République Algérienne Démocratique et Populaire

Ministre de L'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE A. MIRA-BEJAIA

FACULTE DES SCIENCES EXACTES

DEPARTEMENT INFORMATIQUE

MEMOIRE DE FIN DE CYCLE

En vue de l'obtention du

Diplôme de Master en Informatique

Option : Intelligence Artificielle

Thème

Utilisation du clustering pour le processus de validation dans une blockchain

Présenté par :

M BEGAG Issam Mahdi

M HERFOUCHE Omar

Encadré par :

M^me YAICI Malika

Devant membre de jury :

Présidente : M^me GHANEM Souhila.

Examinateur : M OUZEGGANE Redouane.

Promotion : 2022-2023

REMERCIEMENTS

Avant tout, louanges et remerciements au Dieu Tout-Puissant pour ses bénédictions tout au long de notre travail de recherche pour mener à bien ce projet.

Nous tenons à exprimer notre profonde et sincère gratitude à notre encadreur, le Dr Yaici Malika, pour son soutien continu pour sa patience et sa motivation. Elle nous'a aidé pendant tout le temps de la recherche et de la rédaction de ce mémoire.

Travailler avec vous a été un tel honneur.

Nous tenons à remercier vivement les membres du jury d'avoir consacrer de leur temps à la lecture de ce manuscrit, et d'accepter de juger et d'évaluer ce travail.

Une grande partie du mérite revient à nos parents qui nous'ont soutenu, encouragé non seulement dans cette thèse mais à chaque étape de notre vie, vous éclairez notre vie de votre présence et rien ne pourrons jamais vous remplacer, qu'Allah vous préserve et vous protège.

Enfin, nous tenons à remercier notre frères et sœurs, nos amis et tous ceux qui ont contribué, même avec les plus petits efforts, à la réalisation de ce projet.

BEGAG Issam Mahdi

HERFOUCHE Omar

Table des matières

Table des figures

INTRODUCTION GÉNÉRALE

La technologie blockchain a émergé comme une innovation majeure dans le domaine de la gestion des données et des transactions décentralisées. Elle offre des possibilités passionnantes pour sécuriser et valider les échanges de manière transparente et efficace. Ce mémoire se concentre sur l'étude et l'exploration de différents aspects de la blockchain, en mettant l'accent sur la validation des transactions et les algorithmes de consensus, ainsi que sur l'utilisation du clustering pour optimiser les performances de la blockchain.

Nous proposons dans ce mémoire une nouvelle approche pour améliorer la validation dans la blockchain.

Nous avons divisé notre mémoire en quatre chapitres. Dans le premier chapitre nous offrons une introduction générale à la technologie blockchain. Nous explorons les principes de base de la blockchain, en mettant l'accent sur son fonctionnement décentralisé et sa capacité à enregistrer des transactions de manière transparente et immuable. Nous examinons également les avantages et les défis de l'utilisation de la blockchain dans différents secteurs.

Dans le deuxième chapitre, nous nous penchons sur la validation des transactions dans la blockchain. Nous étudions les mécanismes de validation utilisés pour garantir l'intégrité et la sécurité des transactions. Nous analysons en détail les algorithmes de consensus tels que la preuve de travail, la preuve d'enjeu et d'autres approches émergentes. Nous examinons leurs caractéristiques, leurs avantages et leurs limitations, ainsi que leur impact sur la résilience et la scalabilité du réseau blockchain.

Dans le troisième chapitre, on se concentre sur l'utilisation du clustering dans la blockchain. Nous explorons comment cette technique peut être appliquée pour optimiser les performances du réseau. Nous examinons les différentes approches de clustering utilisées. Nous discutons également des implications du clustering sur la sécurité, la répartition des charges et la gestion des ressources dans la blockchain.

Enfin, dans le quatrième chapitre, nous proposons une proposition novatrice pour améliorer la validation dans la blockchain. Nous présentons une approche basée sur l'utilisation d'un algorithme de consensus et l'application de techniques de clustering. On termine ce rapport par une conclusion et des perspectives.

CHAPITRE 1

GÉNÉRALITÉS SUR LES BLOCKCHAINS

Introduction

La Blockchain est une technologie qui permet le stockage et l'échange d'information de manière décentralisée et sécurisée. Dans ce chapitre nous allons présenter un aperçu sur la blockchain : L'évolution, la propre définition et les notions de base reliées à cette technologie.

1.1 Définition

La blockchain est une technologie de stockage et de transmission de données, qui repose sur le principe du pair à pair (P2P). Elle permet de sécuriser et de valider des transactions de manière décentralisée et transparente, sans avoir besoin d'un tiers de confiance centralisé.

La blockchain est un registre public décentralisé, sécurisé et immuable de toutes les transactions effectuées sur le réseau. La blockchain utilise des algorithmes cryptographiques pour assurer la confidentialité, l'intégrité et la validation des données stockées dans la chaine de blocs [24].

1.2 Historique de la blockchain

La blockchain est une technologie relativement récente qui a été créée en 2008 par une personne (ou un groupe de personnes) sous le pseudonyme de Satochi Nakamoto [24]. Elle a été conçue pour servir de base au fonctionnement de la cryptomonnaie Bitcoin.

La blockchain a connu une adoption rapide et a été utilisée pour créer de nombreuses autres cryptomonnaies, ainsi que pour des applications dans divers domaines.

- 1991 : Stuart Haber et W.Scoott Stornita ont introduit le concept de blockchain et ont travaillé sur une chaine sécurisée de cryptomonnaie ou personne ne pouvait altérer les horodatages des documents.
- 2008 : Publicatio du livre blanc de Bitcoin par Satoshi Nakamoto, introduisant le concept de la blockchain [23].
- 2009 : Lancement du réseau Bitcoin, la première blockchain publique, utilisée pour les transactions en cryptomonnaie [23].
- 2014 : Lancement de la blockchain Ethereum, une blockchain programmable qui permet la création de contrats intelligents.
- 2015 : Création de la fondation Ethereum pour soutenir le développement de la blockchain Ethereum [23].
- 2017 : L'année de l'explosion de la blockchain, avec une forte augmentation de la capitalisation boursière des cryptomonnaies et une adoption croissante de la technologie blockchain dans de nombreux domaines.

- 2021 : Lancement de la blockchain Cardano, une blockchain de troisième génération qui vise à être plus évolutive et plus durable que les générations précédentes.

1.3 Architecture pair à pair (P2P)

Est une architecture informatique décentralisée dans laquelle chaque nœud du réseau est à la fois un client et un serveur. Contrairement à l'architecture client-serveur traditionnelle, ou les clients demandent des ressources à des serveurs centralisés, les nœuds du réseau P2P interagissent directement les uns avec les autres pour partager des ressources, des données ou des informations [24].

1.4 Structure d'une Blockchain

1.4.1 Bloc

Chaque bloc contient un ensemble de transaction, ainsi qu'un en-tête qui inclut un identifiant unique, un horodatage et une référence au bloc précédent. Les blocs sont ajoutés à la chaine de blocs dans un ordre chronologique, créant ainsi une chaine de blocs immuable. (Voir figure 1)

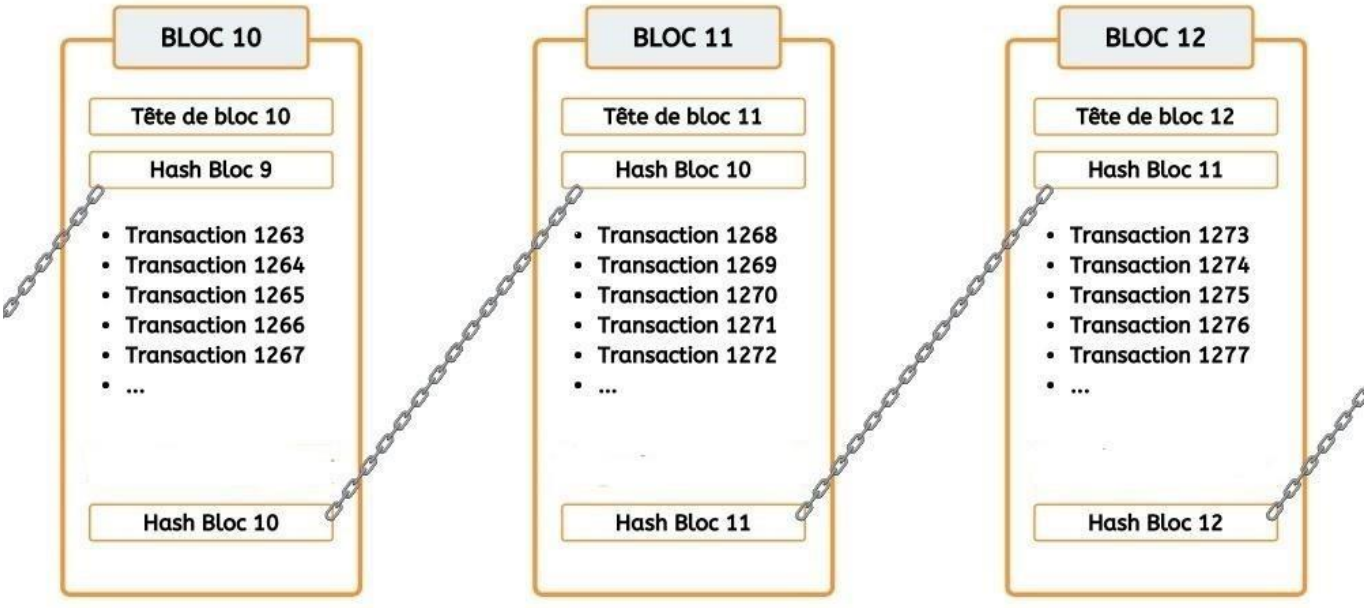

Figure 1.1: Enchainement des blocs[18] .

1.4.2 Mineurs

Les mineurs sont des validateurs qui participent au processus de validation des transactions et de création de nouveaux blocs. Ils sont récompensés par une quantité de crypto-monnaie pour leur travail selon l'organisation de blockchain.

1.4.3 Transactions

Chaque transaction est un échange de données ou de valeur entre deux parties. Les transactions sont vérifiées et validées par les mineurs ou les nœuds du réseau, qui s'assurent que chaque transaction est légitime et conforme aux règles du protocole de la blockchain.

1.4.4 Nœuds

Les nœuds sont des ordinateurs qui stockent une copie de la chaine de blocs et qui participent à la validation de transactions.

1.5 Fonctionnement de la Blockchain

Pour une première approche du fonctionnement des blockchain, le plus facile est de raisonner avec une blockchain purement monétaire. On peut prendre l'exemple de bitcoin, ou d'une blockchain avec de jetons (simples), en commençant par la création d'une transaction peut etre décrit en quelque étapes (voir la figure 2)

1. Un compte (ou portefeuille, portemonnaie, wallet) doit etre créé pour qu'un utilisateur de blockchain puisse envoyer ou recevoir des crypto-monnaie.**A** utilise son portefeuille et effectue une transaction vers **B**. cette transaction est diffusée sur le réseau.

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

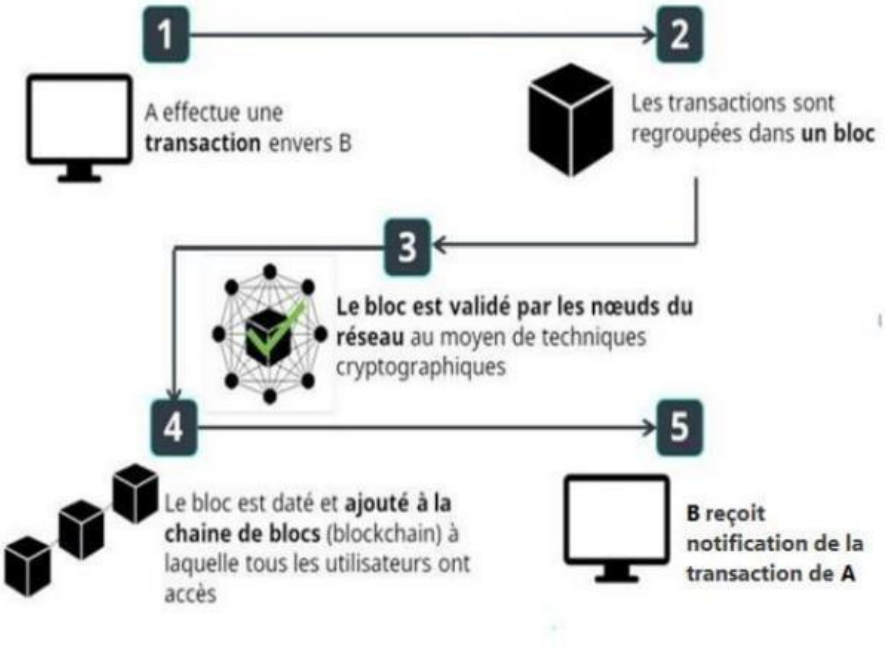

Figure 1.2: fonctionnement d'une blockchain [20] .

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

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

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

1.6 Types de Blockchain

Les systèmes de blockchain actuels peuvent etre grossièrement classées en trois types : les blockchain publiques, les blockchain privées et les blockchain de consortium.

