utilisé pour avoir un niveau de sécurité de 256 bits. Avec cette norme, la courbe, le point de base G et l'ordre de G, n sont connus. Certaines clés privées (sk) et publiques (pk) peuvent maintenant être générées. La clé secrète est de 256 bits de long et la clé publique non compressé est de 512 bits et 257 bits de long compressés. La figure 9 résume la génération des clés public et privée.

- **Le hachage**

Dans l'algorithme, la plupart des messages sont hachés avec une fonction de hachage. De cette manière, le message peut avoir n'importe quelle longueur, mais l'entrée de l'algorithme doit être de 256 bits et ainsi, tout message peut être signé. La fonction de hachage utilisée est SHA-256 et, parfois, lorsqu'un hachage plus court est requis, RIPEMD-160 est utilisé. Ceci est principalement utilisé pour créer des adresses. Dans Bitcoin, presque tout est haché deux fois, double SHA-256 ou d'abord avec SHA-256, puis avec RIPEMD-160 pour un hachage plus court.

1.13.3 Transactions

Les transactions contiennent quelques éléments différents, tous nécessaires pour s'assurer que tout est sécurisé. Une transaction contient les éléments suivants :

- **Les entrées (inputs) :** contiennent une valeur correspondant au nombre de bitcoins qui seront envoyés à une autre adresse. Les entrées ont un hachage de la transaction précédente d'où proviennent les pièces et ce hachage agit comme un pointeur de hachage.
- **Les sorties (outputs) :** Ce champ contient la valeur d'un nombre de bitcoins qui sont envoyés à une adresse spécifique.
- **Un identifiant unique :** Cet identifiant est nécessaire pour suivre toutes les transactions.
- **Signatures :** Ce sont très importants. Sans les signatures, une transaction ne peut être valide. Toute personne qui envoie une entrée doit signer la transaction pour être valide. De cette manière, seuls les détenteurs des pièces peuvent les envoyer.
- **Métadonnées :** Dans ce domaine, des informations supplémentaires sont stockées. Par exemple, la taille de la transaction, le nombre d'entrées et de sorties, le hachage de la transaction, qui peuvent être utilisés comme identifiant unique et comme paramètre de temps de verrouillage. Ce paramètre peut être utilisé pour bloquer une transaction jusqu'à une heure ou un numéro de bloc spécifique.

1.13.4 Blocks

Dans le système Bitcoin, un bloc est créé environ toutes les dix minutes. Les transactions effectuées dans le système Bitcoin sont enregistrées dans les blocs. Un bloc contient un en-tête et un corps, comme le montre la figure 1.11.

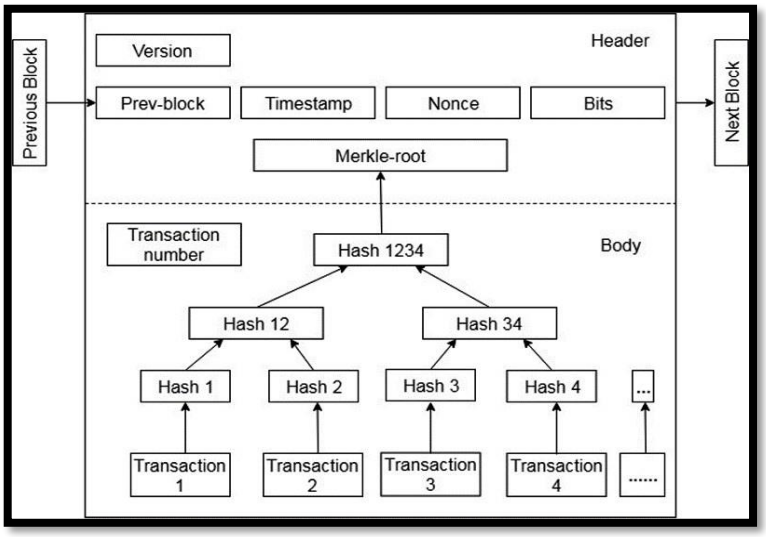


Figure 1.6 :Architecture du bloc Bitcoin (Bashir , 2017)

L'en-tête contient les métadonnées du bloc (voire le tableau). Le corps inclut principalement les détails des transactions dans la structure de l'arbre de Merkel (tableau)

Octets	**Nom**	**La description**
80	En-tête de bloc	Inclut les champs de l'en-tête de bloc décrit dans le tableau suivant.
variable	Compteur	Le champ contient le nombre total de transactions dans le bloc.
variable	Transactions	Toutes les transactions dans le bloc.

Tableau1.2 : La structure d'un bloc (Bashir , 2017)

Octets	**Nom**	**La description**
4	Version	Le numéro de version du bloc qui dicte les règles de validation de bloc à suivre.
32	hachage précédent	Il s'agit d'un double hachage SHA256 de l'en-tête du bloc précédent.
32	Racine de merkle	Il s'agit d'un double hachage SHA256 de l'arbre de sélection de toutes les transactions incluses dans le bloc.
4	Horodatage	c'est le moment où le mineur a commencé à hacher l'en-tête
4	Difficulté	C'est la cible de difficulté du bloc.
4	Nonce	Il s'agit d'un nombre arbitraire que les mineurs modifient à plusieurs reprises afin de produire un hachage qui remplit le seuil de difficulté.

Tableau 1.3 : The structure of a block header (Bashir , 2017)

1.13.5 Synchroniser avec le réseau

Une fois qu'un nouveau nœud a rejoint le réseau bitcoin, il télécharge la blockchain en demandant des blocs historiques aux autres nœuds. Ceci est mentionné ici dans le contexte du mineur Bitcoin; Cependant, ce n'est pas nécessairement une tâche réservée aux mineurs.

- **Validation des transactions** : les transactions diffusées sur le réseau sont validées par des nœuds complets en vérifiant et en validant les signatures et les sorties.

- **Validation de bloc** : les mineurs et les nœuds complets peuvent commencer à valider les blocs reçus en les évaluant par rapport à certaines règles. Cela inclut la vérification de chaque transaction dans le bloc ainsi que la vérification de la valeur de nonce.

- **Créer un nouveau bloc :** les mineurs proposent un nouveau bloc en combinant les transactions diffusées sur le réseau après leur validation.

- **Effectuer une preuve de travail :** cette tâche est au cœur du processus d'extraction et c'est là que les mineurs trouvent un bloc valide en résolvant un casse-tête informatique. L'en-tête de bloc contient un champ de nonce de 32 bits et les mineurs doivent faire varier à répétition le nonce jusqu'à ce que le hachage résultant soit inférieur à une cible prédéterminée.

- **Obtenir une récompense :** une fois qu'un nœud a résolu le casse-tête, il diffuse immédiatement les résultats et les autres nœuds le vérifient et acceptent le blocage. Il y a une faible **chance** que le bloc nouvellement frappé ne soit pas accepté par d'autres mineurs en raison d'un conflit avec un autre bloc trouvé à peu près au même moment. Une fois accepté, le mineur est récompensé par 12,5 bitcoins (à partir de 2016) et tout montant associé.

1.13.6 Algorithme de minage

Le Bitcoin utilise l'algorithme PoW repose sur l'idée qu'un nœud aléatoire est sélectionné à chaque fois pour créer un nouveau bloc. Dans ce modèle, les nœuds se font concurrence pour être sélectionnés proportionnellement à leur capacité de calcul d'exploration de données comprend les étapes suivantes.

1. Le bloc de hachage précédent (P_{hash}) est extrait du réseau bitcoin.
2. Assemblez un bloc de transactions (Tx) potentielles diffusées sur le réseau.
3. Calculez le double hachage de l'en-tête de bloc avec un nonce (N) et le hachage précédent (P_{hash}) en utilisant l'algorithme SHA256.

$$H(H\ (N\ |P_{hash}|\ Tx|Tx|\dots Tx)) < Target$$

4. Si le hachage résultant est inférieur à la difficulté actuelle ($Targe$) arrêtez le processus.
5. Si le hachage résultant est supérieur au niveau de difficulté, répétez le processus en incrémentant le nonce. À mesure que le débit de hachage du réseau bitcoin augmentait, le nombre total de nonces 32 bits était épuisé trop rapidement.

Afin de résoudre ce problème, la solution extra nonce a été mise en œuvre, la transaction coinbase étant utilisée comme source de nonce supplémentaire pour fournir un plus large éventail d'activités à rechercher par les mineurs.

La difficulté d'exploitation a augmenté au fil du temps et les bitcoins pouvant être exploités par des ordinateurs portables à processeur unique nécessitent désormais des centres d'extraction dédiés pour résoudre le casse-tête. (Bashir , 2017)

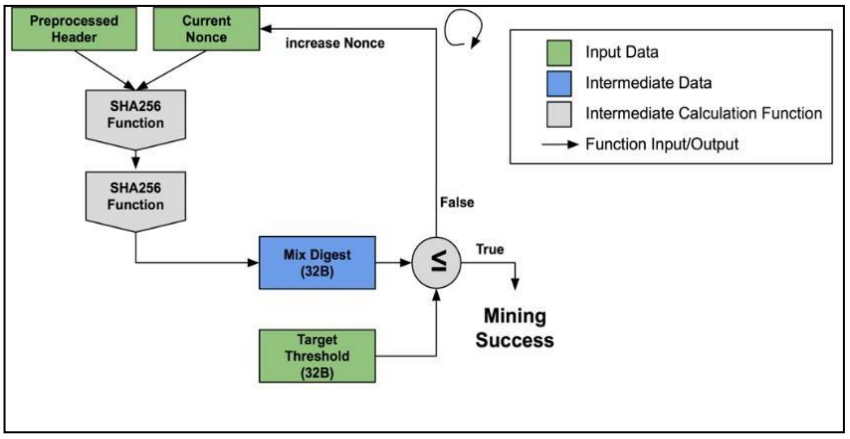


Figure 1.7 : Processus de minage de Bitcoin (Bashir, 2017)

1.14 Conclusion

Dans chapitre, nous avons présenté la technologie Blockchain. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

Le principe de base d'une chaîne de blocs repose sur la notion de preuve de travail, et a recours aux techniques de la cryptographie pour vérifier les détenteurs distincts d'un système d'enregistrement collectif.

Nous avons conclu dans ce chapitre que le protocole et les algorithmes de minage de blockchain peut l'appliquer à n'importe quel domaine pour assurer un haut niveau de sécurité..

LA CRYPTOGRAPHIE DERIERE LA BLOCKCHAIN

2.1. Introduction

Les transactions dans un réseau blockchain sont stocké sur les serveurs des utilisateurs, mis à jour en temps réel et ils sont aussi infalsifiables car ils sont reposés sur un système cryptographique, ensuite sont inscrites dans le livre après validation, par blocs de données, pour former une chaîne de blocs inaltérables.

