Bibliography

[1] Yasmine Bachi. *Sélection des nœuds gateway dans une architecture Blockchain multi-tiers pour l'IoT*. 2021.

[2] Ying-Chang Liang. *Blockchain for Dynamic Spectrum Management*. 2020.

[3] Aktouche Sadek Rayan and Righi Sylia. *Intégration de la technologie Blockchain dans les systèmes de collaboration inter-entreprises*. 2021.

[4] Habibeche Sakina and Fartas Hesna. *Conception et réalisation d'un système sécurisé de gestion des Dossiers Médicaux Utilisant la blockchain*. 2024.

Table des matières

Chapter 1

Les Concepts

Dans un monde où la numérisation des échanges et des transactions s'intensifie, la gestion sécurisée et fiable des données devient un enjeu majeur.
La blockchain, une technologie émergente basée sur un registre distribué et immuable, se présente comme une solution innovante
En garantissant trois principes fondamentaux de la sécurité des systèmes d'information : l'intégrité, l'authentification et la disponibilité.

Grâce à la cryptographie, elle assure l'intégrité des données en empêchant toute modification frauduleuse.
L'authentification est garantie par des signatures numériques et des protocoles de consensus, qui permettent de vérifier l'identité des utilisateurs et d'assurer la fiabilité des transactions. Dans les blockchains privées, ces mécanismes sont renforcés par des accès restreints, offrant un meilleur contrôle sur les acteurs du réseau. Enfin, **sa nature décentralisée garantit une disponibilité continue des informations**, réduisant ainsi le risque de panne ou de manipulation.
Ce chapitre expliquera ces concepts et montrera comment la blockchain, qu'elle soit publique ou privée. et leur utilisations dans différents domaines comme la finance, la logistique et l'identité numérique.

1.1 Définition

La blockchain est une technologie permettant de stocker et de transmettre des informations de manière sécurisée et sans intermédiaire. Elle fonctionne comme un registre distribué où les données sont organisées en blocs liés chronologiquement et protégées par la cryptographie.

Chaque bloc contient des transactions validées par un protocole de consensus (Proof of Work, Proof of Stake,Proof of History, etc.), garantissant l'intégrité

et la transparence des données. Une fois enregistrées, ces données ne peuvent pas être modifiées.

D'abord utilisée pour les cryptomonnaies (Bitcoin, Ethereum), la blockchain est aujourd'hui appliquée dans plusieurs secteurs comme la finance, la logistique et la santé. Son fonctionnement décentralisé réduit les fraudes, améliore la sécurité et renforce la confiance entre les utilisateurs.

1.2 L'importance Blockchian

Les technologies traditionnelles de bases de données présentent plusieurs défis pour l'enregistrement des transactions financières. Prenons l'exemple de la vente d'une propriété. Une fois l'argent échangé, la propriété du bien est transférée à l'acheteur. Individuellement, l'acheteur et le vendeur peuvent enregistrer les transactions monétaires, mais on ne peut se fier à aucune de ces sources. Le vendeur peut facilement prétendre qu'il n'a pas reçu l'argent même s'il l'a reçu, et l'acheteur peut tout aussi bien prétendre qu'il a payé la somme même s'il ne l'a pas fait.

Pour éviter les problèmes juridiques potentiels, un tiers de confiance doit superviser et valider les transactions. La présence de cette autorité centrale complique non seulement la transaction, mais crée également un point de vulnérabilité unique. Si la base de données centrale était compromise, les deux parties pourraient en souffrir.

Blockchain atténue ces problèmes en créant un système décentralisé et inviolable pour enregistrer les transactions. Dans le scénario de la transaction immobilière, Blockchain crée un grand livre pour l'acheteur et pour le vendeur. Toutes les transactions doivent être approuvées par les deux parties et sont automatiquement mises à jour dans leurs deux grands livres en temps réel. Toute corruption des transactions historiques corrompt l'ensemble du grand livre.