- **Blockchain publique**

  Une blockchain publique est ouverte à tous et n'a pas de contrôle centralisé. Toutes les transactions sont transparentes et vérifiables, et les utilisateurs peuvent participer au processus de validation des transactions.

  Les blockchain publique sont considérées comme hautement sécurisées car elles sont décentralisées et résistantes aux attaque malveillantes, car toutes les transactions sont visibles publiquement, ce qui favorise la confiance et la traçabilité [15].

- **Blockchain privée**

  Une blockchain privée est contrôlée par une organisation ou un groupe restreint d'utilisateurs qui ont un accès exclusif aux données. Les transactions ne sont pas publiques et ne sont accessibles qu'aux parties prenantes.

  Les bockchains privées offrent un plus grand degré de confidentalité et de sécurité des données, car seuls les utilisateurs autorisés peuvent accéder à la chaine de blocs et voir les transactions. Cela rend également les blockchain privées plus rapides et plus évolutives que les blockchains publiques, car elles n'ont pas besoin de résoudre les problèmes mathématiques complexes nécessaires à la validation des transactions [15].

- **Blockchain consortium (communautaire)**

  Une blockchain consortium est gérée par un groupe de plusieurs organisations qui se mettent d'accord sur les règles de la blockchain.

  Les blockchains de consortium offrent un compromis entre la confidentialité et la transparence, car elles permettent aux participants de maintenir un certain niveau de confidentialité tout en permettant une certaine visibilité et transparence entre les membres du consortium. Les membres du consortium peuvent donc bénéficier des avantages d'une blockchain privée, tels que la rapidité et l'efficacité, tout en conservant certains avantages d'une blockchain publique, tels que la sécurité et la transparence [9].

- **Blockchian hybride**

  Une blockchain hybride combine des éléments de blockchain publique et privée. Les transactions peuvent être publique ou privées en fonction des besoins des utilisateurs.

1.7 Exemple de Blockchain

1.7.1 Bitcoin

Le bitcoin est le première cryptomonnaie créée en 2009 et la plus connue des applications de la technologie de la blockchain. Il s'agit d'une cryptomonnaie décentralisée, qui utilise une blockchain publique pour gérer les transactions en toute sécurité et en toute transparence.

Le bitcoin n'est pas contrôlé par une banque centrale ou une institution financière centrale. Au lieu de cela, les transactions sont vérifiées par des mineurs, qui résolvent des problèmes mathématique complexes pour ajouter des blocs à la chaine de blocs et valider les transactions. En récompense de leur travail, les mineurs reçoivent des bitcoins [3].

1.7.2 Ethereum

Ethereum est une plateforme open source basée sur la technologie de la blockchain. Elle permet de créer des applications décentralisées et des contrats intelligents (smart contracts) de manière autonome, sans recourir à une tierce partie pour en assure la gestion et la sécurité.

Ethereum utilise une blockchain publique, comme le bitcoin, mais il s'agit d'une blockchain programmable qui offre davantage de fonctionnalités. Elle permet notamment la création de tokens (jetons) personnalisés, la gestion des identités numérique et l'exécution de contrats intelligents complexes.

La plateforme Ethereum utilise une cryptomonnaie appelée ether (ETH) comme moyen de paiement pour les transactions [3].

1.7.3 Ripple

Ripple est une plateforme de paiement qui vise à faciliter les transferts de fonds transfrontaliers. Contrairement à la plupart des autre blockchain, Ripple n'est pas une blockchain publique, mais une blockchain privée, controlée par l'entreprise Ripple Labs.

La blockchain Ripple utilise sa propre cryptomonnaie, appelée XRP, qui peut être utilisée pour effectuer des transactions sur la plateforme. Cependant, l'objectif principal de Ripple est de fournir une infrastructure de paiement efficace pour les banques et

autres institutions financières.

La technologie de Ripple permet des transferts de fonds quasi instantanés, ce qui réduit les délais et les coûts associés aux transferts transfrontaliers traditionnels. Ripple a également développé un système de règlement brut en temps réel appelé RippleNet, qui permet aux banques et aux institutions financières de traiter des paiements en tempsréel.

1.8 Evolution de Blockchain

1.8.1 Blockchain 1.0

La blockchain 1.0 est la première génération de blockchains qui s'est concentrée sur la création de cryptomonnaies décentralisées telles que Bitcoin. Les blockchains 1.0 sont caractérisées par un réseau décentralisé de nœuds qui vérifient et valident les transactions, ainsi que par l'utilisation de techniques cryptographiques pour assurer la sécurité. Les transactions sur les blockchains 1.0 sont généralement anonymes et ne nécessitent pas d'informations personnelles. Cependant, les blockchains 1.0 sont limitées aux transactions financières et ne permettent pas la création de contrats intelligents ou d'applications décentralisées. En somme, la blockchain 1.0 a jeté les bases de l'utilisation de la technologie blockchain et a permis la création des premières cryptomonnaies décentralisées [8].

1.8.2 Blockchain 2.0

La blockchain 2.0, également appelée blockchain intelligente, est une évolution de la première génération de blockchains (la blockchain 1.0) qui a introduit les contrats intelligents. Les contrats intelligents permettent l'automatisation de l'exécution de transactions financières et de processus d'affaires, tout en évitant les erreurs humaines et en réduisant les coûts.

Les blockchains 2.0 offrent également une sécurité renforcée grâce à la technologie de consensus distribué qui assure la validation et la vérification des transactions parun réseau décentralisé de nœuds. De plus, les blockchains 2.0 sont conçues pour être interopérables, ce qui signifie qu'elles peuvent communiquer entre elles pour partager des données et des informations.

En somme, la blockchain 2.0 a apporté de nombreuses améliorations à la première

génération de blockchains, notamment en permettant la création de contrats intelligents, d'applications décentralisées et de jetons personnalisés, tout en offrant une sécurité renforcée et une interopérabilité entre les différentes blockchains [8].

1.8.3 Blockchain 3.0

La blockchain 3.0 est la dernière évolution de la technologie de la blockchain. Cette génération de blockchains est axée sur l'amélioration de la vitesse, de l'évolutivité, de la sécurité et de la facilité d'utilisation grâce à une combinaison de technologies avancées telles que le sharding, l'intelligence artificielle, l'apprentissage machine et les algorithmes de consensus plus efficaces, tout en favorisant l'interopérabilité et une meilleure accessibilité pour les développeurs et les utilisateurs [8].

1.9 Domaines d'application de la blockchain

La blockchain est une technologie qui peut être appliquée dans de nombreux domaines différents. Voici quelques exemples de domaines d'application de la blockchain. La figure ci-dessous regroupe un grand nombre de domaines d'application des blockchains.

1.9.1 La santé

La blockchain offre plusieurs avantages pour le secteur de la santé, tels que la sécurité et la confidentialité des données, la gestion des dossiers de santé électroniques, la gestion des médicaments, les essais cliniques, la gestion des soins de santé et la recherche médicale. Cependant, son utilisation pose également des défis tels que la protection de la vie privée, la réglementation et la conformité, et la compatibilité des systèmes existants [11].

1.9.2 L'identité numérique

La blockchain peut être utilisée pour créer des systèmes de gestion de l'identité numérique décentralisés et autonomes, offrant des avantages tels que la sécurité et la confidentialité des données, la preuve d'identité, la vérification des qualifications et l'interopérabilité des systèmes. Les individus peuvent contrôler et partager leurs données personnelles en toute sécurité, sans avoir besoin d'une autorité centrale pour les vérifier [11].

1.9.3 Le vote

La blockchain peut être utilisée pour garantir l'intégrité et la sécurité des élections, pour faciliter les processus de vote et éviter des problèmes tels que la perte de registres et la fraude électorale. Les électeurs pouvaient compter les votes eux-mêmes et vérifier qu'aucun vote n'avait été supprimé, manipulé ou modifié [11].

1.9.4 La finance

la blockchain est souvent associée à la cryptomonnaie et peut être utilisée pour les paiements, les transferts de fonds, les prêts, les échanges de devises, etc. La technologie permet de sécuriser les transactions et de réduire les frais et les délais de traitement.

1.9.5 L'énergie

la blockchain peut aider à suivre l'utilisation de l'énergie renouvelable, à gérer les transactions énergétiques et à échanger de l'énergie de manière transparente entre les consommateurs.

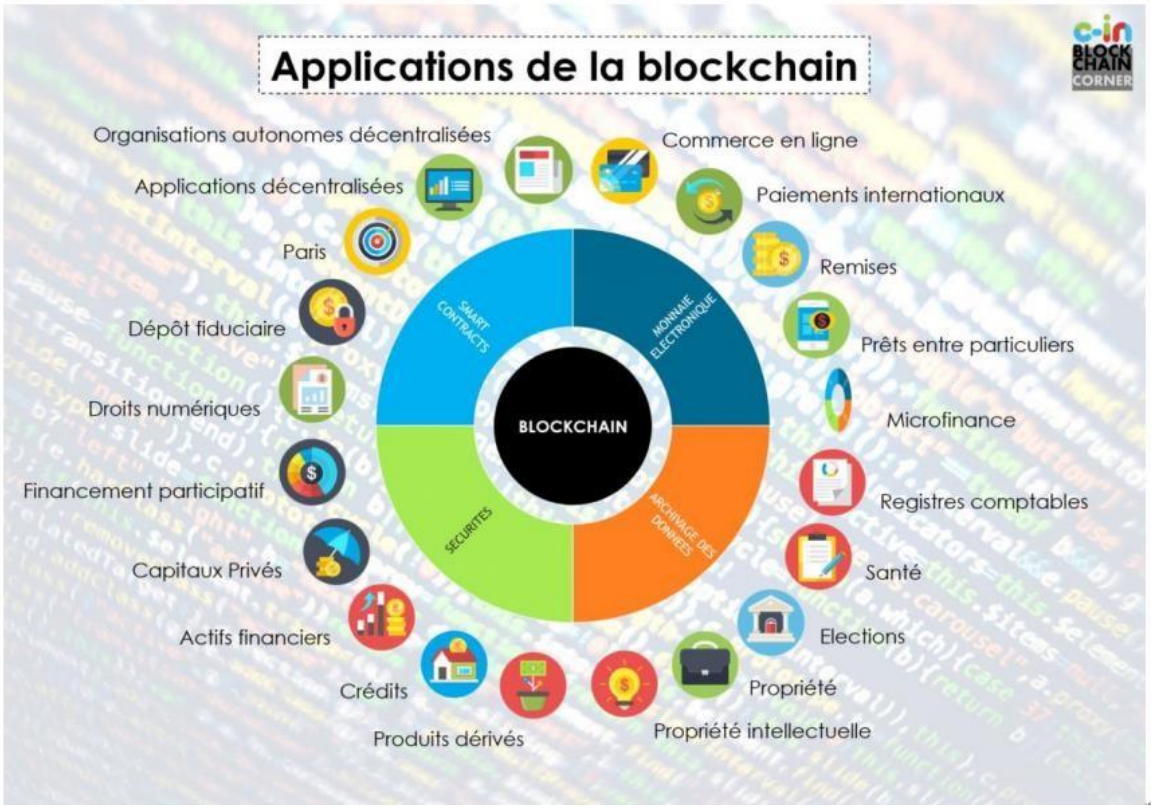

Figure 1.3: Les domaines d'application de la blockchain.

1.10 Avantages et les inconvénients de Blockchain

1.10.1 Les avantages de la blockchain

- **Sécurité** L'aspect décentralisé assure la sécurité des informations et des échanges inscrit dans l'historique de la blockchain. Les transactions sont sécurisées par une cryptographie qui garantissent l'intégrité des données [16].
- **Rapidité et efficacité** Les transactions peuvent être effectuées rapidement et de manière efficace, sans avoir besoin d'intermédiaires [16].
- **Stabilité** Les information contenues dans la chaine de blocs ne peuvent être effacées ni modifiées une fois qu'elles ont été enregistrées [16].
- **Couts réduits** Permet de réduire les couts de transactions en éliminant les intermédiaires et les frais de transaction élevés [16].

1.10.2 les inconvénients de la Blockchain

- **Évolutivité** La blockchain Peut avoir des problèmes d'évolutivité en raison de la grande quantité de données qu'elle doit traiter, ce qui peut ralentir les transactions et rendre son utilisation moins efficace [16].
- **L'attaque à 51%** Elle désigne une attaque d'une blockchain (fonctionnant avec des mineurs) conduite par un ensemble de nœuds du réseau qui contrôle plus de la moitié de la puissance de calcul du réseau. Elle résulte dans la possibilité pour cet ensemble de nœuds de choisir les transactions inscrites dans la blockchain et de rendre possible une double dépense. C'est une attaque classiquement redoutée, car susceptible de rendre inutilisable la blockchain [16].
- **Complexité technique** la mise en place et l'utilisation de la blockchain nécessitent une certaine expertise technique, ce qui peut rendre son adoption difficile pour certains utilisateurs [16].