Dans ce chapitre nous allons démystifier la technologie derrière la blockchain, introduire les principes et les concepts de la cryptographie.

2.2. La cryptologie

Est la science qui englobe la cryptographie et la cryptanalyse. C'est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information.(Lotfi, 2017)

2.1.1. La cryptographie

La cryptographie est l'art de chiffrer, coder les messages est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support non sécurisé.

2.1.2. La cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

2.3. Type de la cryptographie

2.3.1. Chiffrement symétrique

Dans un chiffrement symétrique (chiffrement à clef secrète), deux utilisateurs voulant communiquer vont tout d'abord convenir d'une clef K à utiliser qu'ils gareront secrète.

Lorsque l'un d'entre eux souhaite communiquer le message M il lui appliquera la fonction de chiffrement ( ) en utilisant la clef K pour produire le chiffré $C = E(M, K)$. En envoyant le chiffré C sur le réseau l'utilisateur sait que s'il est intercepté par un tiers ce dernier ne pourra pas en comprendre le sens, seul son interlocuteur connaissant K pourra effectuer la transformation inverse et obtenir $M = (C, K)$, où $D( )$ est la fonction de déchiffrement inverse de $E( )$.

2.3.2. Chiffrement asymétrique

Dans un chiffrement asymétrique (chiffrement à clef publique), chaque utilisateur génère une paire de clefs, l'une appelée clef secrète qu'il est le seul à connaître, l'autre appelée clef publique qu'il diffuse sur un annuaire et qui peut servir aux autres pour le contacter.

Lorsqu'un utilisateur veut envoyer un message M il va aller chercher la clef publique du destinataire $K_{pub,est}$ et l'utilise pour créer un chiffré $C = E(M, K_{pub,dest})$ Contrairement au

chiffrement symétrique, il sera alors lui-même dans l'incapacité d'effectuer la transformation inverse ne possédant pas la clef privée de son interlocuteur. L'interlocuteur sera le seul à pouvoir récupérer le message originel $M = (C, K_{priv,dest})$, grâce à sa clef privée $K_{priv,dest}$.

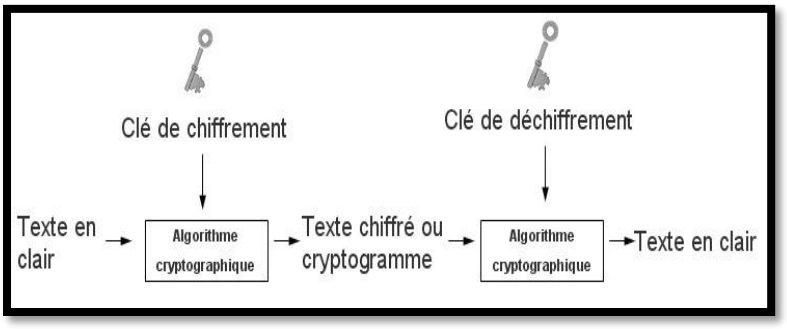


FIgure 2.1 : Chiffrement symétrique (Lotfi, 2017)

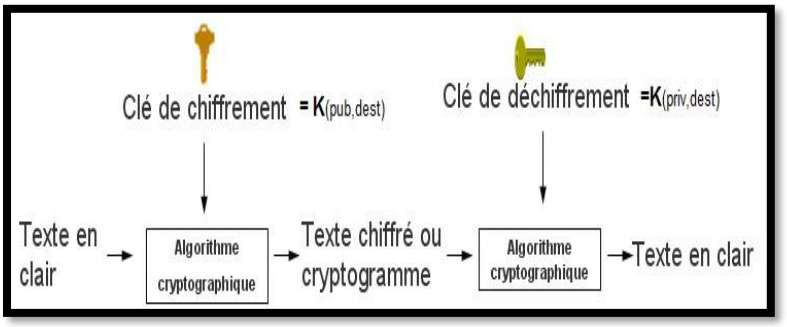


Figure 2.2: chiffrement asymétrique (Lotfi, 2017)

2.4. Objectif de la cryptographie

Globalement, la cryptographie permet de résoudre cinq problèmes différents :

1. **La confidentialité :** Consiste à rendre l'information inintelligible à d'autres personnes que les acteurs de la transaction.
2. **Le contrôle d'accès :** permet de limite l'accès aux donnes, serveur ou personnes autorisées
3. **L'authentification :** Consiste à assurer l'identité d'un utilisateur.
4. **L'Intégrité :** Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication
5. **La non-répudiation** : De l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

2.5. Méthodes de Chiffrement

2.5.1. Chiffrement par bloc

L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire.
2. Découper cette chaîne en blocs de longueur donnée.
3. Chiffrer un bloc en l'additionnant bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré

2.5.2. Chiffrement par clé publique

1) RSA

Proposé en 1977 par (Rivest - Shamir - Adleman) ce système est basé sur le calcul exponentiel. Sa sécurité repose sur la fonction unidirectionnelle suivante : le calcul du produit de 2 nombres premiers est aisé. La factorisation d'un nombre en ses deux facteurs premiers est beaucoup plus complexe. Ce crypto système utilise deux clés *d* et *e*, interchangeables. Le chiffrement C, et le déchiffrement D se fait selon :

- $C = M^e \, mod \, (n)$
- $M = C^d \, mod \, (n)$

2) Courbe elliptique

Il s'agit d'un concept proposé en 1985 par deux chercheurs Miller et Klobitz, de façon totalement indépendante. Ce type de cryptographie, toujours basé sur le modèle asymétrique, permet aussi bien de chiffrer que de signer. On utilise souvent l'abréviation ECC, pour Elliptic Curve Cryptography. Parmi les schémas cryptographiques les plus connus, on retrouve l'algorithme ECDSA.

- **Principe Général :**

Une courbe elliptique est un objet très simple mais qui a des propriétés tout à fait surprenantes. Elles ont la forme suivante :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Pour leur usage en cryptographie, a_1, a_2 et a_3 doivent être égaux à 0. Comme les cryptographes ont l'habitude de renommer $a_4 = a$ et $a_6 = b$, on obtient :

$$y^2 = x^3 + ax + b$$

Deux opérations mathématiques sont possibles sur les courbes elliptiques :

L'addition de points : quand on a deux points P et R sur une courbe elliptique EC, alors on peut calculer leur addition $Q = P + R$, et le résultat Q appartient aussi à EC.

La multiplication de points : quand on a un point P sur une courbe elliptique EC, alors on peut additionner K fois ce même point, ce qui résulte en la multiplication de points $Q = p *$, et le résultat Q appartient aussi à EC.

Pour définir l'addition $Q = P + R$, il faut tracer une droite reliant P et R. Cette droite (en rouge sur la figure 1.a) coupe la courbe elliptique en un troisième point appelé $-Q$. Le symétrique de ce point par rapport à l'axe des abscisses (obtenu en suivant la droite pointillée verte sur la figure 1.a) est le résultat Q de cette addition.

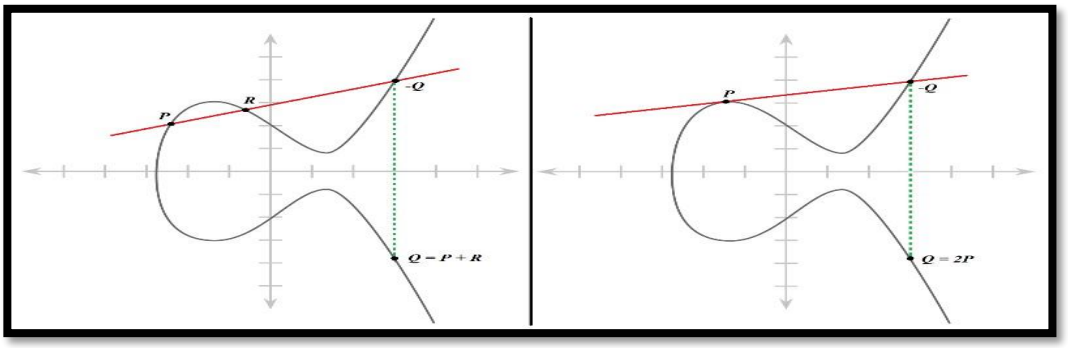


Figure 2.3.a : Addition de deux points *P* et *R*, Figure 2.3.b : Multiplication du point *P* quand *k = 2*.
(Lopez and Dahab, 2000)

- **ECDSA** :

Soit le message m à signer, G un élément d'une courbe elliptique d'ordre n avec n un nombre premier plus grand que 2^{160}. La courbe est également définie par deux éléments a et b qui sont des éléments d'un champ de Galois de cardinalité q.

Préparation des clés

- Choisir un entier s entre 1 et $n - 1$.
- Calculer Q = sG en utilisant l'élément de la courbe elliptique.
- La clé publique est Q et la clé privée est s.

Signature

- Choisir de manière aléatoire un nombre k entre 1 et $n - 1$.
- Calculer (i, j) = kG .
- Calculer : $x = intege(i) mod\, n$
- Calculer : $= \frac{H(m)+sx}{k} mod\, n$ / H(m) : le résultat d'un hachage avec SHA-1 sur m

- Si *x* ou *y* sont nulles, recommencer
- La signature est la paire (*x*, *y*).

Vérification

- Contrôler que x et y sont bien entre 1 et *n*-1
- Vérifier que $x = in(i) \ mod \ n$ sachant que $(i, j) = {}^{H(m)}\underset{y}{mod}\ n)\ G\ (\ {}^{x}\underset{y}{mod}\ n\ )\ Q$.
- Vérifier que *Q* est différent de (0,0) et que Q appartient bien à la courbe elliptique
- Vérifier que nQ donne (0,0)
- Portail de la cryptologie

2.6. Les fonctions de hachage cryptographiques

2.6.1. Définition

Formellement, une fonction de hachage est une fonction de l'ensemble des suites binaires (de longueur quelconque, non bornée) vers les suites de longueur *n* :

$$\mathrm{F} : \{0,1\}^{*} \rightarrow \{0,1\}^{n}$$

Se comporte comme une fonction choisie aléatoirement parmi toutes les fonctions de $\{0,1\}^{*}$ vers $\{0,1\}$. Les fonctions de hachage sont caractérisées par :

1. **Ce sont des fonctions unidirectionnelles :** A partir de (M) il est impossible de retrouver M.
2. **Ce sont des fonctions sans collisions :** A partir de (M) et M il est impossible de trouver $M' \neq M$ tel que $(M') = H(M)$. [03] de cette famille.

2.6.2. Conception de SHA-256

Le SHA-256 a une taille de message d'entrée inférieure à 2^{64}bits. La taille du bloc est de 512 bits et sa taille de mot est de 32 bits. La sortie est un résumé de 256 bits.