1.3 Type de blockchain

Il existe plusieurs types de blockchains, chacun se distinguant par sa gestion des permissions d'accès, de visualisation des données, de validation des transactions et d'ajout de nouveaux blocs à la chaîne. en trouve 4 types principaux : la blockchain publique, privée, hybride et la blockchain de consortium.[4]

1.3.1 Blockchain publique

Une blockchain publique, aussi appelée permissionless, est un réseau ouvert où n'importe qui peut rejoindre et participer au processus de validation des transactions. Tous les membres disposent des mêmes droits pour lire, modifier et valider la blockchain. Ce type de réseau est utilisé principalement pour l'échange et le minage de crypto-monnaies comme Bitcoin, Ethereum et Litecoin. Cependant, il présente certaines limites, notamment une forte consommation d'énergie (dans le cas des blockchains basées sur la preuve de travail PoW). Malgré ces défis, les blockchains publiques restent des systèmes décentralisés et transparents, garantissant une sécurité élevée grâce à la cryptographie.

1.3.2 Blockchain privee

Une blockchain privée, aussi appelée blockchain autorisée, est un réseau fermé où l'accès est limité aux participants autorisés. Contrairement aux blockchains publiques, elle est souvent contrôlée par une seule entité ou un groupe restreint, qui régule les permissions d'affichage, d'écriture et de validation des transactions. Ce type de blockchain est particulièrement adapté aux entreprises et aux institutions souhaitant exploiter les avantages de la technologie tout en maintenant un haut niveau de confidentialité et de contrôle. Grâce à son architecture restreinte, la blockchain privée offre une vitesse de transaction élevée et une meilleure efficacité énergétique.

1.3.3 Blockchain hybrides

Une blockchain hybride combine les caractéristiques des blockchains publiques et privées, offrant ainsi un équilibre entre transparence et confidentialité. Dans ce modèle, certaines informations et transactions sont accessibles à tous, comme dans une blockchain publique, tandis que d'autres sont restreintes aux participants autorisés, comme dans une blockchain privée. Cela permet aux entreprises et aux organisations d'utiliser la blockchain tout en

contrôlant l'accès aux données sensibles. La blockchain hybride offre plusieurs avantages, notamment une meilleure évolutivité, une sécurité renforcée

1.3.4 Blockchain de consortium

Un groupe d'organisations régit les réseaux blockchain de consortium. Des organisations présélectionnées se partagent la responsabilité de la maintenance de la Blockchain et de la détermination des droits d'accès aux données plutôt qu'une entité unique (comme dans une blockchain privée) ou tous les participants (comme dans une blockchain publique). Les industries dans lesquelles de nombreuses organisations ont des objectifs communs et bénéficient d'une responsabilité partagée préfèrent souvent les réseaux blockchain de consortium. Par exemple, le Global Shipping Business Network Consortium est un consortium Blockchain à but non lucratif qui vise à numériser le secteur du transport maritime et à accroître la collaboration entre les opérateurs de ce secteur.

1.3.5 Comparaison entre les type de Blockchain :

Critères	Publique	Privée	Consortium	Hybride
Accès	Ouvert à tous	Restreint	Restreint à plusieurs entités	Mixte (public/privé)
Nœuds	Tout le monde	Un seul propriétaire	Groupe d'organisations	Contrôle sélectif
Consensus	Décentralisé (PoW, PoS)	Centralisé (PoA, pBFT)	Semi-décentralisé (pBFT, RAFT)	Flexible selon le cas d'usage
Vitesse	Lente	Rapide	Moyenne	Variable
Sécurité	Très élevée	Moyenne (dépend d'un seul acteur)	Élevée	Équilibrée
Évolutivité	Faible	Très élevée	Moyenne	Bonne
Exemples	Bitcoin, Ethereum	Hyperledger Fabric, Corda	R3 Corda, Quorum	IBM Food Trust, Ripple

TABLE 1.1 – Comparaison entre les types de Blockchain

1.4 Les composants et la structure

1.4.1 Composants de Blockchain

1. **Nœud (Node)** : Les nœuds sont les participants du réseau dont les appareils leur permettent de suivre le **ledger** distribué et d'agir comme des hubs de communication pour diverses tâches du réseau. Lorsqu'un **mineur** ajoute un nouveau bloc à la blockchain, celui-ci est diffusé à tous les nœuds du réseau.
2. **Transactions** : une transaction fait référence à un contrat ou un accord entre parties et implique le transfert d'argent ou de biens (comme exemple). Le réseau de la blockchain stocke les données transactionnelles sous forme de copies dans un ledger.
3. **Bloc (Block)** : Un bloc dans un réseau blockchain est une unité de stockage contenant un ensemble de transactions validées. Il fonctionne comme un maillon dans une chaîne, chaque bloc étant lié au précédent par un identifiant cryptographique unique appelé hash.