1.11 Conclusion

Dans ce chapitre, nous avons présenté les fondamentaux de la technologie blockchain et son principe de fonctionnement. La technologie blockchain est une innovation révolutionnaire qui peut potentiellement transformer de nombreux secteurs d'activité. Sa

structure décentralisée, sa sécurité, sa transparence et son immutabilité en font un outil précieux pour la gestion et la vérification de données et de transactions. Les applications de la blockchain sont vastes et touchent des domaines tels que la finance, la santé, la logistique, l'énergie, l'immobilier et bien plus encore. Cependant, comme toute technologie émergente, la blockchain présente également des limites et des défis à surmonter.

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

CHAPITRE 2

VALIDATION DANS LA BLOCKCHAIN

Introduction

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

La validation de transaction sur une blockchain est un processus essentiel pour garantir l'intégrité et la sécurité du réseau. Dans ce chapitre nous présentons en détail quelques algorithmes de consensus les plus utilisé dans la blockchain et listons leurs différents avantages et inconvénient.

2.1 Le processus de validation de la blockchain

Le principe de validation de la blockchain repose sur un processus de consensus qui permet de vérifier l'exactitude des transactions et de garantir la sécurité du réseau. Ce processus de consensus implique plusieurs participants qui travaillent ensemble pour valider les transactions et ajouter des blocs à la chaine de blocs.

Le processus de validation commence par la création d'une transaction par un utilisateur de la blockchain. Cette transaction est ensuite diffusée à l'ensemble du réseau pour que tous les participants puissent la voir. Chaque participant peut alors valider cette transaction en utilisant le mécanisme de consensus spécifique à la blockchain.

Le mécanisme de consensus peut être basé sur (preuve de travail, preuve d'enjeu, preuve de authority, etc.). Chacun de ces mécanismes à ses propres règles de validation et de récompense pour les participants.

Une fois qu'une transaction est validée, elle est ajoutée à un bloc qui est ensuite ajouté à la chaine de blocs. Chaque bloc contient un ensemble de transaction qui ontété validées et ajoutées à la blockchain. Les blocs sont reliés les uns aux autres de manière chronologique pour former une chaine de blocs qui contient l'historique complet de transactions de la blockchain.

Lorsqu'un bloc es ajouté à la chaine de blocs, il devient immuable, ce qui signifie qu'il ne peut pas être modifié ou supprimé. Cette caractéristique garantit l'intégrité et la sécurité de la blockchain, car une fois qu'une transaction enregistrée dans la chaine de blocs, elle ne peut être altérée.

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

L'efficacité d'un mécanisme de consensus dans une blockchain est un élément crucial pour garantir la performance, la sécurité et la fiabilité du réseau. Voici quelques critères d'efficacité pour évaluer un mécanisme de consensus :

- Scalabilité : La capacité de la blockchain à gérer un grand nombre de transactions simultanées est importante pour garantir une utilisation efficace de réseau. Les mécanismes de consensus qui peuvent s'adapter à une augmentation de la charge

de travail sans compromettre les performances sont considérés comme plus efficaces [24].

- Vitesse de traitement des transactions : Les transactions doivent etre traitées rapidement pour éviter les retards et les goulots d'étranglement. Les mécanismes de consensus qui permettent un traitement rapide des transactions sont considérés comme plus efficaces.
- Sécurité : La sécurité est un aspect crucial de toute blockchain, car les transactions une fois enregistrées sont immuables et irréversibles. Les mécanismes de consensus qui garantissent une sécurité maximale contre les attaques malveillantes [24].
- Consommation énergétique : la consommation énergétique est un autre critère important pour l'efficacité d'un mécanisme de consensus, car une consommation énergétique élevée peut avoir un impact négatif sur l'environnement et les couts d'exploitation. Les mécanismes de consensus qui consomment moins d'énergie.
- Facilité de mise en œuvre : La complexité du mécanisme de consensus peut influencer le faciliter de mise en œuvre de la blockchain. Les mécanismes de consensus qui sont faciles à mettre en œuvre et à maintenir sont considérés comme plus efficaces.
- Tolérance aux fautes : La tolérance aux fautes fait référence à la capacité du système à maintenir son fonctionnement en présence d'un certain nombre de nœuds malveillants ou défaillants dans le réseau.
- Sureté : La sureté fait référence à la garantie que le système ne subira pas de défaillance catastrophique ou de corruption des données. Cela signifie que le mécanisme de consensus doit être conçu de manière à garantir que les transactions sont traitées de manière cohérente et que les blocs sont ajoutés à la chaine de blocs dans l'ordre correct [24].

2.3 Algorithme de consensus

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

2.3.1 Preuve de travail (POW : proof of work)

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

En 2009, Bitcoin a introduit une manière innovante d'utiliser la preuve de travail, comme algorithme de consensus. Dans ce cas, POW est utilisé pour valider les transactions qui sont regroupées dans des blocs, qui sont liés entre eux pour former une blockchain. Depuis lors, POW s'est propagé pour devenir un algorithme de consensus largement utilisé et est maintenant utilise par de nombreuses crypto-monnaies [28].

2.3.1.1 Principe de fonctionnement

1. Création d'une transaction : Tout utilisateur qui souhaite effectuer une transaction sur la blockchain crée un message contenant les informations sur la transaction, telles que l'adresse du destinataire, le montant envoyé et des données supplémentaires si nécessaire. Cette transaction est ajoutée à un pool de transactions en attente de validation.

2. Regroupement de transactions : Les mineurs du réseau collectent un certain nombre de transactions du pool en un bloc. Les transactions peuvent être choisies en fonction du montant des frais de transaction qu'elles offrent, car les mineurs sont incités à ajouter des transactions avec des frais plus élevés pour maximiser leurs profits [28].

3. Résolution du puzzle : Le bloc de transactions est ensuite soumis à un processus de preuve de travail qui implique la résolution d'un puzzle cryptographique. Le puzzle consiste en un problème mathématique complexe qui doit être résolu en utilisant la puissance de calcul d'un ordinateur. Le but est de trouver un nonce qui, une fois combiné avec les autres données du bloc, produit une empreinte numérique (ou hash) satisfaisant certaines conditions. Les conditions sont définies par le protocole de la blockchain et peuvent être modifiées en fonction de la puissance de calcul du réseau.

4. Validation du bloc : Une fois qu'un mineur trouve un nonce satisfaisant les conditions du puzzle, il l'ajoute au bloc et diffuse le bloc à l'ensemble du réseau. Les

autres nœuds du réseau vérifient alors la validité du bloc en utilisant le nonce et les données du bloc [28].

5. Ajout du bloc à la chaine de blocs : Une fois que le bloc est validé, il est ajouté à la chaîne de blocs. Le mineur qui a résolu le puzzle est récompensé par des crypto-monnaies, généralement la crypto-monnaie native de la blockchain. Les mineurs peuvent également recevoir des frais de transaction pour les transactionsincluses dans le bloc.

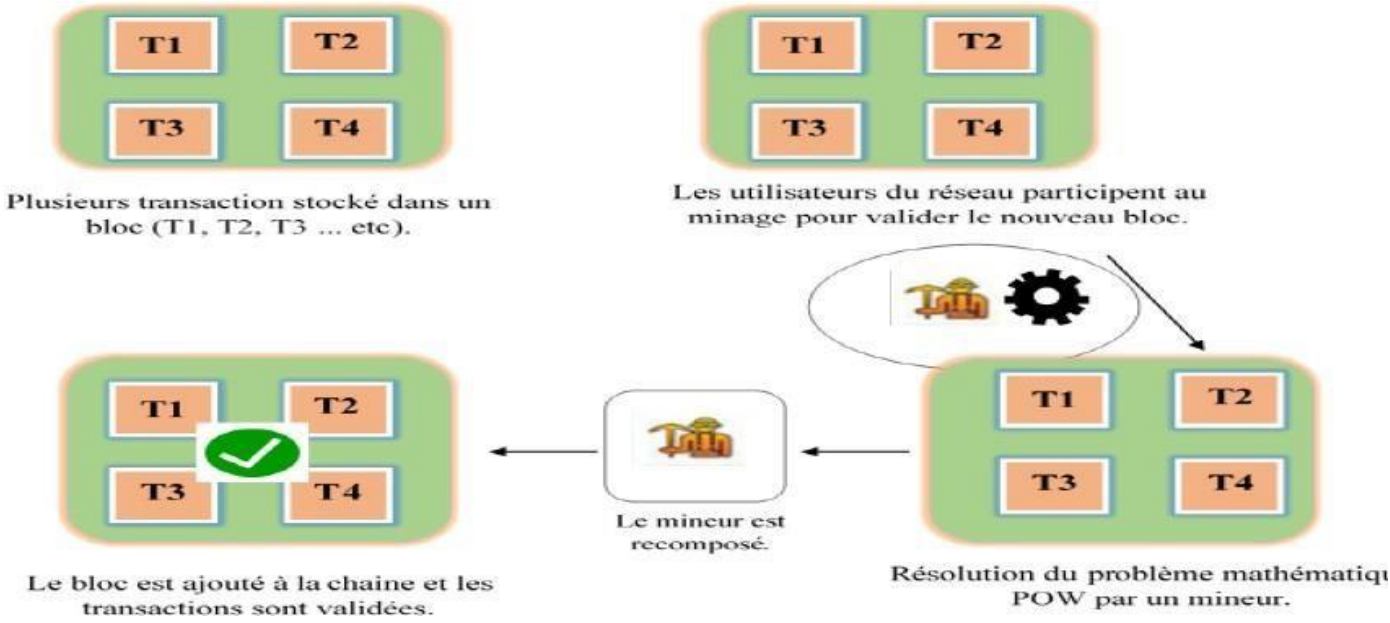

Figure 2.1: POW dans une blockchain [28].

6. Répétition du processus : Le processus de preuve de travail se répète pour chaque nouveau bloc qui est ajouté à la chaîne de blocs. Le puzzle est ajusté en fonction de la puissance de calcul du réseau pour maintenir un temps de traitement constant et garantir que les blocs sont ajoutés à la chaîne de blocs à un rythme régulier.

Les étapes de l'algorithme de POW sont illustrées dans le diagramme de la figure 5

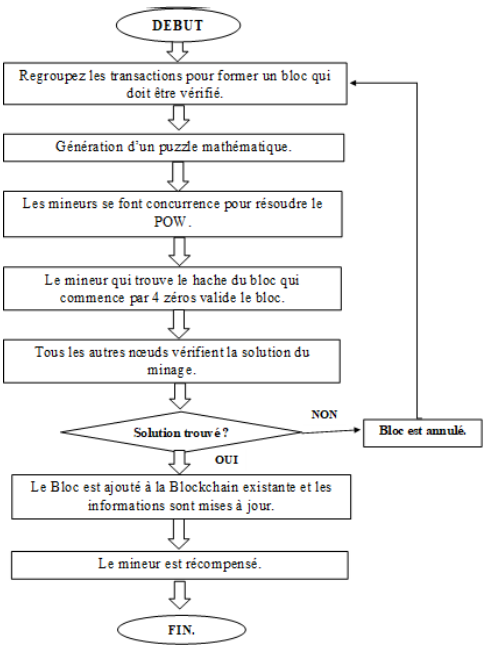

Figure 2.2: organigramme de l'algorithme POW.

2.3.1.2 Avantages de POW

On peut citer les avantages suivants :

- Sécurité : Le POW est considéré comme l'un des mécanismes de consensus les plus sécurisés pour les blockchains car il rend extrêmement difficile la falsification des transactions et la modification de la chaîne de blocs. Cela est dû à la puissance de calcul élevée nécessaire pour résoudre les équations mathématiques complexes pour la validation de blocs [12].
- Décentralisation : Le POW permet à n'importe qui avec un ordinateur et une connexion Internet de participer à la validation de blocs, ce qui favorise la décentralisation de la blockchain.
- Equité : Étant donné que les validateurs doivent consacrer du temps et des ressources pour résoudre les équations mathématiques complexes, le POW favorise une participation équitable au réseau.
- Inviolabilité : Le POW assure l'inviolabilité de la blockchain car les transactions validées ne peuvent pas être modifiées. Cela garantit la sécurité des fonds stockés sur la blockchain [12].

2.3.1.3 Inconvénients de POW

Comme inconvénients, on peut signaler les points suivants :

- Consommation énergétique élevée : La résolution des équations mathématiques complexes pour valider les blocs nécessite une grande quantité d'énergie. Le POW est donc très gourmand en énergie, ce qui peut avoir un impact environnemental important [22].
- Coûts élevés : La validation de blocs sur une blockchain basée sur le POW nécessite l'utilisation d'un matériel informatique de pointe, qui peut être coûteux à acquérir et à entretenir.
- Centralisation potentielle : Bien que le POW favorise la décentralisation, il existe un risque de centralisation dans la mesure où les mineurs ayant accès à une puissance de calcul plus importante peuvent avoir une influence disproportionnée sur le réseau.
- L'attaque de 51% : Si plus de la moitié de la puissance de calcul du réseau est contrôlée par un seul groupe de mineurs, il y a un risque de "51% attack" où le groupe peut potentiellement fausser des transactions et modifier la chaîne de blocs à son avantage [22].
- Évolutivité limitée : Le POW peut devenir inefficace lorsque le nombre de transactions à valider sur la blockchain devient trop important, ce qui limite l'évolutivité de la technologie [22].