La fonction de compression traite un bloc de message de 512 bits et une valeur de hachage intermédiaire de 256 bits. Cette fonction comporte deux composants principaux : une fonction

de compression et un calendrier de messages.

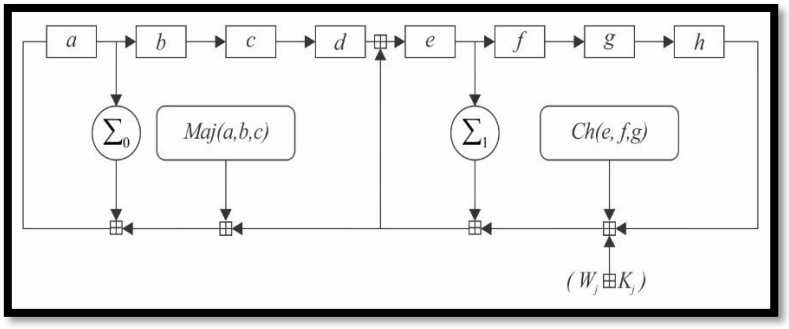
L'algorithme fonctionne comme suit :

- **Prétraitement**

1. Remplissage du message, qui est utilisé pour rendre la longueur d'un bloc à 512 bits si elle est inférieure à la taille de bloc requise de 512 bits.
2. Analyser le message en blocs de message garantissant que le message et son remplissage sont divisés en blocs égaux de 512 bits.
3. Définissez la valeur de hachage initiale, qui correspond aux huit mots de 32 bits obtenus en prenant les 32 premiers bits des parties fractionnaires des racines carrées des huit premiers nombres premiers. Ces valeurs initiales sont choisies au hasard afin d'initialiser le processus et donnent la certitude qu'aucune porte dérobée n'existe dans l'algorithme.

- **Calcul du hachage**

1. Chaque bloc de message est traité dans une séquence et nécessite 64 tours pour calculer la sortie de hachage complète. Chaque tour utilise des constantes légèrement différentes pour s'assurer qu'il n'y a pas deux tours identiques.
2. Tout d'abord, la planification des messages est préparée.
3. Ensuite, huit variables de travail sont initialisées.
4. Ensuite, la valeur de hachage intermédiaire est calculée.
5. Enfin, le message est traité et le hachage de sortie est généré :



Où a, b, c, d, e, f, g et h sont les registres. Maj et Ch sont appliqués bit à bit $\sum_0 et \sum_1$ et effectue une rotation bit à bit. Les constantes rondes sont Wj et Kj, auxquelles on ajoute mod 2 ^ 32.

2.6.3. Arbre de Merkle

Le concept d'arbre Merkle (Merkle Tree) a été introduit par Ralph Merkle .C'est un arbre binaire avec des pointeurs de hachage (Narayanan et al., 2016). Les feuilles dans l'arbre contiennent les données. Le nœud parent, contient un hachage de ces données et est associé à

un autre nœud parent. Cela continue jusqu'à la racine. De cette manière, le nœud racine est le hachage de toutes les données de l'arbre. On peut vérifier chacun des hachages de l'arbre jusqu'à la racine. Si tous les hachages sont corrects, le bloc de données est inclus dans l'arborescence.

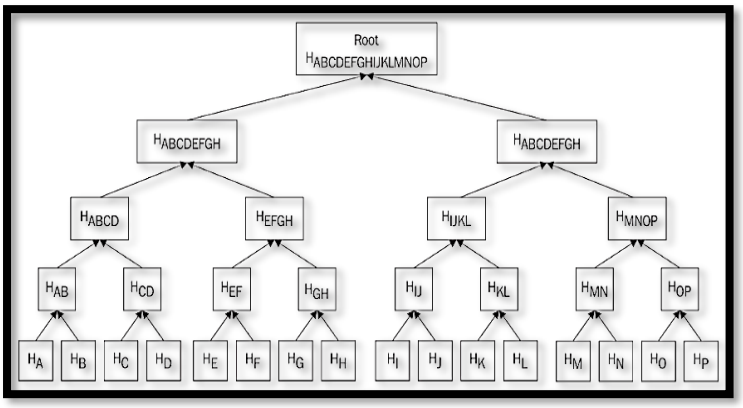


Figure 2.4 : Arber de Merkle (Narayanan et al., 2016)

2.6.4. Signature électronique

C'est l'application la plus importante des fonctions de hachage. Ils permettent à un utilisateur de signer un message à l'aide de sa clé privée . Chacun peut vérifier la validité de cette signature grâce à la clé publique correspondante.

En pratique**, au lieu d'appliquer un schéma de signature S directement à un long message** , on applique la signature à un haché du message $H(M)$, La signature d'un message M est alors $S(H(M))$ (voir la Figure 1.7). Ainsi, l'opération de signature est faite sur un identifiant de petite taille et elle sera moins coûteuse.

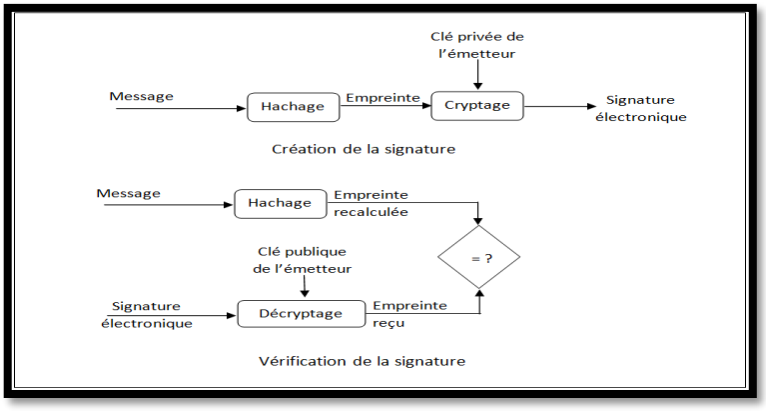


Figure 2.5 – Schéma de signature électronique. (BELFEDHAL, 2016)

L'utilisation de la cryptographie ne se limite pas dans ces applications, plusieurs fonctions de hachage peuvent utiliser dans une seule citation de sécurité, ça des pant le cas d'utilisation.

2.7. Conclusion

Dans chapitre, nous avons présenté la technologie derrière la Blockchain. Les algorithmes de la cryptographie permettent ainsi de sécuriser les données sur un réseau blochchain, et assurant le processus de minage.

LE BITCOIN & LE VOTE ELECTRONIQUE

3.1. Introduction

Comme nous l'avons vu dans les chapitres précédents, la technologie des chaînes de blocs consiste en une évolution de l'ordinateur dans le domaine de la sécurité et des conflits de données. Étant donné que cette technologie fournit un support solide et sécurisé pour la participation d'une base de données en ligne ou au sein d'une communauté en ligne limitée (États, constructeur de véhicules, municipalités, associations, etc.).

À l'heure actuelle, le Bitcoin est l'application la plus connue qui a efficacement exploité la manière dont l'authentification par chaîne garantit la non-répudiation et la confidentialité des données sans recourir à des tiers de confiance.

Dans ce chapitre, nous allons étudier le domaine de vote électronique, ensuite nous discutons les problèmes auxquels il est confronté. Enfin, nous évoquerons le statut du vote électronique basé sur le protocole bitcoin.

3.2. Le vote électronique

Le vote électronique, également appelé « vote par ordinateur », est un système de vote non physique, avec comptage automatique, basé sur des systèmes informatiques et des algorithmes de comptage. Il est caractérisé par la vitesse et la simplicité de son caractère informel.

3.3. Les caractéristiques de vote électronique

Les élections sont un outil qui se démarque pour prendre en compte :

- **Confiance :** Les électeurs font confiance à la validité des résultats lorsqu'ils suivent les règles applicables. Des violations sont parfois enregistrées et un contentieux électoral est présenté. Dans ce cas, il estime l'ampleur des attaques sur les écarts entre les candidats pour décider d'annuler les scrutins ou non.

- **Transparence :** La transparence électorale est un concept complexe. Ce sont toutes des règles et mesures organisationnelles qui permettent de surveiller les attaques potentielles sur la validité des élections (bourrage de bulletins de vote, substitution, lobbying, achat de votes, etc.).

- **Sécurité :** La transparence permet de surveiller les atteintes potentielles à la validité ou au secret du vote. Ces résultats peuvent faire l'objet d'un traitement juridique qui pourrait entraîner l'annulation des élections. Par conséquent, la transparence électorale est une base fondamentale de la confiance des électeurs et de la légitimité des élus. (**Enguehar et al., 2019**)

3.4. Types de vote électronique

Il existe plusieurs types de systèmes de vote électronique qui sont considérés comme un moyen de réduire les coûts, d'améliorer les techniques de vote et de lutter contre les mauvaises pratiques électorales :

3.4.1. Systèmes de vote par Internet

Un système de vote par Internet est un système à distance non supervisé qui permet à chaque électeur de voter à tout moment où il le souhaite avec n'importe quel appareil, juste avec accès à Internet. Cela en fait le système le plus confortable pour tous les utilisateurs. Cependant, de tels systèmes nécessitent une authentification très soignée pour éviter les fraudes.

Les pirates pourraient pirater le système pour affecter les résultats. C'est ce qui en fait pas le premier choix des gouvernements (**Apleasant , 2013**).

3.4.2. Machines à voter électroniques à enregistrement direct

Est un système qui offre des dispositifs électroniques tels qu'un écran tactile, un clavier, une souris ou un stylo électronique pour permettre aux électeurs de saisir leurs choix. C'est aussi un système non distant utilisé avec la supervision dans les bureaux de vote. La machine enregistre alors les choix des électeurs dans la puce mémoire. Une fois le choix terminé, les données enregistrées dans chaque machine seront transmises au centre de comptage par Internet ou par voie manuelle qui imprime les résultats et les envoie. Ensuite, le centre compte tous les votes et annonce les résultats. Chaque machine peut avoir ou non un enregistrement papier qui permet à chaque électeur de vérifier son choix après le vote afin que les gens soient généralement plus à l'aise pour l'utiliser car il offre plus de transparence (**Apleasant , 2013**).

3.4.3. Bulletin de vote électronique

Ce système similaire aux systèmes précédent. Les deux prennent le choix de l'électeur à l'aide d'appareils électroniques. La différence est que le premier ne stocke pas les données de vote, mais impriment un jeton avec le choix de l'électeur. Ensuite, l'électeur met ce jeton dans une urne électronique qui compte les votes automatiquement. Le deuxième est composé de deux machines, l'une pour prendre le choix de l'électeur et l'autre pour l'enregistrer. C'est un système facile à utiliser et à comprendre pour tout le monde, en particulier les anciens, car il est similaire à la méthode traditionnelle. C'est donc un bon choix pour entrer dans le monde du vote électronique pour les pays qui ne l'ont jamais utilisé auparavant (**Apleasant , 2013**).