   Dans le domaine des cryptomonnaies, un bloc peut être comparé à une page d'un registre comptable où sont enregistrées les transactions avant d'être ajoutées de manière permanente et immuable à la blockchain. Chaque bloc contient :

   (a) Les transactions validées depuis le bloc précédent.
   (b) Un horodatage (timestamp) pour dater son ajout à la blockchain.
   (c) Le hash du bloc précédent, assurant la continuité et la sécurité de la chaîne.
   (d) Un hash unique, généré à partir des données du bloc, garantissant son intégrité.

   Cette structure permet de sécuriser et de suivre toutes les transactions effectuées, en assurant leur transparence et leur immuabilité.
4. **Chaîne (Chain)** : La chaîne est le concept qui relie tous les blocs entre eux grâce à un système de hachage. Chaque bloc est connecté au précédent via son **hash**, formant ainsi une structure enchaînée garantissant l'intégrité des données. Il existe plusieurs algorithmes de consensus (Proof of Work, Proof of Stake, Paxos, Raft, etc.), chacun ayant ses avantages et inconvénients.
5. **Mineurs (Miners)** :Le minage est le processus de validation et d'ajout de transactions à une blockchain, notamment dans les cryptomonnaies utilisant des mécanismes comme la Preuve de Travail (PoW) ou le Byzantine Fault Tolerance (BFT), en fonction du type de blockchain.

Les participants qui réalisent cette tâche sont appelés **mineurs**. Dans une blockchain publique, n'importe quel utilisateur peut devenir mineur, tandis que dans une blockchain privée, seuls des participants autorisés ont la capacité de valider les transactions et d'ajouter des blocs.

Les mineurs jouent un rôle clé dans le réseau en mettant à profit leur puissance de calcul pour résoudre des problèmes cryptographiques complexes. Leur mission consiste à[1] :

(a) Vérifier l'authenticité des transactions.
(b) Regrouper les transactions au sein d'un bloc.
(c) Ajouter ce bloc à la blockchain en résolvant une énigme mathématique.

Dans une blockchain publique, ce processus repose sur la **Preuve de Travail (PoW)**, qui exige des mineurs qu'ils résolvent un puzzle cryptographique complexe via un processus de hachage nécessitant une puissance informatique importante. Le premier mineur à trouver une solution valide obtient le droit d'ajouter un nouveau bloc à la blockchain et reçoit une récompense en cryptomonnaie, comme le Bitcoin.

6. **Consensus** : Le **consensus** est une caractéristique essentielle de la blockchain est qu'elle supprime la nécessité d'un tiers de confiance pour valider les transactions. À la place, un consensus est établi entre l'ensemble des nœuds avant qu'un bloc, regroupant plusieurs transactions, ne soit ajouté à la chaîne. Pour garantir une création impartiale des blocs et résister aux attaques malveillantes, un algorithme de consensus est mis en œuvre. Il en existe plusieurs, tels que la preuve de travail (PoW), la preuve d'enjeu (PoS) et la tolérance pratique aux pannes byzantines (PBFT), chacun étant adapté à différents types de blockchains et exigences de performance selon les applications.

1.4.2 Structure de Bloc

Un bloc est composé d'un en-tête et d'un corps, où un en-tête contient le hachage du bloc précédent, un horodatage, un Nonce et la racine Merkle. La racine Merkle est le hachage racine d'un arbre Merkle qui est stocké dans le corps du bloc.