2.3.2 Preuve d'enjeu (POS : proof of stake)

Le concept de Proof of Stake (POS) a été introduit pour la première fois en 2011 par Sunny King et Scott Nadal dans un document intitulé "PPCoin : Peer-to-Peer Crypto-Currency with Proof-of-Stake". [26] Cette proposition visait à résoudre certains des problèmes de Proof of Work (POW), notamment la consommation d'énergie élevée et le risque de centralisation du contrôle de la blockchain.

En 2012, Peercoin a été lancé en tant que première cryptomonnaie à utiliser le mécanisme de consensus POS. La plateforme Ethereum a également commencé à travailler sur un mécanisme de consensus POS appelé Casper en 2014. Casper a été officiellement publié en 2017 dans un document intitulé "Casper the Friendly Finality Gadget".

2.3.2.1 Principe de fonctionnement

Le principe de fonctionnement de Proof of Stake (POS) diffère de celui de Proof of Work (POW). Au lieu de résoudre des problèmes mathématiques complexes comme dans POW, POS repose sur le staking (ou la mise en jeu) de crypto-monnaies par les participants pour sécuriser la blockchain .

Voici les étapes du fonctionnement de base de proof of stake (POS) :

1. Staking : Les validateurs doivent détenir une certaine quantité de crypto-monnaies pour être autorisés à participer au processus de validation des blocs. Cette quantité de crypto-monnaies est mise en jeu pour garantir la participation des validateurs dans le processus de validation des blocs. Plus la quantité de crypto-monnaies mise en jeu est élevée, plus le validateur a de chances d'être sélectionné pour valider un bloc [2].

2. Sélection des validateurs : Les validateurs sont sélectionnés pour valider les blocs en fonction de la quantité de crypto-monnaies qu'ils ont mises en jeu. Le système utilise une méthode de sélection aléatoire pondérée, où les validateurs avec une plus grande quantité de crypto-monnaies mise en jeu ont une plus grande chance d'être sélectionnés pour valider un bloc [2].

3. Validation des blocs : Une fois sélectionné pour valider un bloc, le validateur doit proposer un bloc contenant les transactions en cours. Le validateur doit prouver qu'il détient suffisamment de crypto-monnaies mise en jeu pour être autorisé à valider le bloc. La méthode de preuve de possession (proof of ownership) est utilisée pour prouver la possession des crypto-monnaies en mise en jeu.

4. Vérification des blocs : Les autres validateurs vérifient la proposition de bloc et s'assurent qu'elle est conforme aux règles du système PoS. Si une majorité de validateurs approuve la proposition de bloc, elle est ajoutée à la chaîne de blocs [2].

5. Récompenses : Les validateurs sont récompensés pour leur participation dans le processus de validation des blocs. Les récompenses peuvent prendre la forme de frais de transaction ou de nouveaux tokens créés lors de la validation du bloc [2].

6. Pénalités : Si un validateur enfreint les règles du système PoS, il peut perdre sa mise en jeu ou être exclu du processus de validation des blocs. Les infractions peuvent inclure la validation de blocs invalides ou la tentative de validation de blocs frauduleux.

Les étapes de l'algorithme de POS sont illustrées dans le diagramme de la figure 6

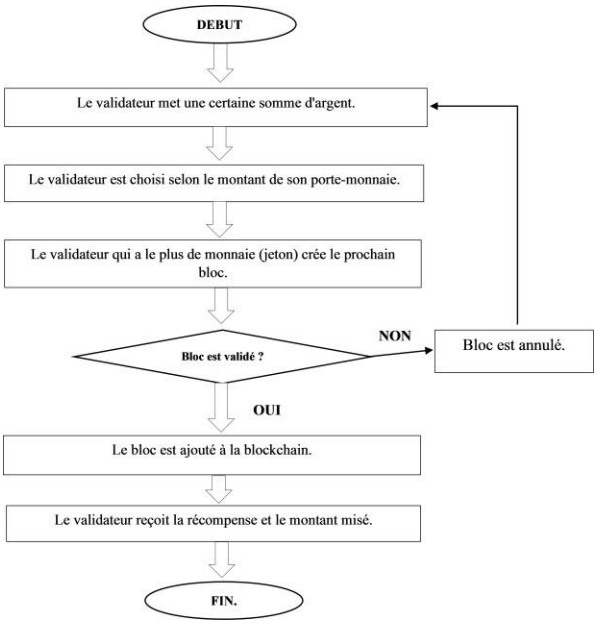

Figure 2.3: organigramme de l'algorithme POS.

2.3.2.2 Avantages de POS

On peut citer les points suivants comme avantages:

- Economie d'énergie : contrairement à proof of work (POW), qui nécessite une puissance de calcul importante, POS utilise beaucoup moins d'énergie pour valider les blocs. Cela est dû au fait que le processus de validation ne repose pas sur la résolution de problèmes mathématiques complexes [2].

- Sécurité améliorée : Dans un système POS, un attaquant potentiel doit détenir une majorité de la crypto-monnaie en circulation pour mener une attaque réussie. Cette quantité de crypto-monnaies serait si importante qu'elle serait très coûteuse à acquérir, rendant l'attaque peu rentable [2].

- Décentralisation accrue : Avec POS, chaque détenteur de crypto-monnaies à la possibilité de devenir un validateur. Cela permet une plus grande participation des membres de la communauté à la validation des blocs et renforce ainsi la décentralisation du système [2].

- Réduction des couts : Dans un système POS, les coûts associés au minage de crypto-monnaies (comme l'achat de matériel informatique) ne sont pas nécessaires,ce qui peut réduire les coûts pour les validateurs.
- Vitesse de transaction améliorée : La vitesse de transaction peut être améliorée dans un système POS, car le temps de validation des blocs est réduit par rapport à POW.
- Pas de risque de centralisation : Contrairement à POW, où les mineurs les plus puissants peuvent monopoliser le processus de validation des blocs, POS ne présente pas ce risque de centralisation.

2.3.2.3 Inconvénients de POS

Malgré ses avantages, ces problèmes suivants ont été signalés:

- Risque de centralisation : Bien que la décentralisation soit l'un des avantages de POS, il existe un risque que la validation des blocs soit centralisée entre les détenteurs de crypto-monnaies ayant une grande quantité de jetons. Cela pourrait potentiellement rendre le système vulnérable à des attaques.
- Équité contestée : Dans un système POS, les validateurs ayant une grande quantité de crypto-monnaies ont un avantage sur les autres, car ils ont plus de chances d'être choisis pour valider un bloc. Cela peut être considéré comme inéquitable par certains membres de la communauté.
- Difficulté à établir une participation active : Dans un système POS, il est important que les validateurs participent activement à la validation des blocs. Cependant, il peut être difficile de mesurer ou d'encourager une participation active.
- Risque de "Nothing-at-stake" : Dans un système POS, les validateurs n'ont rien à perdre s'ils votent pour plusieurs branches lors d'une bifurcation de la blockchain, contrairement à POW où les mineurs doivent dépenser de l'énergie pour résoudre un bloc. Cela peut potentiellement créer un risque de sharding de la blockchain [2].
- Risque d'attaque de 51 % : Bien que cela soit moins probable qu'avec POW, il existe toujours un risque d'attaque de 51 % dans un système POS, où un attaquant potentiel détient plus de 50 % des jetons en circulation et peut donc manipuler la blockchain [2].

2.3.3 Preuve d'Authorité (POA: proof of authority)

La preuve d'Authorité (POA) a été introduite pour la première fois en 2017 par Gavin Wood, co-fondateur d'Ethereum [6].

Le protocole POA a été conçu pour répondre aux besoins des blockchains privées et de consortium, qui ont des exigences de performance et de sécurité différentes de celles des blockchains publiques. La POA utilise un petit nombre de validateurs de confiance pour valider les transactions.

La première implémentation de la POA a été réalisée par la société Parity Technologies avec leur client de blockchain open-source, Parity Ethereum. Le protocole POA a également été adopté par des consortiums de banques, d'entreprises et de gouvernements pour leurs blockchains privées [1].

2.3.3.1 principe de fonctionnement

1. Sélection des validateurs : Les validateurs sont choisis par les développeurs de la blockchain ou la communauté. Ce sont généralement des entités bien connues qui ont été vérifiées. Leur identité et informations de contact sont publiques. Le nombre de validateurs dépend de la blockchain, mais doit être suffisamment décentralisé, généralement entre 10 et 50 validateurs.

2. Génération de blocs : Quand un bloc est généré par un mineur contient plusieurs transactions et est signé par le mineur [19].

3. Validation individuelle : Chaque vérificateur exécute indépendamment les mêmes vérifications sur le bloc pour s'assurer de sa validité.

4. Seuil de validation : Une fois qu'un certain seuil de votes de validation est atteint, par exemple les 2/3 des votes, le bloc est considéré comme finalisé et irrévocable. Il est ajouté à la chaîne de blocs principale [19].

5. Rotation des validateurs : Pour maintenir la décentralisation, de nouveaux validateurs peuvent être ajoutés et d'anciens validateurs peuvent être supprimés de temps en temps, en fonction de l'organisation de la blockchain.

6. Récompense des validateurs : Les validateurs sont récompensés pour leurs services [19].

2.3.3.2 Avantages de POA

On cite comme avantages:

- Efficacité énergétique : Contrairement à la preuve de travail (Proof of Work, ou POW), la POA ne nécessite pas de résolution de problèmes complexes, ce qui réduit considérablement la consommation d'énergie.
- Rapidité : La POA permet un temps de validation rapide des transactions et la création de nouveaux blocs, ce qui rend le réseau plus réactif.
- Sécurité : Les validateurs sont sélectionnés en fonction de leur réputation et doivent mettre en jeu leur identité. Cela dissuade les comportements malhonnêtes et renforce la sécurité du réseau.
- Scalabilité : La POA permet de traiter un plus grand nombre de transactions par seconde que les systèmes basés sur la preuve de travail, ce qui améliore la capacité du réseau à prendre en charge un plus grand nombre d'utilisateurs.
- Coûts réduits : La preuve d'autorité permet de réduire les coûts de transaction et de maintien du réseau, car elle ne nécessite pas de matériel spécialisé ou une grande quantité d'énergie.

2.3.3.3 Inconvénients de POA

On cite comme Inconvénients:

- Centralisation : La sélection de validateurs pré-approuvés peut entraîner une centralisation du pouvoir et du contrôle, ce qui est contraire à l'esprit de décentralisation des blockchains.
- Manque de transparence : La sélection des validateurs et la confiance en ces derniers reposent sur des processus centralisés et opaques, ce qui peut susciter des doutes sur l'intégrité du réseau.
- Exclusion des petits acteurs : Les utilisateurs ordinaires ne peuvent pas participer au processus de validation des transactions, ce qui limite leur influence sur le réseau et peut créer des inégalités.
- Résistance à la censure : La POA est moins résistante à la censure que les systèmes basés sur la preuve de travail, car les validateurs peuvent être soumis à des pressions externes pour censurer certaines transactions.

2.3.4 Preuve d'enjeu Délégué (DPOS : delegated proof of stake)

Le concept de DPOS est une évolution de la Preuve d'Enjeu (POS), a été proposée pour la première fois en 2014 par Dan Larimer, le fondateur de Bitshares, une blockchain qui utilise DPOS comme mécanisme de consensus. Depuis lors, DPOS a été adopté par d'autres blockchains, telles que EOS, Steemit et Lisk [4].

2.3.4.1 Principe de fonctionnement

Voici les étapes du fonctionnement de base de delegated proof of stake (DPOS) :

1. Les détenteurs de tokens sélectionnent des délégués : Dans un système DPoS, les détenteurs de tokens ont le pouvoir de sélectionner des délégués pour valider les transactions. Les détenteurs de tokens peuvent voter pour des délégués en utilisant leurs jetons, et les délégués ayant le plus grand nombre de voix deviennent les nœuds de validation [5].

2. Les délégués valident les transactions : Les délégués élus ont pour responsabilité de valider les transactions et de produire des blocs de transactions [5].

3. Récompenses pour les délégués : Les délégués élus reçoivent des récompenses pour leur travail de validation. Ces récompenses peuvent être sous forme de jetons, qui sont créés lors de la validation de nouveaux blocs [5].

2.3.4.2 Avantages de DPOS

On cite comme avantages:

- Evolutivité : DPOS permet une évolutivité supérieure à celle de la preuve de travail en réduisant le temps de bloc et en augmentant le nombre de transactions pouvant être traitées par seconde [5].

- Efficacité énergétique : Contrairement à la preuve de travail qui nécessite une énorme quantité d'énergie pour valider les transactions, DPOS ne nécessite pas de ressources importantes en énergie pour fonctionner [5].

- Décentralisation : Bien que DPOS nécessite un petit nombre de validateurs pour valider les transactions, il permet toujours une certaine forme de décentralisation en permettant aux utilisateurs de voter pour leurs validateurs préférés.