3.4.4. Systèmes de reconnaissance optique

Ces systèmes sont une combinaison de bulletin de vote papier et de comptage électronique. L'électeur marque son choix avec un stylo ou un crayon sur un bulletin de vote donné, puis met ce papier sur un appareil qui peut le lire. La machine compte les votes en utilisant les notes faites par les électeurs sur le bulletin papier.

Ces systèmes sont un excellent choix car ils coûtent beaucoup moins cher par rapport aux autres systèmes, mais de nombreux facteurs peuvent affecter le processus de comptage, comme le type d'encre ou l'épaisseur du papier (**Apleasant , 2013**).

3.5. Les problèmes de vote électronique

Les élections gouvernementales dans le monde sont confrontées à des menaces croissantes pour la sécurité et à des préoccupations concernant l'intégrité des élections. Le vote par bulletin papier reste la forme de vote la plus répandue dans le monde. C'est le moins sensible aux cyberattaques mais très sensible aux erreurs humaines et à la fraude. Alors que de nombreux pays passent aux machines à voter électroniques, ils sont vulnérables aux cyberattaques en raison d'une technologie obsolète, mal conçue ou mise en œuvre. Des pirates ont démontré qu'ils pouvaient pirater chacune des 22 machines à voter achetées sur les sites d'enchères du gouvernement américain et sur eBay (**Sue, 2018**). Dans certains cas, les pays qui avaient introduit le vote électronique sont revenus au vote papier en raison de problèmes de sécurité.

3.5.1. Les problèmes de sécurité

Les systèmes de vote électronique sont confrontés à des problèmes de sécurité et à un défi de confidentialité. La fiabilité est la capacité d'un système à fonctionner sans erreur et sans panne. Voici quelques attaques contre la fiabilité du système de vote en ligne :

- ✓ Lenteur,
- ✓ Effondrer,

- ✓ Ne pas présenter de candidats,
- ✓ Absence du bouton de vote,
- ✓ Prouvez des résultats incorrects.

De plus, une erreur logicielle ou une perte de votes affecte la sécurité du système de vote électronique.

3.5.2. Les failles de vote électronique

Toutefois il existe des failles spécifiques au vote par Internet comme :

- **Les attaques de « Déni de service »**

Le système de vote, saturé de requêtes, n'est plus en mesure de répondre en un temps raisonnable et finit pas se mettre en indisponibilité.

- **Homme-au-milieu**

Un virus hébergé sur le terminal de l'électeur peut modifier le choix effectué par ce dernier juste avant qu'il ne soit chiffré puis envoyé au système de vote. Le vote, non chiffré, peut également être envoyé à des tiers à l'insu de l'électeur.

- **Liberté de vote**

Dans le cas d'élections via Internet, chaque personne ne doit soumettre son vote qu'une seule fois. A cet effet, il se voit attribuer l'identité de l'électeur et son vote tout en veillant au respect du secret du vote. Lorsqu'un défaut de confidentialité apparaît, il ne vote pas librement, recourant à un changement de choix.

- **Usage des droits à voter**

Derrière l'organisation électronique des élections se cache un gestionnaire qui renseigne sur le

processus de vote. Dans ce cas, il ne peut être garanti que l'administrateur n'utilisera pas les informations personnelles à mauvais escient et ne modifiera pas le vote.

Aucun système n'est parfait, des bogues logiciels doivent donc se produire d'une manière ou d'une autre. Le programme de vote électronique est très complexe et plus le programme est complexe, plus il est difficile de trouver et d'éliminer les erreurs. C'est pourquoi les erreurs entraînent une perte de sons et une panne du système.

3.6. La blockchain et le vote électronique

Le vote en ligne basé sur la technologie blockchain est très attrayant en raison de l'accessibilité et de l'intégrité qu'il peut apporter aux élections. Les caractéristiques fondamentales de la blockchain - immuabilité, responsabilité et sécurité - stimulent le potentiel de la technologie pour conserver en toute sécurité les registres d'inscription des électeurs et enregistrer les votes. Visualisation non autorisée. L'utilisation de la technologie de registre distribué (DLT) signifie que les informations ne sont pas centralisées, garantissant que toutes les données sont copiées sur les nœuds du réseau. Les informations ne peuvent pas être perdues et il n'y a pas de points centraux pour les cyberattaques telles que la suppression de bases de données ou les attaques par déni de service. Le réseau peer-to-peer sous-jacent fournit un mécanisme de validation qui protège l'intégrité des données verrouillées dans chaque bloc. Pour prévenir la fraude électorale, une application de vote peut utiliser plusieurs méthodes d'identification et d'authentification avant le vote. Cette numérisation des processus d'inscription et de vote des électeurs s'est également avérée rendre les élections moins chères et plus faciles à organiser.

3.7. Etat de l’art

Il existe peu de travaux qui démontrent l'utilisation de la blockchain dans le processus de vote. En Virginie, un formulaire de vote pour les résidents étrangers a été créé par vote mobile. Ces votes sont stockés sur une blockchain privée gérée par des mineurs. L'identité cryptée est préservée pour chaque électeur avec les votes, ce qui permet d'annuler le vote. Dans d'autres travaux, des symboles ont été imprimés et distribués pour être scannés et obtenir rapidement des explications sur les résultats des élections. Sur d'autres plateformes, chaque électeur reçoit

une paire de clés, lors de la création de son compte, pour garder le vote secret.

3.7.1. Système 1 : « Smartmatic-Cybernetica »

En 2016 , Smartmatic-Cybernetica a organisé la première élection en ligne au monde en utilisant la technologie blockchain pour le caucus du parti républicain de l'Utah en 2016. Près de 90% des électeurs se sont inscrits pour voter en ligne. La plateforme a permis à 24 486 électeurs de voter en toute sécurité depuis 45 pays différents à l'aide de leur ordinateur, tablette ou smartphone. (**Smartmatic, 2016**)

3.7.2. Système 2 : « Votem »

En 2017, les fans de musique ont pu utiliser la plateforme de vote mobile basée sur la blockchain de Votem pour voter pour l'introniser 2018 au Rock and Roll Hall of Fame. Votem a traité plus de 1,8 million de votes sans fraude, compromis, attaques ou piratage d'aucune sorte, ce qui en fait la plus grande utilisation du vote en ligne utilisant la technologie blockchain à ce jour.Le système Votem a récemment été utilisé pour le vote des intronisés 2018.(**Votem,2017**)

3.7.3. Système 3 : « Voatz »

En 2018, la première utilisation de la technologie blockchain lors d'une élection fédérale américaine, l'État de Virginie-Occidentale a utilisé l'application de vote mobile de Voatz pour permettre aux électeurs étrangers de voter aux élections de mi-mandat aux États-Unis de 2018. Au total, 144 électeurs de 31 pays ont participé au projet pilote. L'application Voatz s'appuie sur la technologie blockchain pour créer un enregistrement immuable des votes exprimés. Il utilise également un logiciel de cybersécurité pour détecter les logiciels malveillants sur les smartphones et la biométrie pour l'identification et l'authentification. (**Voatz,2018**)

3.8. Synthèse

Alors que Voatz et Votem sont des startups américaines en démarrage, Smartmatic-Cybernetica est un partenariat européen d'entreprises établies dont la technologie de vote non-blockchain a été utilisée pour organiser des élections dans le monde entier depuis 2005. Cela montre un large intérêt existant pour la blockchain- basées sur des solutions de vote en ligne afin d'augmenter la participation des électeurs et d'améliorer la sécurité électorale.

Ces études de cas démontrent que la technologie de la blockchain a été utilisée avec succès pour les élections gouvernementales et privées. Dans tous les cas, les élections en ligne se sont déroulées sans aucun problème de sécurité et avec une réponse extrêmement positive des électeurs et des participants.

Cependant, de nombreux experts en sécurité et en élection restent sceptiques quant à la capacité de la technologie de la blockchain à faire évoluer ou à résoudre les problèmes inhérents au vote en ligne.

«*Les technologies de vote mobile et Internet ne sont actuellement pas suffisamment sécurisées pour les applications à grande échelle. La technologie blockchain et son architecture environnante, y compris la menace de* logiciels *malveillants sur les appareils personnels, rendent cette forme de vote à distance actuellement impraticable pour une pratique à grande échelle ou à l'échelle nationale. La détection de logiciels malveillants sur les appareils personnels peut entraîner des failles de sécurité et la consommation d'énergie des fournisseurs hébergeant l'application est coûteuse.* » (**Irene .2018**)

Smartmatic-Cybernetica, les développeurs à l'origine de l'étude sur la blockchain, sont également sceptiques quant à la nécessité de la technologie blockchain pour le vote en ligne. Smartmatic-Cybernetica construit des solutions de vote électronique pour les pays du monde entier, ils sont préoccupés par les problèmes de gouvernance et de confidentialité qui entourent le vote par blockchain.

3.9. Conclusion

Le vote électronique était une question de machines à voter. Le vote en ligne n'était pas la première option pour des raisons de sécurité, mais au fil des années, les machines à voter sont devenues de plus en plus vulnérables. Par conséquent, les développeurs ont commencé à travailler pour sécuriser le vote en ligne en raison de l'évolution du développement de la sécurité. Par conséquent, les fonctionnalités de la blockchain devraient être exploitées pour résoudre tous les problèmes de sécurité et de confidentialité pour des élections justes et transparentes.

CHAPITRE 4

CONTRIBUTION

4.1 Introduction

Comme nous l'avons vu dans les chapitres précédents, la technologie des chaînes de blocs consiste en une évolution de l'ordinateur dans le domaine de la sécurité et des conflits de données. Étant donné que cette technologie fournit un support solide et sécurisé pour la participation d'une base de données en ligne ou au sein d'une communauté en ligne limitée (États, constructeur de véhicules, municipalités, associations, etc.).

À l'heure actuelle, la crypto-monnaie est l'application la plus connue qui a efficacement exploité la manière dont l'authentification par chaîne garantit la non-répudiation et la confidentialité des données sans recourir à des tiers de confiance tels que des banques ou des banques. États. Cependant, la crypto-monnaie commence à peine à utiliser cette technique dans des zones plus vastes et plus sensibles

Dans ce chapitre, nous présentons notre contribution et les outils que nous avons utilisés pour implémenter le cas d'étude, et nous conclure avec les résultats que nous avons atteints

4.2 La contribution

Bien qu'il n'existe pas encore de solution parfaite pour la sécurisation dans la gestion de vote, l'adoption de technologies telles que Blockchain pour accroître la transparence de la gestion des d'élection renforcera la fiabilité du processus dans son ensemble. En outre, cela réduira les tâches fastidieuses, manuelles et répétitives pour les fabricants, les clients, les autorités et toutes les autres parties prenantes, à condition que les clés de cryptage soient utilisées sous le contrôle de l'utilisateur

L'application de cette technologie au secteur des votes fournira un enregistrement fiable et sûr de tous les choix des électeurs dans le grand livre distribué et horodaté, ce qui permettra de suivre les choix de la source au résultat final. Les utilisateurs pourront importer et exporter des données via une interface utilisateur avec différents niveaux de fonctionnalité et d'accès.