1. **En-tête (Header)** : L'en-tête permet d'identifier un bloc spécifique dans la blockchain et assure la gestion des blocs au sein du réseau. Il joue un rôle crucial dans le processus de validation des blocs, notamment dans le minage, où les mineurs le hachent régulièrement en modifiant le nonce jusqu'à ce qu'ils trouvent une valeur répondant aux exigences du réseau. L'en-tête d'un bloc contient trois ensembles de métadonnées essentielles :

   (a) **Informations sur le bloc précédent** : inclut le *hash* du bloc précédent, garantissant ainsi la liaison entre les blocs et la sécurité de la blockchain.

   (b) **Informations sur le bloc actuel** : comprend des données comme le *horodatage* (*timestamp*) et la racine de l'*arbre de Merkle*, qui permet de vérifier l'intégrité des transactions contenues dans le bloc.

   (c) **Informations pour le consensus** : inclut la *valeur de la difficulté* et le *nonce*, utilisés dans le processus de minage (dans les blockchains PoW comme Bitcoin).

   (d) **Merkle Root** : Le **Merkle Root** est une structure de données qui organise et vérifie les transactions contenues dans un bloc. Elle est utilisée pour simplifier et accélérer la vérification des transactions dans un bloc. Comme une modification minime d'une transaction peut entraîner un changement radical du Merkle Root, la validation peut être effectuée en comparant uniquement cette racine, plutôt que de vérifier individuellement toutes les transactions du bloc.

2. **Body** :Contient principalement les transactions validées qui sont enregistrées dans ce bloc.

Voici un schema present la strctur de blockchain. Nous désignons une transaction par TX et prenons le 3eme bloc, qui ne contient que quatre transactions, comme exemple pour illustrer la structure d'un arbre de Merkle [2].

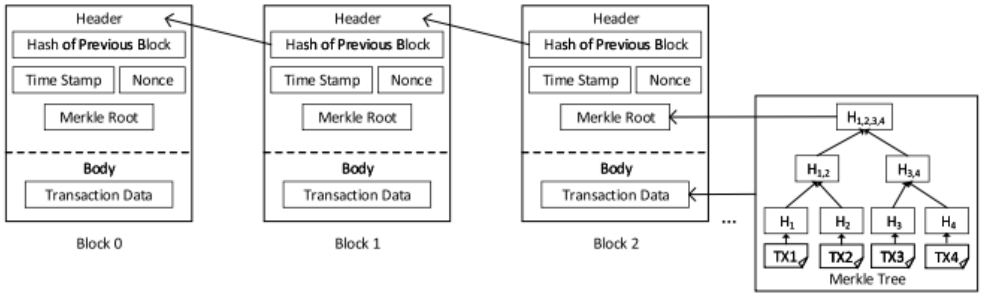

FIGURE 1.1 – Structure du Block

1.5 Caractéristiques essentielles de la Blockchain

1. **Décentralisation** : La blockchain permet d'effectuer des transactions entre deux nœuds sans passer par une autorité centrale. Cette absence d'intermédiaire garantit un système plus robuste, réduit les coûts liés aux services tiers et évite les risques de *Single Point of Failure (SPOF)* rencontrés dans les systèmes centralisés.
2. **Immutabilité** : Les transactions enregistrées dans la blockchain sont permanentes et ne peuvent être modifiées. Grâce au chaînage cryptographique entre les blocs et à l'utilisation du *Merkle Tree*, toute tentative de modification altérerait le hachage du bloc concerné, invalidant ainsi toute la chaîne de blocs qui en découle.
3. **Anonymat** : Les utilisateurs interagissent avec la blockchain via des adresses générées de manière pseudonyme, sans révéler leur identité réelle. Ils peuvent également créer plusieurs adresses afin de préserver leur confidentialité. L'anonymat est une caractéristique clé des blockchains publiques.
4. **Transparence** : L'ensemble des transactions effectuées sur le réseau est consultable par tous les participants. Cet historique, accessible en

permanence, garantit une transparence totale, notamment dans les blockchains publiques.

5. **Traçabilité** : Chaque transaction est enregistrée avec des métadonnées détaillées, telles que la date, l'identité cryptographique du propriétaire et d'autres informations pertinentes. Cela permet un suivi précis et fiable des actifs transférés au sein du réseau.
6. **Non-répudiation** : Une transaction validée ne peut être niée par ses auteurs. Grâce au mécanisme de signature cryptographique, chaque transaction est associée à une preuve d'authenticité garantissant son origine et empêchant toute contestation ultérieure.