- Sécurité : DPOS utilise des mécanismes de sécurité sophistiqués pour empêcher toute tentative de fraude ou de piratage [5].
- Flexibilité : Les développeurs peuvent facilement ajouter de nouvelles fonctionnalités à DPOS sans avoir à modifier le protocole fondamental.
- Gouvernance : DPOS permet aux utilisateurs de participer à la prise de décision en matière de développement et de gestion du réseau en leur permettant de voter pour les modifications proposées.

2.3.4.3 Inconvénients de DPOS

Le consensus de DPOS a cependant lui aussi ses limites qui sont :

- Centralisation accrue : Bien que DPOS permette une certaine forme de décentralisation, il est également sujet à une centralisation accrue car seuls quelques validateurs sont impliqués dans la validation des transactions [5].
- Risque de censure : Étant donné que les validateurs sont sélectionnés par les utilisateurs, il existe un risque de censure ou de manipulation de la part de ces validateurs.
- Risque de collusion : Il y a un risque que les validateurs se mettent d'accord pour manipuler le système en leur faveur.
- Dépendance à l'égard des validateurs : Comme le système dépend des validateurs, une défaillance ou une compromission de leur part peut entraîner une panne du système.
- Complexité : DPOS est plus complexe que la preuve de travail en raison de la nécessité de sélectionner les validateurs et de mettre en œuvre des mécanismes de vote et de gouvernance [5].

2.3.5 Preuve de temps écoulé (POET: proof of Elapsed Time)

La Preuve de Temps Ecoulé : proof of Elapsed Time) est un concept relativement nouveau en matière de mécanisme de consensus. Depuis lors, il n'a pas encore été largement utilisé dans les systèmes de blockchain existants, mais suscite un intérêt croissant en tant que méthode alternative p our atteindre un consensus distribué.

L'idée principale de l'ETP est de lier le temps écoulé depuis le dernier bloc miné à la difficulté de la preuv traditionnelle, où e de travail (PO W). Contrairement à la preuve de travail la difficulté est fixée en fonction de la puissance de calcul de l'ensemble du réseau, la difficulté de l'ETP dépend du temps écoulé depuis le dernier bloc. Cela signifie que plus de temps s'écoule entre deux blocs minés, plus la difficulté pour miner le prochain bloc sera faible, ce qui permettrait à plus de mineurs d'avoir une chance de miner le bloc suivant [7].

2.3.5.1 principe de fonctionnement

1. Initialisation : Chaque nœud participant à la blockchain exécute un logiciel avec une TEE (Trusted Execution Environment), comme Intel SGX. La TEE garntit que le code s'exécute dans un environnement sécurisé et isolé, ce qui empeche les autres applications ou le système d'exploitation de manipuler le processus [7] .

2. Génération de l'attente : Chaque nœud génère un nombre aléatoire (délai d'attente) en utilisant un générateur de nombre aléatoires sécurisé à l'intérieur de la TEE.Ce délai d'attente est associé à un certificat qui prouve que le nombre a été généré à l'intérieur de la TEE.

3. Début de l'attente : Les nœuds commencent à attendre pendant la durée spécifiée par leur délai d'attente. Pendant cette période, ils continuent à exécuter leurs fonctions normales, telles que la validation des transactions et la propagation des messages sur le réseau.

4. Fin de l'attente : Lorsqu'un nœud a attendu pendant la durée spécifiée, il crée un objet appelé "preuve de temps écoulé (POET) qui inclut le certificat TEE, la durée d'attente et d'autres informations pertinentes pour le bloc en cours [7].

5. Proposition de bloc : Le nœud envoie sa preuve de temps écoulé à tous les autres nœuds du réseau en tant que proposition pour créer le prochain bloc. Les autres nœuds vérifient la validité de la preuve (par exemple, en s'assurant que le certificat TEE est valide et que le délai d'attente a été respecté).

6. Sélection du leader : Les nœuds comparent les preuves de temps écoulé qu'ils ont reçues et choisissent celle avec le plus petit délai d'attente. Le nœud ayant soumis cette preuve est sélectionné comme leader pour créer le prochain bloc.

7. Création du bloc : le leader crée un nouveau bloc contenant les transactions en attente et l'ajoute à la chaine.
8. Propagation du bloc : Le leader envoie le nouveau bloc aux autre nœuds du réseau, qui valident le bloc et mettent à jour leur copie de la chaine en conséquence [7].
9. Nouveau tour : Le processus recommence à l'étape 2, avec chaque nœud générant un nouveau délai d'attente et attendant de proposer le prochain bloc.

2.3.5.2 Avantages de POET

- Économie d'énergie : Contrairement aux protocoles de consensus basés sur la preuve de travail (POW), comme celui utilisé par Bitcoin, POET ne nécessitepas une grande quantité de puissance de calcul pour sécuriser le réseau. Cela signifie qu'il est beaucoup plus économe en énergie et donc plus respectueux de l'environnement.
- Sécurité : Le processus de sélection aléatoire du leader dans POET garantit qu'aucun nœud ne peut contrôler le réseau. De plus, la preuve de temps fournit une méthode fiable pour valider les transactions, ce qui garantit la sécurité et l'intégrité de la blockchain
- Scalabilité : POET est un protocole de consensus hautement évolutif, car il peut être utilisé sur des réseaux de toutes tailles sans compromettre la sécurité ou la performance
- Facilité d'utilisation : La preuve de temps dans POET est facile à comprendre pour les développeurs et les utilisateurs, ce qui facilite l'adoption de la technologie.De plus, l'absence de mineurs ou de validateurs centraux rend le processus de validation des transactions plus simple et moins coûteux.

2.3.5.3 Inconvénients de POET

- Centralisation : POET nécessite une infrastructure matérielle spécifique pour générer les épreuves de temps, ce qui peut entraîner une centralisation de la production de ces épreuves de temps. Cela peut potentiellement compromettre la décentralisation du réseau et réduire la sécurité.
- Dépendance envers Intel : POET est développé par Intel, ce qui signifie que le protocole est étroitement lié à cette entreprise et à sa technologie. Cela peut limiter

la compétition dans le domaine de la technologie de consensus et rendre difficile l'adoption de la technologie par d'autres acteurs du marché.

- Complexité : Le protocole POET est relativement complexe à mettre en œuvre, ce qui peut rendre son adoption difficile pour les développeurs et les utilisateurs. Cela peut également rendre le protocole plus sujet aux erreurs et aux vulnérabilités.
- Risques liés à la preuve de temps : Bien que la preuve de temps soit plus économe en énergie que la preuve de travail, elle repose sur l'hypothèse que les nœuds participant au réseau suivent les règles de manière honnête. Si un nœud parvient à générer une épreuve de temps plus rapidement que les autres, cela peut potentiellement compromettre la sécurité du réseau.

2.4 Conclusion

Comme nous avons vu et après avoir examiné les différents algorithmes de consensus tels que POW, POS, POA, POET, et DPOS, il est clair qu'aucun d'entre eux n'est parfait. Chacun a ses propres avantages et inconvénients en termes de sécurité, de vitesse de transaction, de coûts de fonctionnement, de centralisation, etc. Par conséquent, il est important de choisir l'algorithme de consensus le mieux adapté aux besoins spécifiques d'un projet blockchain. Toutefois, il est à noter que la preuve de travail semble offrir une plus grande stabilité aux réseaux en prévenant les attaques à longue portée.

CHAPITRE 3

ETAT DE L'ART SUR LE CLUSTERING DANS LES BLOCKCHAIN

Introduction

L'un des défis majeurs dans l'utilisation de la blockchain est la gestion efficace des données et des communications au sein du réseau. C'est là que le regroupement et le clustering entrent en jeu. Le regroupement consiste à former des sous-groupes de nœuds ou d'entités ayant des caractéristiques similaires, tandis que le clustering implique l'organisation des données en groupes homogènes en fonction de divers critères.

Dans cette revue, nous explorerons l'utilisation du regroupement et du clustering dans le contexte de la technologie blockchain. Nous examinerons comment ces techniques peuvent améliorer l'efficacité des communications, renforcer la confiance et la sécurité, optimiser le stockage des données et détecter les comportements malveillants.

Nous analyserons plusieurs articles qui abordent ces questions dans des domaines variés, tels que les réseaux pair-à-pair, les systèmes de transport intelligents, la fabrication intelligente, le stockage sur le cloud, et d'autres encore. Ces articles proposent des approches novatrices qui exploitent les avantages de la blockchain et du regroupement pour résoudre des problèmes spécifiques et améliorer les performances des systèmes décentralisés.

3.1 Articles traités

3.1.1 CTB-PKI: Clustering and Trust Enabled Blockchain Based PKI System for Efficient Communication in P2P Network [CTB] [10]

Cet article propose une approche différente pour accroître l'efficacité de l'infrastructure à clé publique basée sur la blockchain (BC-PKI). Dans un réseau blockchain, chaque transaction nécessite la sélection d'une autorité de certification (AC). Par conséquent, un grand nombre de transactions nécessite un effort de calcul important. Cette procédure de sélection de AC devient la principale cause de surcharge de calcul du réseau, ce qui réduit les performances du réseau. Pour contourner le problème, un regroupement de réseaux (clustering) est une solution potentielle.

L'approche proposée crée des clusters de nœuds participants en fonction de leur temps de validation, de leur temps de réponse et de leur niveau de confiance. Cette méthode sélectionne un cluster en fonction du budget de temps de réponse et de temps devalidation donné par le nœud qui a l'intention de démarrer une transaction. Ensuite, le nœud qui a le niveau de confiance le plus élevé dans ce cluster est choisi comme autorité de certification pour la prochaine transaction. Au lieu de rechercher sur tous les nœuds participants, cette approche recherche sur les nœuds du cluster choisi, ce qui réduit l'espace de recherche du processus de sélection de l'AC.

Les auteurs ont adopté une approche d'évaluation de la confiance où le facteur de confiance est quantifié en fonction de son expérience et de sa réputation. La confiance de nœud est réévaluée après chaque transaction réussie et non réussie. Un nœud qui effectue des transactions plus réussies a plus de valeur de confiance. Le nœud quia une valeur de confiance plus élevée a une probabilité plus élevée d'être sélectionné comme autorité de certification pour une transaction. Le processus de réévaluation de la confiance est suivi du processus de regroupement. Le CTB-PKI proposé utilise les algorithmes de clustering K-Means (avec silhouette score) et DBScan.

La CTB-PKI proposée est implémentée dans l'open-source Plateforme Go-Ethereum (GETH) et évaluée sur la base des trois métriques (i) temps de réponse avec et sans clustering, (ii) temps de validation avec et sans clustering, et (iii) coût du gaz utilisé pour différentes transactions.

3.1.2 A Blockchain-Assisted Trusted Clustering Mechanism for IoT-Enabled Smart Transportation System [Vanet] [17]

Dans Vehicular Ad-hoc Network (VANET), la communication entre l'infrastructure et les nœuds de participation au réseau présente plusieurs inconvénients. Lorsque l'infrastructure VANET reçoit une énorme quantité de demandes de véhicules, le temps de réponse peut augmenter, ce qui entraîne un taux de frais généraux (overhead ratio) plus élevé. Pour relever les défis associés au taux élevé de communications et aux limitations qui en découlent, les chercheurs ont proposé un mécanisme de regroupement dans lequel les véhicules se regroupent pour former un cluster. Le cluster est dirigé par le chef de cluster (head) et les nœuds participants du cluster ne sont autorisés à communiquer qu'avec le chef. Cependant, les chefs de cluster sont autorisés à communiquer avec l'infrastructure pour réduire les communications et alléger la charge avec l'aide d'autres chefs de cluster.

Pour maintenir la sécurité, le mécanisme proposé utilise la blockchain pour crypter les informations sensibles liées aux véhicules, c'est-à-dire le degré de confiance et la qualité de service, en termes de paramètres prédéfinis. Les informations cryptées sont enregistrées par la station de base pour propagation et agrégation afin d'éliminer l'exécution réussie de nombreuses attaques potentielles dans l'environnement VANET.

Dans l'architecture proposée, la station de base, est l'entité la plus importante, communique avec les unités routières (UR) pour maintenir la fiabilité dans l'environnement. Les UR lancent le processus de clustering et assistent les nœuds en tant qu'autorité frontale. L'unité demande à la station de base de démarrer le processus d'évaluation en calculant d'abord le degré de confiance. Après l'achèvement du processus d'évaluation de confiance, la station de base compare le degré de confiance avec la valeur seuil pourla prise de décision. Le processus de sélection des chefs de cluster commence par le calcul des paramètres QoS et leur fusion avec des degrés de confiance pré-évalués pour la sélection finale.