Veillera également à ce que les responsables de processus de vote se conforment, et aidera les régulateurs à identifier et à lutter contre les violations illicites des votes le tableau suivant présente la solution base sur la blockchain pour les problèmes déjà cite dans la première partie de cette mémoire.

Problème	**Solution de blockchain**
Fraude et manipulation	Avec la technologie blockchain, il est important que les données saisies soient correctes, car il n'est plus possible de les modifier par la suite
Mauvaise ou perte d'informations	Une fois que quelque chose est entré dans une blockchain, celle-ci est immédiatement sécurisée. Les votes étant saisis numériquement avec une solution de blockchain, ils ne peuvent pas être perdus physiquement. Une implémentation blockchain est la bonne solution pour résoudre ce problème.

Manque de connaissances sur la technologie	La technologie Blockchain ne modifiera pas le manque actuelle des connaissances et de l'expertise en informatique.
Manque de contrôle	Si les organisations sauvegardent les données en utilisant Blockchain et s'assurent que cela se fait de la bonne manière, il est possible d'utiliser la technologie Blockchain en tant que "facteur de confiance". Les données qu'il contient ne peut pas être modifié et s'il est entré correctement, vous pouvez garantir la fiabilité des informations. Ceci offre une solution pour les services d'inspection.

Tableau 4.1 Les solutions

4.3 Architecture proposée

4.3.1 Aperçu de la conception de l'architecture

Afin de gagner en efficacité dans la gestion de la confiance pour le réseau de gestion d'élection, nous proposons un système de suivi des votes basé sur la blockchain.

La figure suivante montre l'architecture globale proposée pour le réseau de gestion des d''élection. Dans le modèle proposé, le réseau est divisé en deux groupes différents - le réseau principal et le réseau de bord - en utilisant la technique de la blockchain.

- Le réseau central est constitué de nœuds de mineur dotés de ressources de calcul et de stockage élevées. Seront responsables de la création des blocs et de la vérification de la preuve de travail.

- Les nœuds de bord sont les participants dans le système d''élection. Ils disposent d'une capacité de stockage et de calcul limitée

Chaque nœud périphérique agit comme un serveur centralisé pour une infrastructure publique spécifique . La nature distribuée du modèle proposé peut améliorer la résilience de l'ensemble du système et limiter l'impact des attaques, même lorsque le nœud est compromis. En d'autres termes, si le nœud de bord est compromis, l'effet résultant doit être limité à la zone locale.

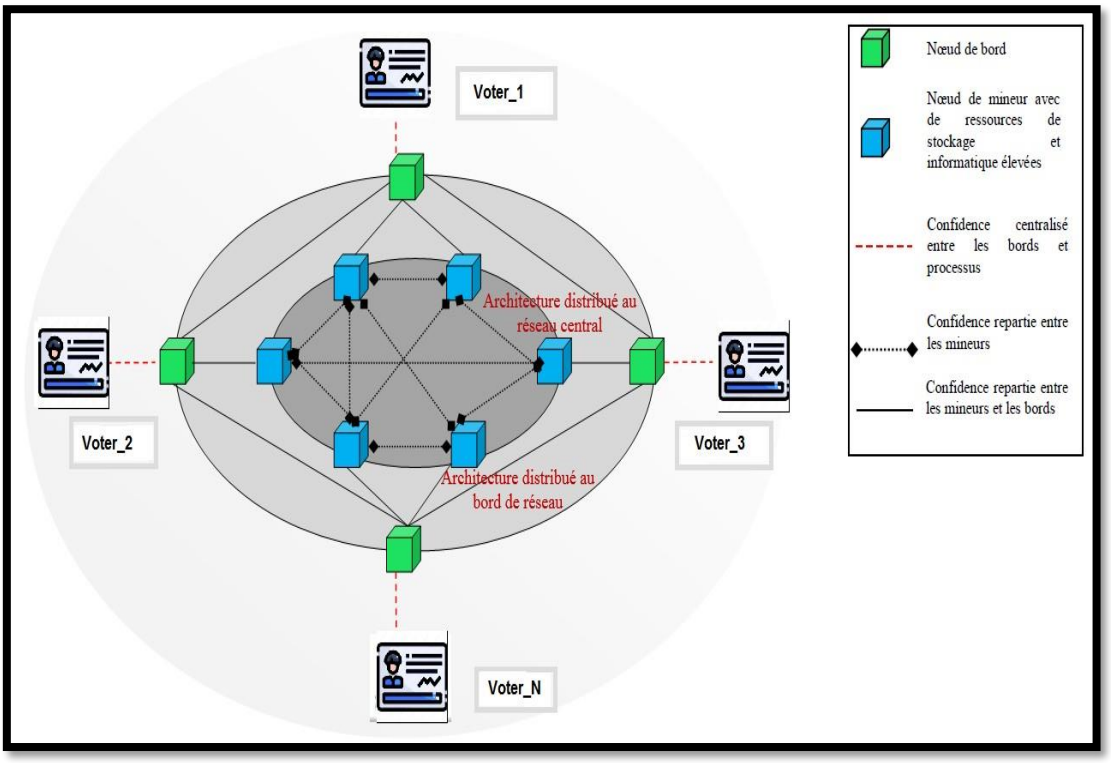


Figure 4.1 Architecture proposée pour le réseau de gestion des élections.

4.3.2 Workflow de modèle proposé

Dans la gestion de vote un grand volume de données est généré et nécessite un suivi en temps réel. Dans notre modèle proposé, les nœuds périphéries offrent un choix en temps réel. Le nœud périphérie a une capacité de stockage et de calcul limitée. Une fois les données choisissent, le nœud périphérie transfère les données cryptées choisi vers le réseau central. Le nœud mineur du réseau central validera et vérifiera le **PoW** et générera des blocs.

Pour garantir l'intégrité des données stockées dans le réseau central, nous utilisons une signature numérique et stockons des hachages dans une chaîne de blocs. Ces hachages dans la blockchain sont immuables et servent de preuves pour prouver l'intégrité des données.

La figure 3.2 illustre le flux de travail de notre modèle proposé.

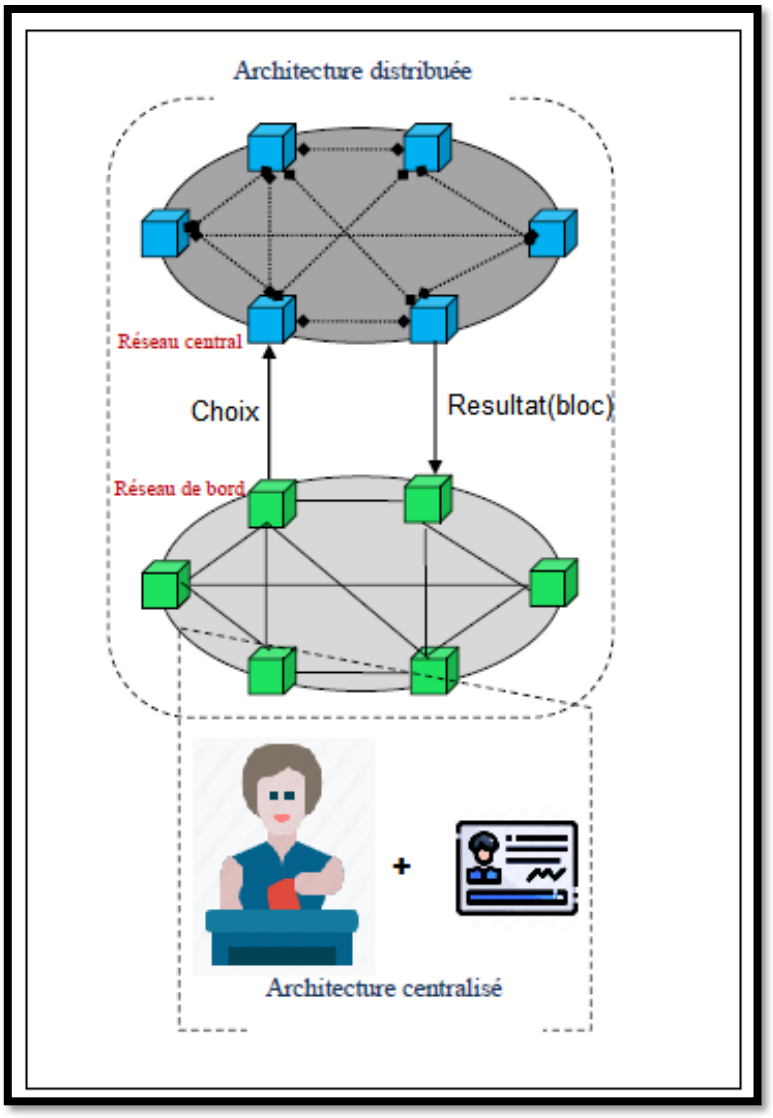


Figure 4.2 Architecture de workflow proposée

4.3.3 Processus de minage sur le réseau principal

Après avoir reçu une transaction sur le nœud principal du nœud périphérique, le processus d'extraction est lancé.

En raison de la limitation des ressources sur le nœud périphérique, nous exécutons le processus d'extraction sur le réseau principal dans le modèle proposé. Le processus d'extraction comprend les étapes suivantes :

- **Étape 1 :** chaque fois que le noeud périphérique affecter un choix, il envoie une demande de transaction à chaque mineur du réseau principal.

- **Étape 2 :** à la réception de la demande de transaction, le nœud mineur vérifie si la transaction est modifiée ou non et si la transaction existe ou non dans la chaîne de blocs. Si la transaction n'est pas modifiée et qu'elle n'existe pas dans la chaîne de blocs, le nœud mineur passe à l'étape 3. Sinon, il abandonne le processus d'exploration et diffuse le rapport dans le réseau central.

- **Étape 3 :** Dans cette étape, le nœud mineur récupère le hash de bloc précédent et lance le processus de POW.

  Dans le cas du bloc de genèse, le hash de bloc précédent est zéro. Le bloc de genèse est le premier bloc de la blockchain. Dans le processus de PoW, le nœud du mineur créera un nouveau bloc en hachant de manière itérative les informations, qui comprend le hash de bloc précédent, l'ID de bloc créé, la date et l'heure, la transaction vérifiée à l'aide de l'algorithme de PoW décrit ci-dessous.

- **Étape 4 :** une fois le bloc créé, pour garantir l'intégrité des informations de tous les blocs de la chaîne de blocs, les nœuds mineurs vérifient et vérifient tous les blocs existants.