Les paramètres de confiance qui sont utilisés dans le mécanisme proposé appartiennent à la composante réputation de la confiance, c'est-à-dire la coopération, l'honnêteté et la fiabilité. Le calcul de confiance est effectué par la station de base lorsque les nœuds demandent à UR de rejoindre le cluster. Les nœuds ne permettront de rejoindre un cluster que lorsque le degré de confiance est supérieur à la valeur seuil. Les paramètres de confiance de coopération améliorent la coopération, et l'évaluation de ce paramètre est calculée en évaluant le degré de collaboration sur un nœud particulier. L'honnêteté

est le paramètre clé, car elle offre les capacités d'améliorer le niveau de crédibilité. Le paramètre d'honnêteté est également lié à la coopération, ce qui signifie que si les nœuds ont un niveau d'honnêteté plus élevé, cela augmentera également le niveau de coopération. La fiabilité est calculée par le nombre d'opérations divisé par le nombre d'échecs auxquels les nœuds sont confrontés lorsqu'ils deviennent chef de cluster. L'évaluation des paramètres de QoS ne sera effectuée par le mécanisme proposé que lorsqu'un nœud particulier devient candidat pour être chef de cluster. Les paramètres QoS consistent en un taux de livraison de paquets pour faciliter la communication, un temps d'exécution pour évaluer le taux de réponse et un score d'opinion moyen fourni par les chefs adjoints du cluster.

3.1.3 Blockchain Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS [CPS] [25]

Cyber-Physical System (CPS) est l'unification des processus informatiques et physiques, et c'est un système intelligent qui intègre le calcul, la communication et le contrôle. Il est largement utilisé dans les systèmes de fabrication.

Les auteurs ont proposé une stratégie de division d'une blockchain basée sur le regroupement de communautés de nœuds. C'est une méthode pour diviser les nœuds en différents groupes dans un système CPS. Chaque groupe est une chaîne et contient des nœuds conservant des données similaires. Un nœud peut être ajouté à différentes chaînes selon la stratégie. Pour la synchronisation des données, les nœuds d'une même chaîne n'ont besoin que de synchroniser les données des nœuds qui ont rejoint cette chaîne.

Dans la production réelle, il existe des différences dans les communications entre les nœuds, qui peuvent être utilisées comme base pour le chaînage des données. Sur cette base, un modèle de confiance de graphe pondéré non orienté est proposé. Dans ce modèle, il est fait abstraction du périphérique en tant que nœud dans un graphe non orienté. Le poids des arcs représente une certaine relation de communication entre deux nœuds connectés, et le degré de densité des communications représente la communication entre un nœud et les autres nœuds conjoints. La densité est une variable pour mesurer le degré de relation de confiance entre les appareils.

Les auteurs divisent les équipements du système en différents groupes en fonction de densité de la communication entre les équipements, de sorte que les équipements

ayant des relations de communication étroites puissent être regroupés dans la mesure du possible, de manière à former une chaîne de données dans le système blockchain avecune structure multichaîne.

Selon la densité des communications entre les appareils, un seuil est défini et la relation de communication entre les nœuds est divisée en deux catégories. La première est que la relation de communication est relativement dense et que les poids des arcs entre les nœuds sont supérieurs au seuil défini. L'autre est moins de communication et les poids des arcs entre les nœuds sont inférieurs au seuil ou il n'y a pas d'arcs. Selon les résultats de la classification, les nœuds ayant une relation de communication dense sont dans le même groupe.

3.1.4 On Cloud Storage Optimization of Blockchain with a Clustering-Based Genetic Algorithm [Cloud] [27]

En raison du grand nombre d'appareils IoT qui agissent toujours comme générateurs de données dans de nombreux systèmes, les transactions seront générées à un rythme élevé. Le problème de stockage dans la blockchain est plus grave dans l'IoT.

Dans cet article, pour étendre la capacité de la blockchain, pour chaque pair, les anciens blocs créés précédemment et moins susceptibles d'être interrogés sont sélectionnés, et sont stockés dans le cloud. Sur la base de cette idée, des fonctions objectives liées à la probabilité de requête, au coût de stockage et à l'occupation de l'espace local ont été formés, ce qui réduit naturellement le problème à la sélection de blocs. Les résultats peuvent être obtenus en résolvant un problème d'optimisation multi-objectifs. Un algorithme génétique de tri non dominé avec regroupement (NSGA-C nondominated sorting genetic algorithm with clustering) a été conçu, qui modifie la méthode de sélection des individus de la couche de dominance critique en ajoutant un regroupement pour assurer la diversité. La solution appropriée peut être sélectionnée dans l'ensemble de Pareto pour répondre aux exigences des différents utilisateurs.

En raison de la limitation des ressources mémoire, les appareils IoT ne deviennent souvent pas directement des pairs dans le réseau blockchain. Au lieu de cela, ils sont connectés à des pairs dans la blockchain et le registre est stocké dans les pairs correspondants.

Les transactions sont générées dans les appareils IoT qui sont connectés aux pairs dans la blockchain. Pour chaque pair Ni, les premiers blocs Mi sont selectionnés et à

sont stockés dans le cloud. Chaque fois qu'il y a N blocs générés, les premiers Mi blocs sont sélectionnés. Pour déterminer la valeur de Mi, ils prennent en considération la probabilité de requête des blocs Mi, le coût de stockage dans le cloud et l'occupation de l'espace local. Pour garantir la fiabilité du système, un pair correspond à au moins un serveur cloud. Plus précisément, un pair peut sélectionner plusieurs serveurs cloud selon les besoins pour éviter la perte accidentelle de données stockées dans le cloud.

3.1.5 Behavior pattern clustering in blockchain networks [Behavior][13]

Dans cet article, le problème du clustering des modèles de comportement dans les réseaux blockchain est introduit et un nouvel algorithme appelé BPC est proposé pour résoudre ce problème. Une longue liste de mesures de similarité de séquence potentielles est évaluée et une distance qui convient au problème de regroupement des modèles de comportement est sélectionné.

Dans une blockchain publique, il y a généralement des millions de nœuds. Certains nœuds peuvent tenter de tricher dans le réseau pour des intérêts illégaux et avoir des comportements anormaux alors que les nœuds majoritaires se comportent normalement. Il faut énormément de temps et d'efforts pour étudier manuellement les comportements de tous les nœuds. Face à ce problème, cet article propose de regrouper automatiquement les modèles de comportement de tous les nœuds en catégories. Après le regroupement, des modèles de comportement représentatifs pour chaque catégorie en tant que modèles de comportement sont sélectionnés qui sont ensuite utilisés pour identifier les modèles de comportement étranges qui ne sont conformes à aucun modèle.

Chaque nœud correspond à une séquence. Une séquence est généralement extraite lorsque le montant de la transaction change au fil du temps pour le nœud, ce qui est dû au fait que le montant de la transaction est généralement la caractéristique la plus prédominante d'un nœud. Cependant, si une autre fonctionnalité du nœud est recherchée, cette fonctionnalité du nœud peut être extraite et utiliser la nouvelle séquence à la place.

L'algorithme BPC est similaire mais différent de l'algorthme k-means. Il faut d'abord initialiser les centres de cluster k. Puis on attribue chaque séquence à un groupe approprié, le nouveau centre du cluster est calculé puis on teste si l'itération du cluster converge.

Il existe trois différences principales entre le k-means et l'algorithme BPC. (1) kmeans

initialise les centres de cluster de manière aléatoire, tandis que BPC trie les séquences et sélectionne k séquences uniformément dans la liste triée. (2) le k-means utilise la distance euclidienne entre les tuples statiques, tandis que BPC utilise la distance DTW entre les séquences. (3) kmeans utilise la valeur moyenne des tuples dans le cluster comme centre de cluster pour ce cluster, tandis que BPC sélectionne la séquence avec la plus petite distance à son n/k ème voisin le plus proche parmi toutes les séquences du cluster comme centre du cluster.

3.1.6 Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering [CCR][14]

Les auteurs proposent un nouveau schéma de blockchain de consortium à des fins de cybersécurité du réseau véhiculaire. Le système est basé sur un smart contract et un consensus qui permet aux véhicules de détecter et de révoquer les véhicules malveillants en temps réel. Premièrement, un cadre est conçu pour intégrer la technologie blockchain pour se protéger contre les fausses attaques basées sur la position. Deuxièmement, il vise à créer des réseaux de blockchain dynamiques pour la gestion décentralisée de la confiance embarquée sur des véhicules. De plus, il permet la révocation de manière coopérative entre les véhicules, en tenant compte des changements de pseudonyme.

Le modèle de consortiums Blockchain est basé sur la preuve de la position de chaque véhicule dans les clusters et le partage des décisions sur le comportement des véhicules entre tous les participants. Les auteurs tentent de construire des communautés et de permettre à un processus coopératif de transmettre périodiquement des CAM (Cooperative Awareness Messages). Lorsque le véhicule est allumé, son module de communication sans fil commence à transmettre des messages CAM périodiques. A l'initialisation, le véhicule n'a pas encore connaissance de son voisinage pour détecter et révoquer les véhicules malveillants. Le processus de construction de la communauté est déclenché lorsque le véhicule reçoit plusieurs messages CAM, avec des pseudonymes différents.

Une fois qu'un véhicule reçoit les messages CAM, il enregistre les identifiants des véhicules dans un délai Thar et envoie la liste au TMC (Traffic Management Center). Ainsi, le TMC reçoit plusieurs listes après le delai Thar. Après concaténation des listes, le TMC obtient un graphe. Ensuite, sur la base des règles de graphe suivantes, le TMC émet la liste initiale de la communauté avec un identifiant de cluster (IDclus). Les véhicules de la communauté utiliseront leurs pseudonymes comme jetons pour signer lestransactions afin d'éviter tout risque de pistage.

1. Au début de la procédure de clustering, chaque nœud est dans un état initial. Ensuite, le système initialise un timer (Thar), pendant lequel les véhicules échangent et collectent des CAM pour former leur table de voisinage à un saut (NS).
2. Premièrement, le TMC doit traiter les conditions des véhicules afin d'identifier les meilleurs candidats OBU (On Board Unit) pour la communauté. Ensuite, il sélectionne le cluster head (CH). Le NS représente une liste de véhicules voisins qui présentent un modèle de mobilité similaire, se déplaçant dans la même direction. Le TMC décide ensuite si le véhicule peut être candidat à la communauté. Pour cela, le temps de liaison (Tlink) doit être inférieur à un seuil prédéterminé Tth.
3. Le véhicule ayant le temps de liaison le plus long est le plus susceptible de prendre la tête de cluster. Ensuite, le CH reçoit la liste (Listcom) des véhicules susceptibles de contribuer à la communauté.
4. Lorsqu'un véhicule Vj reçoit un message de formation de cluster du TMC, il envoie immédiatement un message ReqJoin à CHi. Une fois que CHi reçoit le message ReqJoin, il vérifie d'abord si cet ID est disponible dans Listcom. Si tel est le cas, CH ajoute Vj à sa liste de membres de cluster Gcom et renvoie un message ACKJoin ; sinon, il ignore la demande d'adhésion.

3.2 Récapitulatif

On a résumé les propositions des différents travaux en répondant aux questions suivantes : pour quoi la clusterisation ? quels sont les paramètres pertinents ? un Cluster Head (CH) est il nécessaire ? et enfin comment est formé le cluster ?

3.2.1 Objectif de la clusterisation

La clusterisation est utilisé pour la sélection de l'autorité de certification (CA) dans un système à clé PKI dans [CTB] et pour sélection les blocs à mettre sur le cloud et alléger la blockchain dans [Cloud].

Dans [Vanet] Elle aide à réduire les communications V2V, V2I, I2I (overhead ratio) et dans [CPS] elle aide à réduire la nécessité de synchroniser les données entre plusieurs noeuds (périphériques).

Elle permet aussi la détection des comportements anormaux dans une blockchain [Behavior] et pour détecter les véhicules malveillants et les révoquer [CCR].

3.2.2 Selection d'un cluster head (CH)

Dans [CTB] le noeud ayant le niveau de confiance le plus élevé et sélectionné comme CH et devient l'autorité de certification pour l'ensemble du cluster, de même pour [Vanet]le niveau de confiance indique le nœud CH et il gère les communications dans son cluster. Des CH auxiliaires sont aussi prévus pour l'évaluation de la confiance.

Le CH est choisi par le TMC et maintient une liste des véhicules de son cluster dans [CCR].

Les propositions données dans [CPS], [Cloud] et [Behavior] ne nécessitent pas de CH. La clusterisation est ici utilisé principalement comme classification.

3.2.3 Algorithme utilisé

L'algorithme K-means clustering est utilize dans [CTB], et un nouvel algorithme BPC proche de K-means clustering est utilisé dans [Behaviour].

Dans [Vanet] un noeud rejoint un voisin (un cluster) si son niveau de confiance est supérieur à un seuil et dans [CPS] un noeud rejoint un voisin (un cluster) si le taux des communications (densité) est supérieur à un seuil.

Un noeud rejoint un cluster si son ID existe dans la liste du CH dans [CCR], les listes étant formés par le TMC suivant un graphe de communications.

Un nouvel algorithme NSGA-C pour résoudre une fonction multi-objectives (problème de classification) est utilisé dans [Cloud]

3.3 Synthèse

D'après les travaux étudiés, la clusterisation est utilisé pour diverses raisons mais surtout pour réduire le nombre de nœuds qui effectuent une opération quelconque. Celaréduit le temps de communications et sa densité, le temps d'exécution, le temps de réponse, le nombre de requêtes à gérer etc.

La présence d'un CH n'est pas toujours nécessaire, sauf si on veut attribuer un rôle spécifique avec des fonctions spécifiques à un nœud particulier. La sélection du CH dépend de l'objectif de la clusterisation (niveau de confiance, puissance, capacité de stockage) etc.

Dans notre problématique, notre objectif ressemble à celui de [CPS] qui est de sélectionner un miner pour un sous ensemble de nœuds dans une blockchain. Donc, les nœuds de la blockchain seront clusterisés et un CH sera sélectionné pour qu'il devienne le miner de son cluster. Notre objectif rejoint celui de [cloud] car le problème est la difficulté de maintenance d'une blockchain.

3.4 Conclusion

Les articles examinés mettent en évidence le rôle essentiel de la technologie blockchain dans l'amélioration de l'efficacité, de la sécurité et de la collaboration dans divers domaines. L'utilisation du regroupement et de techniques avancées de clustering dans ces systèmes blockchain offre des avantages significatifs.

Les approches de regroupement basées sur la blockchain permettent de résoudre divers problèmes, tels que l'optimisation des communications, la gestion des certificats, la détection des comportements malveillants et l'optimisation du stockage des données. En exploitant les caractéristiques de la blockchain, telles que la transparence, l'immutabilité des données et la décentralisation, ces approches offrent des solutions innovantes et prometteuses.

L'utilisation du regroupement renforce la confiance dans les transactions et les communications en créant des sous-groupes de nœuds ou d'entités ayant des caractéristiques similaires. Cela facilite la vérification des informations, la détection des anomalies et la prévention des attaques malveillantes. De plus, le regroupement permet d'améliorer les performances des systèmes blockchain en réduisant les coûts de stockage, en augmentantla scalabilité et en facilitant la prise de décision.

Cependant, il convient de noter que chaque approche de regroupement et d'utilisation de la blockchain présente ses propres avantages et limites. Il est important de prendre en compte les spécificités du domaine d'application et les exigences du système pour choisir la meilleure approche. De plus, des recherches supplémentaires sont nécessairespour explorer davantage ces concepts, résoudre les défis techniques et développer des solutions pratiques et adaptées à chaque domaine.

En résumé, les articles examinés démontrent le potentiel de la technologie blockchain et du regroupement pour améliorer différents aspects des systèmes décentralisés. Ces recherches contribuent à l'avancement des connaissances dans le domaine de la blockchain et offrent des perspectives stimulantes pour le développement de solutions innovantes dans des domaines tels que les réseaux pair-à-pair, les systèmes de transport intelligents, la fabrication intelligente, le stockage sur le cloud et bien d'autres.

CHAPITRE 4

PROPOSITION

La validation des transactions dans un système de blockchain peut être coûteuse en raison de la consommation d'énergie, des besoins en puissance de calcul et du stockage. Pour réduire ces coûts, il est souvent nécessaire de regrouper les nœuds de validation dans des clusters et d'utiliser un nœud commun pour la validation entre ces clusters. La clustérisation permet de réaliser des économies d'échelle, d'optimiser l'utilisation des ressources, de réduire la consommation d'énergie et de mieux gérer la bande passante et le stockage. L'utilisation d'un nœud commun facilite la coordination et la validation efficace des transactions à travers les clusters.

Dans notre cas, nous avons pensé à utiliser l'algorithme des ensemble d'arbitres proposé par Raynal [21] comme méthode de clustering.

4.1 Principe des permissions d'arbitres

Dans les systèmes répartis, plusieurs entités autonomes, telles que des processus ou des machines, collaborent pour atteindre un objectif commun. La synchronisation est un aspect essentiel de ces systèmes, car elle permet de coordonner les actions des différentes entités et de garantir un comportement cohérent.

Le principe des permissions d'arbitres est une approche utilisée pour résoudre les problèmes de concurrence dans les systèmes répartis. Un arbitre, qu'il soit centralisé ou distribué, est chargé d'examiner les demandes d'accès des processus et d'accorder les permissions en fonction des règles prédéfinies. Son rôle principal est de garantir l'exclusion mutuelle, c'est-à-dire qu'un seul processus peut accéder à la ressource partagée à la fois. L'arbitre vérifie les conditions d'accès, accorde la permission si elles sont remplies, et bloque les autres processus en attente. Cela assure un ordre d'accès cohérent et évite les conflits d'accès concurrents. Cependant, l'utilisation d'un arbitre peut introduire des points de défaillance uniques et limiter la scalabilité du système.

A l'inverse dans les algorithmes à permissions d'arbitres, un site i n'accorde sa permission à un moment donné qu'à un seul autre site parmi ceux qui l'ont sollicitée. Toutefois un site qui a obtenu toutes les permissions qu'il a demandé doit les rendre à sa sortie de section critique. Pour réaliser cela on considère les règles ou contraintes sur la construction des ensembles d'arbitres. La première règle à respecter est :

$$\forall i, j : Ri \cap Rj \neq \emptyset$$

Cette condition assure que 2 sites ou nœuds quelconques demandent la permissionà au moins un site commun qui décidera lequel des deux obtiendra la section critique. Celui-ci joue le rôle d'arbitre pour leurs conflits. La figure suivante montre deux sites A et B qui veulent accéder à la section critique. Chacun sollicite donc son ensemble d'arbitre, en gras sur le schéma, pour obtenir leurs permissions. Si le site A est le premier à obtenir la permission de leur arbitre commun alors il va accéder à la section critique. Le site B sera donc empêché d'accéder à la section critique. Il va attendre son tour et n'obtiendra la permission jusqu'à ce qu'elle soit remise à l'arbitre par le site A.

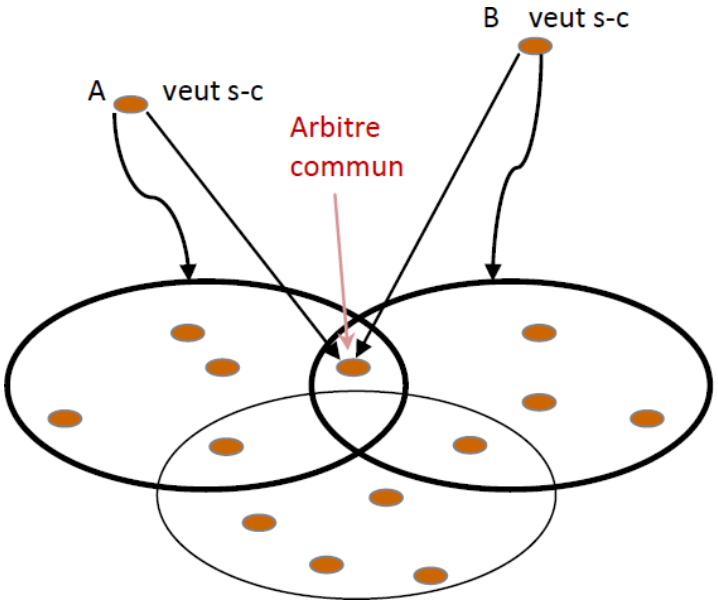

Figure 4.1: Rôle décisif d'un arbitre.

4.2 Contraintes sur les ensembles Ri

Le but de poser ces deux contraintes est d'obtenir un algorithme réparti « symétrique » dans lequel chaque noeud va jouer le même rôle que les autres. Ces contraintes s'énoncent comme suit :

(c1) :A$icard(i) = K$

(c2) :Ai : i est contenu dans D ensembles Rj
La construction des ensembles en annexe.

4.3 Approche proposée

4.3.1 Introduction

Dans notre approche, nous avons utilisé le principe des ensembles d'arbitre pour faciliter la validation des transactions dans notre système distribué. Ils permettent de coordonner l'accès à des ressources partagées, comme c'est le cas dans une blockchain où plusieurs nœuds doivent se mettre d'accord sur la validité des transactions.

La figure suivante illustre le cas optimal de 7 nœuds :

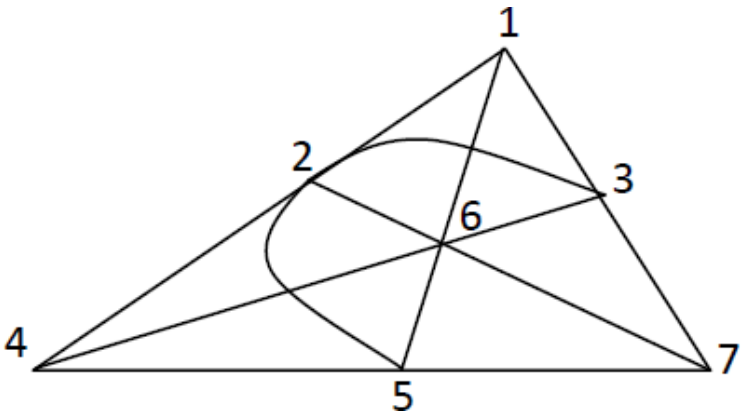

Figure 4.2: Plan projectif fini d'ordre 2.

Les ensembles d'arbitres :

R1= {1,2,4}

R2= {2,6,7}

R3= {1,3,7}

R4= {3,4,6}

R5= {2,3,5}

R6= {1,5,6}

R7= {4,5,7}

Dans cette approche, le nœud 1(émetteur) crée un bloc contenant la transaction et procède à une sélection parmi les clusters auxquels il est connecté, tels que R1, R3 et R6. Supposons que le nœud 1(émetteur) choisisse le cluster R1. Le bloc est alors soumis au cluster R1, composé des nœuds 1, 2, 4. Les nœuds du cluster R1 effectuent un processus de consensus interne pour valider la transaction contenue dans le bloc. Ce processus de consensus peut impliquer des mécanismes tels que la preuve de travail.

Une fois que le consensus est atteint au sein du cluster R1, le nœud 1(émetteur) diffuse le bloc contenant la transaction validée aux autres clusters auxquels il appartient,c'est-à-dire R3 et R6. Les nœuds des clusters R3 (nœuds 1, 3, 7) et R6 (nœuds 1, 5, 6) reçoivent le bloc et l'enregistrent dans leur blockchain.

4.3.2 L'algorithme proposé

Création de la transaction

1. Choix l'émetteur et récepteur
2. Signature de la transaction avec la clé privée de l'émetteur

Assemblage de la transaction

1. Ajout de la transaction au pool de transactions en attente

Construction de l'entête du bloc

1. Calcul du hachage du bloc précédent
2. Ajout de l'horodatage de l'émetteur
3. Définition de la version du protocole
4. Initialisation du nonce à zéro

Création du bloc

1. Construction de l'entête du bloc
2. Calcul de la preuve de travail
3. Validation du bloc

Choix du cluster

1. Créer une liste vide "groupes valideurs"
2. Parcourir chaque cluster
   Si le nœud émetteur fait partie du groupe
   Ajouter le groupe à la liste "groupesvalideurs"
3. Sélectionner aléatoirement un groupe parmi "groupesvalideurs"

Algorithm 1: Algorithme principal (chez l'emetteur)

```
While vrai
    if la création de la transaction est réussie then
        Sélection du cluster par le nœud émetteur pour la validation
        Création du bloc
        Diffusion du bloc dans le cluster selectionné par le nœud émetteur
        Validation du bloc par chaque nœud dans le cluster selectionné
        if le bloc est valide then
            Enregistrement du bloc
            Diffusion du bloc validé sur les autres clusters
        else
            Marquer la transaction comme échouée
        end
    end
end
```

Algorithm 2: Algorithme (chez le nœud appartenant au cluster selectionné)

```
Lors de la réception d'un bloc de l'émetteur
    Exécuter la preuve de travail
    if preuve réussi then
        Valider le bloc
        Informer l'émetteur "bloc valide"
        Enregistrer le bloc
    else
        Informer l'émetteur "bloc non valide"
    end
end
```

Algorithm 3: Algorithme (chez le nœud appartenant aux autres clusters)

```
Lors de la réception d'un bloc validé
    Enregistrement du bloc
```

4.3.3 Description de la solution proposée

La première partie de l'algorithme concerne la création et l'assemblage des transactions. Tout d'abord, un émetteur et un récepteur sont choisis pour la transaction.Ensuite, la transaction est signée avec la clé privée de l'émetteur pour garantir son authenticitéet son intégrité. Une fois signée, la transaction est ajoutée au pool de transactions en attente, qui est une liste de toutes les transactions en attente d'inclusion dans un bloc.

Ensuite, l'algorithme se concentre sur la construction de l'entête du bloc. L'entête contient des métadonnées importantes. Tout d'abord, le hachage du bloc précédent est calculé. Cela crée une référence au bloc précédent dans la chaîne, assurant ainsi la continuité de la blockchain. Ensuite, l'horodatage actuel est ajouté à l'entête pour enregistrer le moment où le bloc est créé. La version du protocole est également définie dans l'entête pour indiquer la version utilisée. Enfin, le nonce est initialisé à zéro. Le nonce est un nombre utilisé dans le processus de preuve de travail pour trouver un résultat satisfaisant.