- **Étape 5 :** lors de la dernière étape, le nœud mineur envoie une chaîne de blocs mise à jour à tous les nœuds de bord.

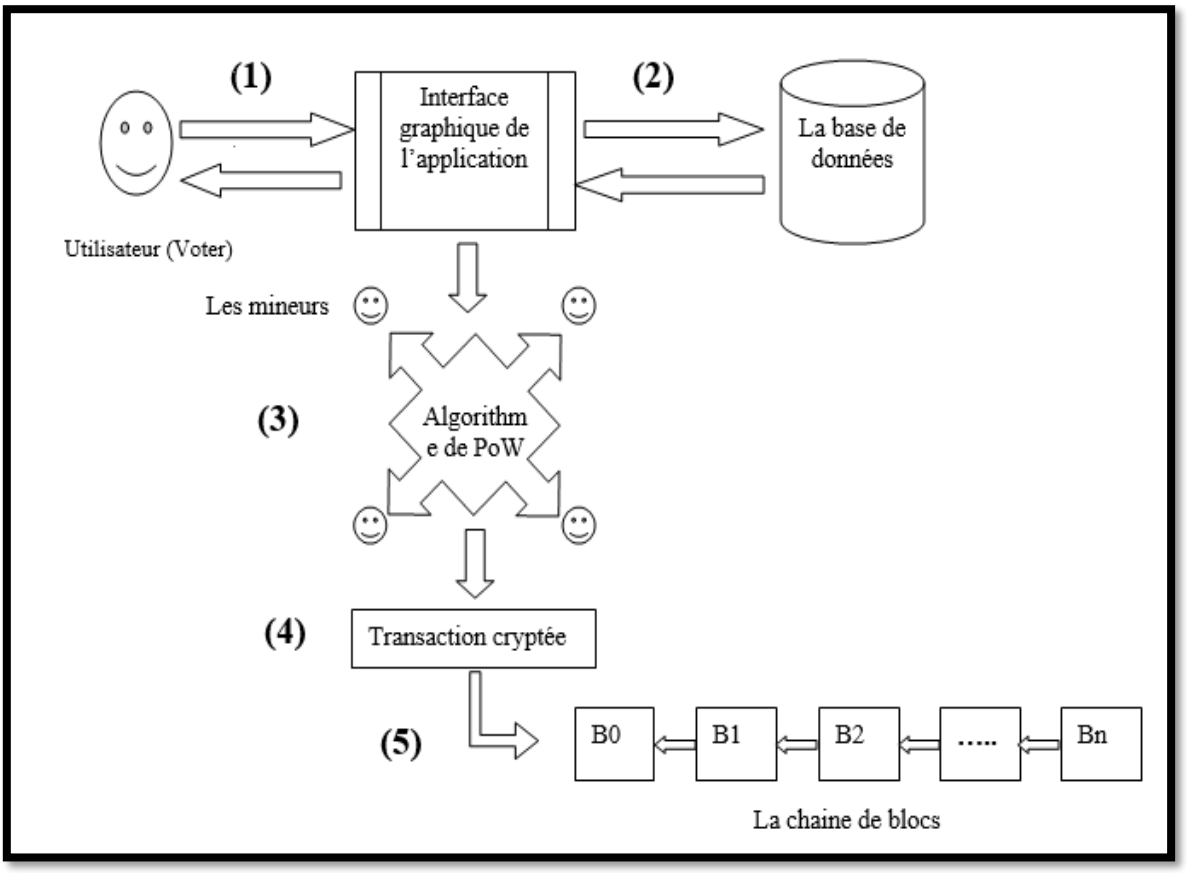


Figure 4.3 Fonctionnement de Processus de minage proposée

4.4 Cas d'utilisation

Dans notre cas d'étude nous avons choisi de suivi de simple vote à travers 3 candidats et un ensemble de mineurs et des électeurs.

4.4.1 Algorithme de PoW proposé

- **Étape 1 :** L'électeur utilise SHA-256 pour générer la valeur de hachage de son choix et signe leur hash avec sa clé privée.

- **Étape 2 :** L'électeur envoie son id de la carte, son choix, le temps de vote et sa signature aux mineurs de réseaux.

- **Étape 3** Le mineur vérifiera la signature avec la clé public de l'électeur et utilise SHA-256 pour générer la valeur de hachage, qui doit commencer par deux zéros (00) (La difficulté).

- **Étape 4 :** Lorsqu'un mineur atteint la valeur cible, il extrait le hash de block précèdent et crée un novelle bloc et le diffuse aux autres nœuds qui doivent confirmer mutuellement l'exactitude de la valeur de hachage.

4.5 Implémentation

4.5.1 Environnement de développement

- **Environnement et technologies logicielles**

a. Ressources matérielles

• Processeur	Intel ® core ™ i5
• Mémoire installe (RAM) :	4.00Go
• Type de système :	Système d'exploitation 64 bits

Tableau 4.2 Ressource matérielle

b. Ressources logicielles

• Système d'exploitation	Windows 10
• Editeur utilisée	Anaconda Jupyter Notebook

Tableau 4.3 Ressource logicielle

- **Langage utilisé**

Python est un langage de programmation interprété, de haut niveau et polyvalent. La philosophie de conception de Python met l'accent sur la lisibilité du code avec son utilisation notable d'espaces blancs importants. Ses constructions de langage et son approche orientée objet visent à aider les programmeurs à écrire un code clair et logique pour les projets à petite et grande échelle.

Dans notre implémentation nous avons choisi la version 3.6 de langage python

- **Outils utilisés**

SQLite est un système de gestion de base de données relationnelle (SGBDR) contenu dans une bibliothèque C. Contrairement aux serveurs de bases de données traditionnels, comme MySQL ou PostgreSQL, sa particularité est de ne pas reproduire le schéma habituel client-serveur mais d'être directement intégrée aux programmes. L'intégralité de la base de données (déclarations, tables, index et données) est stockée dans un fichier indépendant de la plateforme. L'accès à une base de données avec SQLite se fait par l'ouverture du fichier correspondant à celle-ci : chaque base de données est enregistrée dans un fichier qui lui est propre, avec ses déclarations, ses tables et ses index mais aussi ses données.

Cette caractéristique rend SQLite intéressante comme alternative aux fichiers textes, utilisés comme moyen de stockage intégré dans beaucoup d'applications. Dans notre implémentation nous avons choisi la version 3.

4.5.2 Présentation de l'application

1) Interface de login

La première interface affichée est l'interface de login / Registre (Figure 3.6), pour enregistrer, le votant (utilisateur) doit introduire son numéro de la carte national ainsi qu'un mot de passe, le système vérifie si le votant n'est pas déjà inscrit et que son numéro de la carte est valide , si la vérification est bonne les données sont enregistrées dans la base de données (Figure 3.7) est l'utilisateur obtient un wallet (Clé privé + Clé public) pour assurer les autres fonctionnalités de système (Figure 3.8), sinon un message d'erreur est affiché (Figure 3.9).

Figure 4.4 Interface login /Registre

2) Base de données des électeurs

La figure suivante montre un tableau de base de donnes des utilisateurs qui est composé de trois champs :

- **Id_Cart :** Numéro de la carte nationale d'utilisateur
- **Pkey :** Le clé public de électeurs générer par le système
- **Statut :** une valeur binaire : 'not yet' c.-à-d. que le voter n'est pas voter encore, 'voted' c.-à-d. que l'utilisateur a donné son choix.

	id_cart	pkey	statut
	Filtre	Filtre	Filtre
5	8457956125	7a1ed7d483c0152c08124cb187d2a22e	not_yet
6	7451263215	c7181e1fa4869987d807de6561fa118f	not_yet
7	2145125986	6a0735739c74aea6962aca0004d89ca6	not_yet
8	8745125693	1bd3e7d434d23258c2402fbe52b90a7f	not_yet
9	1245879543	00306caa7f0a530cdc0c514717a3eda6	not_yet
10	21145451546316	4ea791dbd3151c5e8dce14410eb6888b	not_yet
11	1236598651	3378321cf37770342d4c472bbcd01267	not_yet
12	000325698	7e5edbf81e4e8237e010e1fc39744426	not_yet
13	4487595689	c14343a0eefb1278d5ff5979eb2f5ccd	not_yet
14	2565485478	c28f5fd8195c01f2bbd149555a6bf542	not_yet
15	1212121212	55b6acab16b69464390d51150d7843f9	not_yet
16	6985654785	ecf2ef311a77d49e1ee6100ba2de42fb	not_yet
17	7845495686	21899eff94785d4a9c2c4efd135ba920	not_yet
18	1452368759	55c775a72d4dbb5d313b014d72e8ad...	not_yet
19	7789564589	28347c140a308c1ab60423c682f09107	voted

Figure 4.5 Interface de base de données des utilisateurs

3) La wallet électronique :

La figure suivante montre un message (pop-up) qui contient les clés du votre après ca inscription

Figure 4.6 Les données de wallet (Clé privé +Clé public)

4) Message d'erreur

Un message(pop-up) d'erreur est affiché si l'utilisateur veut falsifié les donnes dans le système.

Figure 4.7 Interface de message d'erreur

5) Interface de vote

Aprés le login de l'utilisateur une interface de vote est affichée, l'interface est composée de 3 candidats (Figure 3.11), 3 bouttons de vote et aussi 3 compteurs. A travers cette interface l'utilisateur peut choisir un est un seul candidat. Le système vérifiera si le votant n'a pas voter encore, si la vérification est bonne l'interface de minage est affichée (Figure 3.12).

6) Base de données des candidats

La figure 3.11 suivante est le premier tableau crée dans la base de données, dans cette étape nous avons choisi 3 candidats :

1. **candidat_A,**
2. **candidat_B ,**
3. **candidat_C .**

Nous avons attribué à chaque candidat une adresse (clé public) , le dernier champ dans le tableau est un compteur pour le nombre de votant.

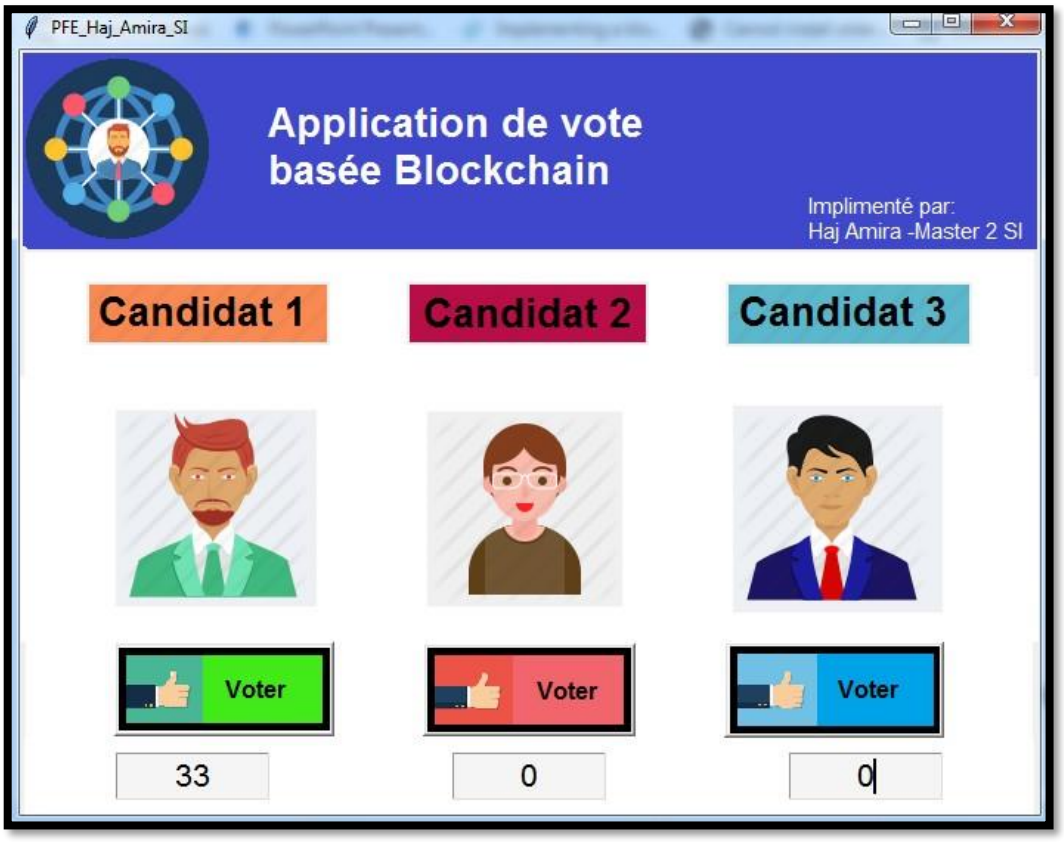


Figure 4.8 Interface de vote

	Name	adress	votes
	Filtre	Filtre	Filtre
1	Candidat_A	2c32ac8a61d718888dc9ffdd86eabf36	18
2	Candidat_B	d6ba9473a2585b3665e050b2005383bb	0
3	Candidat_C	67e86618140538e67b294c71c5e0d4a7	0

Figure 4.9 Base de données des candidats

7) Le minage

Aprés que le votant a effectué son choix, une nouvelle partie d'interface est affichée, cette partie affiche un message de choix du votant et affiché, aussi cette interface contient une bouton (Miner le bloc) , pour que l'utilisateur veut valider leur choix il clique sur cette bouton et le processus de minage sera commencé.

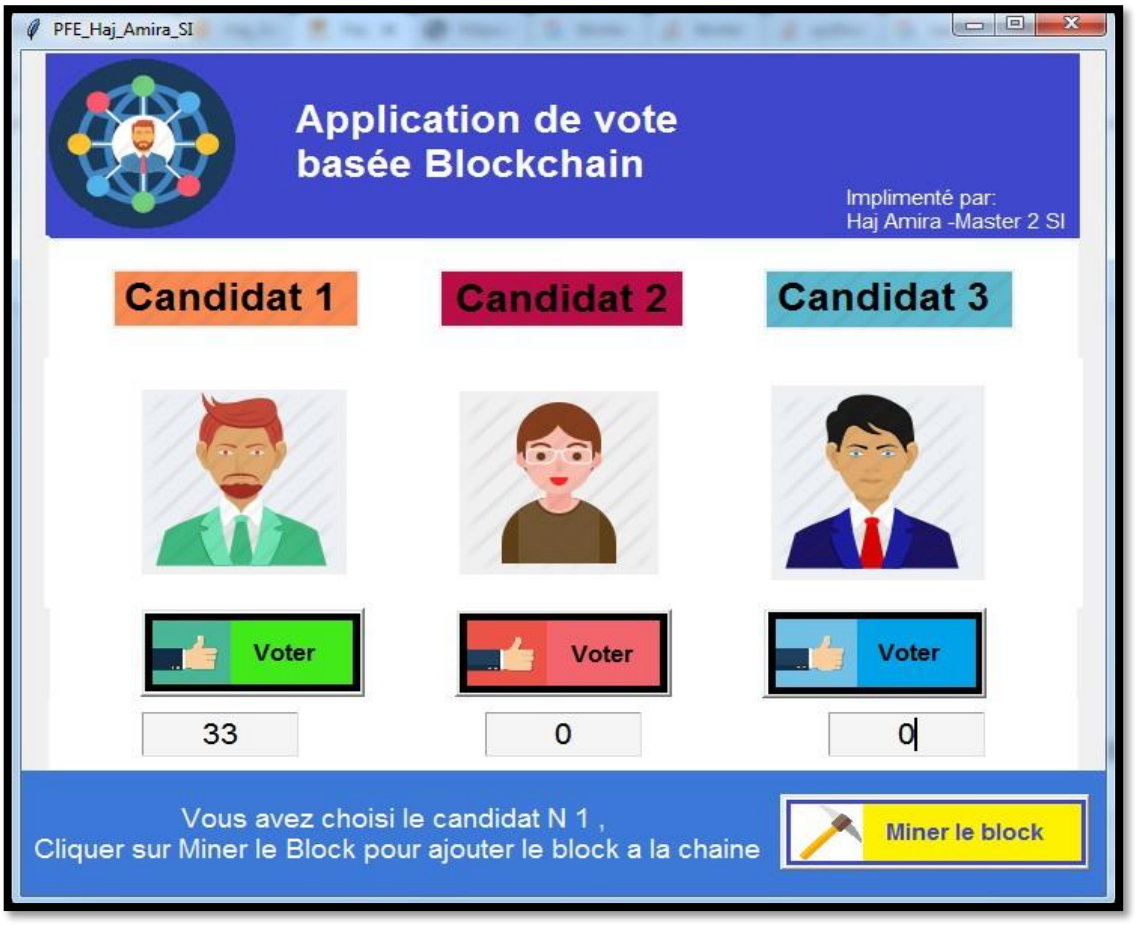


Figure 4.10 L'interface de minage

8) Historique de minage

Maintenant le minage a commencé, les mineurs sont entrain de résoudre le puzzle, à chaque fois que un mineur clacule un hash , il le affiche jusqu'à l'arrivation au bon hash , à ce point, les données de novelle bloc est affiché (hash de code précèdent, l'index, la transaction , le nonce , le timestamp) et le bloc est ajouté dans la base de données (Figure 3.12) et les résultat sont affichés pour tout les membre de réseau blockchain .

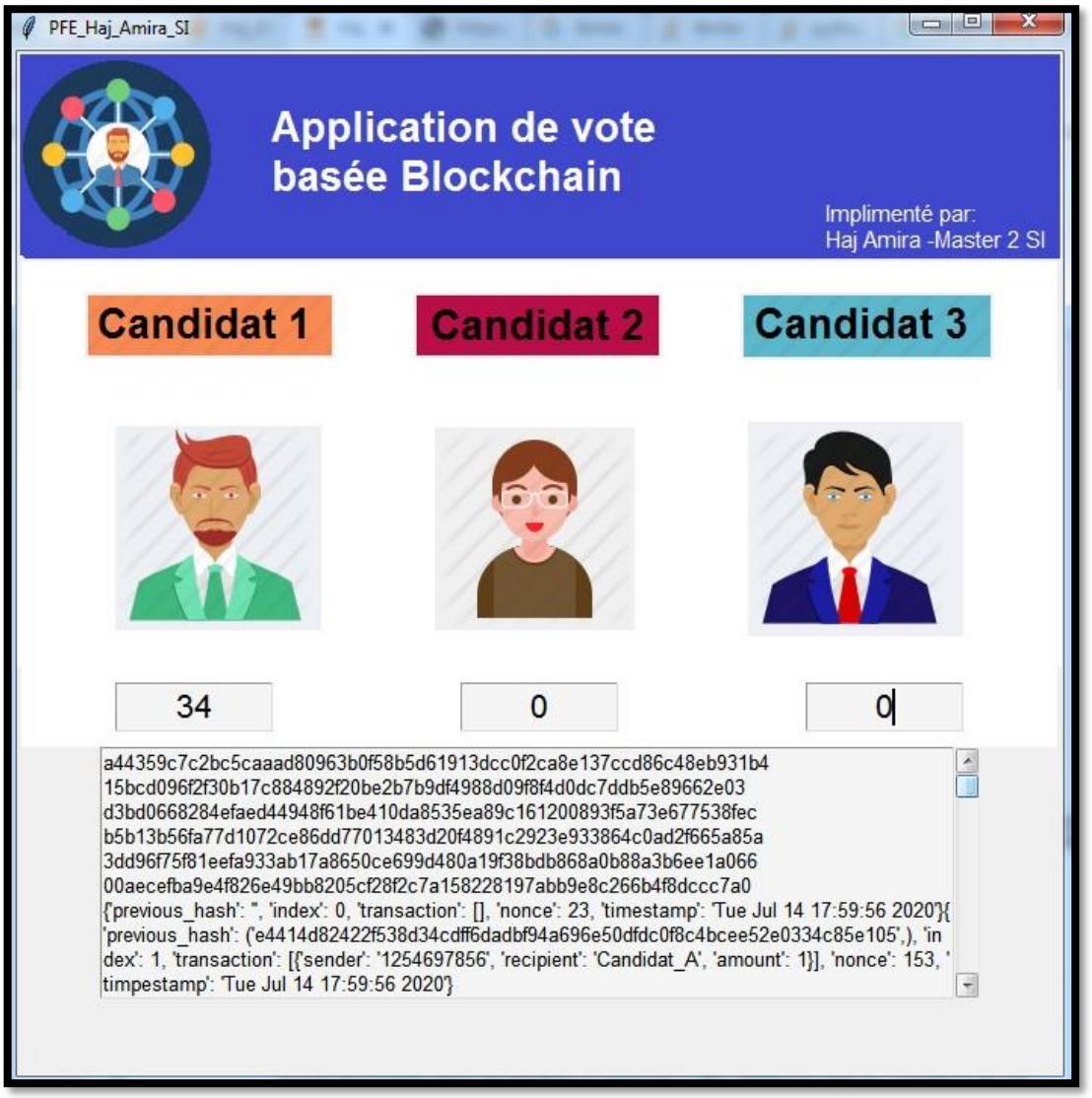


Figure 4.11 L'interface de l'historique de minage

9) Base de donnes de bloc

Le tableau suivant montre les données des blocs, il est composé de 4 champs :