Une fois que l'entête du bloc est construit, l'algorithme passe à la création du bloc lui-même. Le bloc est créé en ajoutant l'entête et les transactions valides du pool de transactions en attente. Ensuite, la preuve de travail est calculée pour le bloc.Une fois que la preuve de travail est trouvée, le bloc est considéré comme valide et peut être ajouté à la blockchain.

Ensuite, l'algorithme effectue une étape de choix de cluster.l'algorithme vérifie si le nœud émetteur (celui qui crée la transaction) fait partie du groupe. Si c'est le cas, le groupe est ajouté à la liste "groupes valideurs". Ensuite, un groupe est sélectionné aléatoirement parmi les groupes de la liste "groupes valideurs".

L'algorithme principal se déroule chez l'émetteur.Il commence par créer la blockchain clustérisée en effectuant le clustering des nœuds.Si la création de la transaction est réussie, l'émetteur sélectionne un cluster pour la validation. Le bloc est créé en suivant les étapes de construction de l'entête et de création du bloc.Le bloc est ensuite diffusé dans le cluster sélectionné par le nœud émetteur. Chaque nœud dans le cluster sélectionné valide le bloc. Si le bloc est valide, il est enregistré et diffusé sur les autres clusters. Si le bloc n'est pas valide, la transaction est marquée comme échouée.

Chez les nœuds appartenant au cluster sélectionné, lorsqu'ils reçoivent un bloc de l'émetteur, ils exécutent la preuve de travail pour vérifier sa validité. Si la preuve de travail réussit, le bloc est validé et le nœud informe l'émetteur que le bloc est valide.

Ensuite, le bloc est enregistré dans la blockchain du nœud.

Chez les nœuds appartenant aux autres clusters, lorsqu'ils reçoivent un bloc validé provenant d'un autre cluster, ils l'enregistrent dans leur propre blockchain.

4.4 Conclusion

Nous avons proposé, dans cette partie, notre algorithme basé sur le principe des ensembles d'arbitres et la technique de clustering blockchain, Nous avons décrit son fonctionnement. Notre approche présente plusieurs avantages, tels que des économies d'échelle, une meilleure utilisation des ressources, une réduction de la consommation d'énergie et les coûts et une gestion améliorée de la bande passante et du stockage. De plus, elle permet une coordination efficace des nœuds de validation à travers les clusters, ce qui facilite la validation des transactions dans un système distribué.

Cependant, il est important de noter que notre approche n'est qu'une proposition et peut être adaptée en fonction des besoins spécifiques d'un système de blockchain donné.

Conclusion générale

!'objectif de notre travail consiste à la réalisation d'un algorithme qui puisse parvenir à améliorer la validation dans les réseaux Blockchain.

Pour ce faire nous avons commencé par dresser un panorama général de la blockchain. Nous avons exploré les avantages de la blockchain en termes de sécurité, de transparence et d'efficacité, ainsi que les défis auxquels elle est confrontée.

Ensuite, nous avons étudié la validation des transactions dans la blockchain. Nous avons examiné les mécanismes de validation tels que la preuve de travail, la preuve d'enjeu et d'autres algorithmes de consensus, en évaluant leurs avantages et leurs inconvénients. Nous avons également abordé les implications de ces algorithmes.

Dans un second temps, nous avons exploré l'utilisation du clustering dans la blockchain. Nous avons étudié les différentes approches de clustering utilisées pour optimiser les performances du réseau, en analysant leurs avantages et leurs limites. Nous avons également mis en évidence les considérations de sécurité et de gestion des ressources liées à l'utilisation du clustering dans la blockchain.

Enfin, nous avons présenté une proposition novatrice pour améliorer la validation dans la blockchain en combinant un algorithme de consensus spécifique avec des techniques de clustering. Il s'agit de l'algorithme à permissions d'arbitres qui permet un clustering optimal avec un nœud commun pour assurer la cohérence. Lors de la réalisation de ce travail on a eu à étudier le concept de blockchain et les algorithmes de consensus. On a réussi à proposer une nouvelle méthode de clustering que nous pensons être performante.

Evidemment le travail n'est pas complet, il nous reste à l'évaluer par simulation ou par utilisation réelle et aussi à proposer son implémentation avec un algorithme de consensus sur une blockchain.

BIBLIOGRAPHY

[1] *https://academy.binance.com/en/articles/proof-of-authority-explained (consulté avril 2023).*

[2] *https://academy.binance.com/en/articles/proof-of-stake-explained (consulté avril 2023).*

[3] *https://academy.binance.com/fr/articles/history-of-blockchain , (consulté le 24 avril 2023).*

[4] *https://academy.binance.com/fr/articles/proof-of-stake-explained.(consulté avril 2023).*

[5] *https://coinacademy.fr/academie/preuve-participation-deleguee-dpos/ (consulté avril 2023).*

[6] *https://coinacademy.fr/gavin-wood/ (consulté avril 2023).*

[7] *https://www.geeksforgeeks.org/proof-of-elapsed-time-poet-in-blockchain/ (consulté mai 2023).*

[8] *https://www.smartgrids-cre.fr/encyclopedie/la-blockchain-appliquee-alenergie/une-grande-variete-de-blockchain, (consulté le 25/04/2023).*

[9] P. ADAM-KALFON, *Blockchain, catalyseur de nouvelles approches en assurance*, (2018).

[10] R. P. B. S. Amrutanshu Panigrahi, Ajit Kumar Nayak AND S. Kant, *Ctb- pki: Clustering and trust enabled blockchain based pki system for efficient communication in p2p network*, (2022).

[11] A. O. Ayadi, *Etat de l'art de la blockchain dans : Analyse et étude de la sécurité des données médicales dans l'internet des objets à partir d'une approche technologique blockchain, mémoire de master professionnel en informatique, réseaux et systèmes distribués, université constantine 2*, (2019).

[12] G. D. Bikramaditya Singhal AND P. S. Panda., *Beginning blockchain : A beginner's guide to building blockchain solutions*, (2018).

[13] Z. L. BUTIAN HUANG AND Q. HE, *Behavior pattern clustering in blockchain networks*, (2017).

[14] A. Didouh, H. Labiod, Y. E. Hillali, AND A. Rivenq, *Blockchain-basedcollaborative certificate revocation systems using clustering*, (2022).

[15] C. DOROTHE, *Blockchain,la révolution de l'économie de partage*, (2017).

[16] R. A. GOLOSOVA, J., *The advantages and disadvantages of the blockchain technology*, (2018).

[17] K.AWAN AND A. ALMOGREN, *A blockchain-assisted trusted clustering mechanism for iot-enabled smart transportation system.*, (2022).

[18] M.GUILLAUME, *C'est quoi un bloc sur la blockchain*, https://www.cryptovore.fr/cryptoschool/cest-quoi-un-bloc/ *, (consulté avril 2023).*

[19] V. G. PAULO VERÍSSIMO AND C. NATOLI., *Deconstructing blockchains: A comprehensive survey on consensus,membership and structure*, (2019).

[20] D. PUTHAL, N. MALIK, S. P. MOHANTY, E. KOUGIANOS, AND G. DAS, *Everything you wanted to know about the blockchain: Its promise, components, processes,and problems*, IEEE Consumer Electronics Magazine, 7 (2018), pp. 6–14.

[21] M. RAYNAL, *Synchronisation et état global dans les systèmes répartis, Eyrolls, Paris*, 1992.

[22] V. SAINI., *consensus blockchain.https ://hackernoon.com, (consulté avril) 2023*.

[23] S. S. SARMAH, *Understanding blockchain technology*, Computer Science and Engineering, (2018).

[24] SATOSHI NAKAMOTO, *bitcoin: a peer-to-peer elctronic cash system*, (http://bitcoin.org/bitcoin.pdf ,2008).

[25] H. X. SUISHENG LI AND S. LIU, *Blockchain dividing based on node community clustering in intelligent manufacturing cps.*, (2019).

[26] S. N. SUNNY KING, *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake*, (2012).

[27] M. XU, G. FENG, AND X. ZHANG, *On cloud storage optimization of blockchain with a clustering-based genetic algorithm*, (2020).

[28] D. Yafimava, *Blockchain insight. openledger*, (2019).

Construction d'ensembles Ri optimaux

Pour construire des ensembles Ri optimaux, on cherchera à minimiser les valeurs de K et D précédemment citées. Mais le plus important encore est de savoir construire ces ensembles d'arbitres. Dans la suite de notre travail, on ne va pas donner de méthodes de construction mais uniquement quelques unes de leurs propriétés. Par ailleurs, notre travail va concerner le routage des messages entre les noeuds en utilisant ces ensembles pour contrôler leur propagation à travers le réseau.

Considérons un ensemble Ri. La contrainte (c2) permet de déduire que tout élément j de Ri appartient à (D-1) autres ensembles ; or suivant la contrainte (c1) il y a K éléments dans Ri. On déduit que le nombre maximum d'ensembles qui peuvent être construits et qui satisfont la propriété d'intersection $Ri \cap Rj = \emptyset$ est égal 1+K(D-1).

Les contraintes (c1) et (c2) lient les valeurs K et D. On obtient n=K*n/D avec n est le nombre de noeuds dans le réseau. On a divisé le nombre total (union de tous les ensembles) des noeuds sur le nombre de fois qu'ils sont répétés. Le cas optimal où la répétition est réalisée exactement D fois permet de déduire que K=D. Ainsi on déduit que le nombre maximum d'ensemble est 1+K(D-1) = 1+K(K-1) = n, on a autant d'ensembles d'arbitres que de noeuds. Cette dernière formule est équivalente à $K = \theta \cdot \sqrt{n}$, cela veut dire que le cardinal des ensembles d'arbitres est proportionnel à $\sqrt{n}$, la racine carrée du nombre de noeuds.

Construction d'ensembles Ri presque optimaux

Cette approche est très intéressante du fait que même si on ne dispose pas d'un nombre de noeuds satisfaisant , on peut quand même construire des ensembles d'arbitres, appelés des ensembles presque optimaux. Ainsi, dans le cas où il n'existe pas de plans projectifs finis deux attitudes sont possibles :

- **Affaiblir les contraintes c1 et c2:**
  On cherche l'ordre k du premier plan projectif que l'on sait construire tel que n k(k+1)+1 et l'on crée k(k+1)+1-n sites fictifs supportés de façon la plus équitable possible, par les sites effectifs. C'est-à-dire on augmente le nombre n de noeuds avec le nombre fictif nécessaire pour atteindre le nombre qui permettra la construction du prochain plan projectif fini. Ensuite, on répartit équitablement les noeuds fictifs

sur les noeuds effectifs et lors de la construction on remplace les noeuds fictifs par les noeuds effectifs qui leur correspondent. Si on reprend l'exemple précédent avec 5 noeuds seulement, on place les sites fictifs 6 et 7 sur les sites effectifs 2 et 5 respectivement et on confond 6 avec 2 et 7 avec 5, on obtient les ensembles d'arbitres :

R1 = {1,2,4}
R2 = {2,5}
R3 = {1,3,5}
R4 = {2,3,4}
R5 = {2,3,5}

- **Ne plus chercher des ensembles Ri de taille minimale:**

  Dans ce cas il existe une solution très simple. On regroupe les n sites dans une matrice carrée de taille $\lceil \sqrt{n} \rceil$ et l'ensemble Ri d'un site contient les sites placés sur la même ligne et la même colonne que lui. Toutefois la solution n'est pas optimale car deux ensembles Ri et Rj peuvent avoir de $2\lceil \sqrt{n} \rceil$ à éléments en commun, or dans le cas optimal l'intersection est un singleton. La construction des ensembles pour l'exemple précédent composé de 5 noeuds nous donne un ensemble R5 de cardinalité égale à 6.

  R5={12,8,5,9,13,10}

(-

ABSTRACT

A blockchain is a decentralized network where participants can securely perform transactions without the need for a central authority. The nodes in the network must reach a consensus on the validity of transactions by using a consensus algorithm.

In this thesis, an innovative proposal based on the use of clustering for the validation process in a blockchain using the principle of arbitration sets has been presented. The main objective of this study is to explore how clustering can be applied to improve the validation process in a blockchain.

For this, a study on blockchain and clustering has been conducted on recent articles.

Keywords: Blockchain, Clustering, Validation, referee permissions principals.

RÉSUMÉ

Une blockchain est un réseau décentralisé où les participants peuvent effectuer des transactions en toute sécurité, sans avoir besoin d'une autorité centrale. Les nœuds du réseau doivent parvenir à un accord sur la validité des transactions en utilisant un algorithme de consensus.

Dans ce mémoire, une proposition novatrice basée sur l'utilisation du clustering pour le processus de validation dans une blockchain en utilisant le principe des ensembles d'arbitre a été présenté. L'objectif principal de cette étude est d'explorer comment le clustering peut être appliqué pour améliorer le processus de validation dans une blockchain. Pour cela une étude sur la blockchaine , le clustering a été effectué sur des articles récents

Mots clés : Blockchain, Clustering, La validation, Principe Ensembles d'arbitre.