- **Time :** c'est le temps de validation de transaction
- **Phash :** c'est le hash de bloc précèdent, en remarque les couleur (rouge , vert et bleu) dans le tableau montre que chaque novelle hash de bloc il est considéré comme un hash précèdent pour la nouvelle bloc au future
- **Hash :** c'est le hash de la nouvelle transaction
- **Transactions** : il est composé de l'id de voter, l'adresse de candidat choisit

	indexe	time	phash	hash	transactions
	Filtre	Filtre	Filtre	Filtre	Filtre
1					
2	2	Mon Jul 13 22:35:00 2020		cea410d06921cdf0fb1f578f0b92e3dba0d9c081b4...	
3	2	Tue Jul 14 21:09:04 2020	cea410d06921cdf0fb1f578f0b92e3dba0d9c081b4...	87f9b7e4f1bfcf9f1ce77a6a2c3256d4b5f1f0cad7a...	sender : 123657895 , receiver: Candidat_A
4	2	Tue Jul 14 21:09:14 2020	87f9b7e4f1bfcf9f1ce77a6a2c3256d4b5f1f0cad7a...	1bdd26e54566f7386c8b857d92a82cc52d7ac97ff5...	sender : 1254697623 , receiver: Candidat_B
5	2	Tue Jul 14 21:10:27 2020	1bdd26e54566f7386c8b857d92a82cc52d7ac97ff5...	264e6a515c6c0bfae074118a2323444ef09ee7109...	sender : 8457956125 , receiver: Candidat_C

Figure 4.12 Base de données des blocs

Nous remarquons que le premier bloc (en violet) n'a pas de phash , aussi pour les données du bloc le nonce est ajouté mais nous avons choisi de ne pas stockée dans la base de données.

4.6 Résultats et discussion

Nous avons mis en place **une preuve de concept (PoC)** et nous avons eu l'idée d'appliquer la technologie blockchain à la gestion d'élection afin de prouver son utilité. A la fin de ce travail, nous avons pu constater les avantages suivants :

- ✓ **La sécurité et la transparence :**

  Nous avons suggéré un système de vote électronique basé sur la blockchain. Le système est sécurisé à l'aide de l'algorithme de PoW et totalement transparent. Tout électeur inscrit pourra voter en utilisant n'importe quel appareil connecté à Internet. La blockchain sera vérifiée publiquement et distribuée d'une manière que personne ne peut gâcher.

- ✓ **Surveillance précise des flux de vote :**

  En téléchargeant les informations sur les flux de vote vers l'application on obtient une base de données verrouillée et sécurisée à partir de laquelle, à tout moment et avec une fiabilité absolue, on peut identifier la source des votes, ainsi suivre des changements de statut et de propriété des votes au cours de processus d'élection.

- ✓ **Nouvelle opportunité gouvernementale :**

  La technologie Blockchain permet la mise en œuvre complète de vote électronique, en introduisant une nouvelle solution technologique, avec une efficacité accrue et en créant de nouveaux emplois.

- ✓ **Recherche & Développement :**

  Il offre la possibilité de surveiller la mise en œuvre et les ajustements de la réglementation liés à la gestion des d'élection et permettant de mieux comprendre le développement de nouvelles technologies soutenant la transparence de processus de vote ,mais aidant également à sensibiliser le public aux avantages de l'utilisation de ce modèle .

.

Cependant, l'un des inconvénients de notre système de vote est l'impossibilité de modifier un vote en cas d'erreur de choix. L'utilisateur ne pourra voter qu'une seule et une seule fois.

4.7 Conclusion

Ce présent chapitre a été consacré aux différents outils ayant contribués à l'aboutissement de ce projet. On a détaillé le système proposé et son fonctionnement (architecture, les transactions,
…etc.) a été mise en évidence. Nous avons présenté aussi l'implémentation du système ainsi que les différents langage et outils utilisé. Enfin nous avons conclu par le service qui permettre de contrôler le processus d'élection.

CONCLUTION GÉNÉRALE & PERSPECTIVES

La blockchain est utilisée pour créer la confiance dans deux dimensions : l'origine de l'information et son instabilité (intégrité dans le temps).

Il est utile de comprendre les chaînes clés dans le contexte de Bitcoin, mais surtout, ne supposez pas que tous les écosystèmes blockchain ont besoin de mécanismes tels que le travail à l'épreuve de Bitcoin, la règle de la chaîne la plus longue. D'autre part, des enregistrements distribués et des chaînes spéciales peuvent être déployés pour résoudre d'autres problèmes. Comme toujours, chaque solution présente des avantages et des inconvénients et doit être considérée individuellement pour chaque cas d'utilisation.

L'intégration de la blockchain permettra de mieux protéger la vie privée en contrôlant l'accès à ses données.

À une époque où la technologie de blockchain évolue, elle peut être perçue comme une opportunité de restaurer des utilisateurs horizontaux sur le réseau, en créant des fournisseurs de services réels et des utilisateurs de services en même temps via une approche d'égal à égal. La procédure publique a tous les avantages de profiter de cette possibilité pour s'assurer que les enregistrements des opérations ou des biens sont conservés avec le service de contrôle,

Dans les projets gouvernementaux tels que le système d'élection. Cette évolution améliorera non seulement le processus de suivi, mais facilitera également le contrôle du processus, ce qui conduira à un fonctionnement efficace ainsi aux contrôleurs d'assurer un suivi et un contrôle des responsabilités.

Enfin, bien qu'il n'existe pas encore de solution parfaite, l'adoption de technologies telles que Blockchain pour accroître la transparence de la gestion des d'élections renforcera la fiabilité du processus dans son ensemble. En outre, cela réduira les tâches

fastidieuses, manuelles et répétitives pour les autres parties prenantes, à condition que les clés de cryptage soient utilisées sous le contrôle de l'utilisateur.

En premier lieu, nous avons commencé par une introduction générale ainsi que notre problématique, nous avons donné une vue globale sur la technologie blockchain, ensuite, nous avons présenté la cryptographie derrière la blockchain, démystifier la blockchain leur architecture, caractéristiques et domaines d'application. Par la suite, nous avons abordé la gestion de vote et les technologies déjà utilisée pour garder la trace de vote dans lesquelles nous avons présenté un état de l'Art de gestion de vote électronique deux grandes.

Pour conclure, nous tenons à préciser que notre contribution comporte deux parties essentielles :

1. Nous avons proposé une nouvelle architecture pour suivi les votes sur l'algorithme de Pow.

2. Nous avons également implémenté notre architecture à l'aide d'un ensemble des outils et en langage python

Comme perspective, nous envisageons de raffiner notre étude à travers les points suivants :

1. Implémenter une application mobile pour scanner et lire les QR code, pour faciliter le processus de vote implémentée dans cette mémoire.

2. Introduire la notion des smart contracte de Blockchain et d'essayer d'implémenter un système basé sur cette technologie.

Références

LOFTI , 2017 : LOTFI, I. 2017. Cryptographie à base de courbes elliptiques : https://www.researchgate.net/publication/323946296_Cryptographie_a_base_de_courbes_elliptiques

Eyal et al., 2016 : EYAL, I., GENCER, A. E., SIRER, E. G. & VAN RENESSE, R. Bitcoin-ng: A scalable blockchain protocol. 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), 2016. 45-59.

Ølnes et al., 2017 : ØLNES, S., UBACHT, J. & JANSSEN, M. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Elsevier

Gaetani et al., 2017 : GAETANI, E., ANIELLO, L., BALDONI, R., LOMBARDI, F., MARGHERI, A. & SASSONE, V. 2017. Blockchain-based database to ensure data integrity in cloud computing environments.

Gervais et al., 2016 : GERVAIS, A., KARAME, G. O., WÜST, K., GLYKANTZIS, V., RITZDORF, H. & CAPKUN, S. On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016. ACM, 3-16.

Atzori, 2015 : ATZORI, M. 2015. Blockchain technology and decentralized governance: Is the state still necessary? Available at SSRN 2709713.

Swan, 2015 : SWAN, M. 2015. Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc.".

Leloup, 2017 : LELOUP, L. 2017. Blockchain: la révolution de la confiance, Editions Eyrolles.
Antonopoulos, 2014 : ANTONOPOULOS, A. M. 2017. Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc."

Lopez and Dahab, 2000 : LOPEZ, J. & DAHAB, R. 2000. An overview of elliptic curve cryptography.

Narayanan et al., 2016 : NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. &

GOLDFEDER, S. 2016. Bitcoin and cryptocurrency technologies. s Princeton University Press.

BELFEDHAL, 2016 : BELFEDHAL, A. E. 2016. Etude et Implémentation des Fonctions de Hachage Cryptographiques Basées sur les Automates Cellulaires.

BASHIR , 2017 : BASHIR, I. 2017. Mastering blockchain, Packt Publishing Ltd.

Casino et al., 2018 : CASINO, F., DASAKLIS, T. K. & PATSAKIS, C. 2018. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics.

Zheng et al., 2017 : ZHENG, Z., XIE, S., DAI, H., CHEN, X. & WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 2017. IEEE, 557-564.

Hannesse et al : HANNESSE, T., DE HERTAING, A. R. & DE BROQUEVILLE, O. Les banques doivent-elles craindre les blocktechs* et leur technologie blockchain?

Leloup, 2017 : LELOUP, L. 2017. Blockchain: la révolution de la confiance, Editions Eyrolles.

Wright & De Filippi, 2015 : DE FILIPPI, P. & LOVELUCK, B. 2016. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Review, 5.

Antonopoulos, 2014 : ANTONOPOULOS, A. M. 2017. Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc.".

Eyal et al., 2016 : EYAL, I., GENCER, A. E., SIRER, E. G. & VAN RENESSE, R. Bitcoin-ng: A scalable blockchain protocol. 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), 2016. 45-59.

Enguehar et al., 2019 : Enguehard, Chantal. "Blockchain et vote électronique." Terminal. Technologie de l'information, culture & société 124 (2019).

Apleasant , 2013 : Common Electronic Voting and Counting Technologies **;**https://www.ndi.org/e- voting-guide/common-electronic-voting-and-counting-technologies ; December 17, 2013

Sue, 2018 : Sue Halpern , Election-Hacking Lessons from the 2018 Def Con Hackers Conference ; https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers conference

Smartmatic, 2016 : Smartmatic – Cybernetica Centre of Excellence for Internet Voting, IBM Research Zurich, University of Tartu (UT), Technical University Eindhoven, University of Salerno, GRNET, University of Edinburgh, Guardtime AS and GUNET.

Votem , 2017 : http://www.votem.com/wp-content/uploads/2016/11/The-Future-of-Voting-Study.pdf

Voatz,2018 : https://voatz.com/faq.html

Irene Solaiman , 2018 : https://www.belfercenter.org/publication/defending-vote-casting-using-blockchain-based-mobile-voting-applications-government.