Voici un schéma descriptif qui représente la Caracteristiques de Blockchain[1].

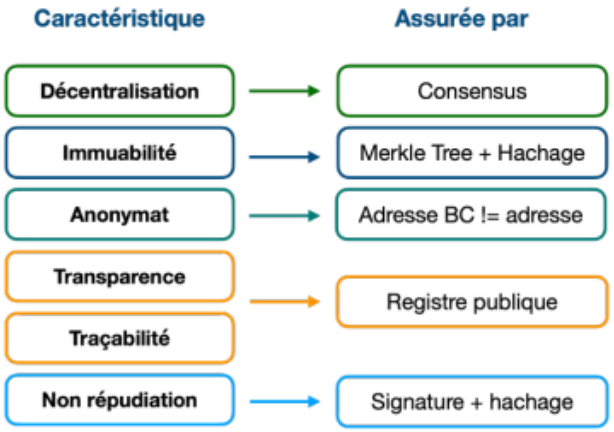

FIGURE 1.2 – Caractéristiques de Blockchain

1.6 Smart Contracts (SC)

un contrat écrit en code exécutable. Ils fonctionnent selon une logique conditionnelle de type SI-ALORS-SINON, permettant l'exécution automatique des clauses contractuelles dès que les conditions préétablies sont remplies. Par exemple, si un produit est livré, alors le compte du client est automatiquement débité[3].

Implémentés sur la blockchain (BC), les contrats intelligents y sont stockés de manière immuable, ce qui empêche toute modification ou falsification. Pour mettre à jour un contrat existant, il est nécessaire d'en déployer un nouveau.

Les principales caractéristiques des Smart Contracts incluent notamment :

1. Vérification automatique des conditions contractuelles.
2. Auto exécution des actions si une condition est satisfaite.

L'exécution de chaque clause d'un contrat intelligent (Smart Contract - SC) est consignée sous forme de transaction immuable sur la blockchain, garantissant ainsi la transparence et la traçabilité des actions effectuées.

Différents langages de programmation sont utilisés pour développer des Smart Contracts, en fonction de la plateforme blockchain choisie. Parmi les plus courants, on retrouve :

1. **Solidity** : Principalement utilisé pour les Smart Contracts sur Ethereum.
2. **Go** : Utilisé pour les Smart Contracts sur Hyperledger Fabric.
3. **Java** : Supporté par certaines blockchains d'entreprise comme Hyperledger Fabric et Corda.
4. **Node.js (JavaScript)** : Employé pour certaines plateformes blockchain et pour l'intégration avec des applications web.

Le choix du langage dépend donc de l'écosystème blockchain et des exigences techniques du projet.

1.7 Algorithmes de consensus :

Le consensus est le processus qui permet aux nœuds d'une blockchain de s'accorder sur la validation des blocs, même en l'absence de confiance mutuelle. Dans un système distribué, cette tâche est complexe, car des nœuds malveillants peuvent tenter d'influencer le processus.

Chaque blockchain utilise un algorithme de consensus adapté à ses besoins en termes de sécurité, rapidité de validation et nature des données. Dans la suite, nous présenterons les principaux algorithmes existants[2] :

1.7.1 Preuve de Travail (PoW - Proof of Work)

1. Algorithme largement utilisé, notamment dans Bitcoin.
2. Repose sur un processus de **minage** où les nœuds (mineurs) doivent résoudre un problème cryptographique en trouvant un **Nonce** (nombre aléatoire).
3. Ce Nonce est validé en vérifiant si le **hachage** du bloc satisfait certaines conditions.

4. **Caractéristiques** :
   (a) Sécurise le réseau en rendant les attaques très coûteuses.
   (b) Consomme une quantité importante de ressources informatiques et d'énergie.
   (c) Récompense les mineurs avec des tokens et des frais de transaction.

1.7.2 Preuve d'Enjeu (PoS - Proof of Stake)

1. Vise à réduire la consommation énergétique du PoW.
2. Un nœud est sélectionné pour créer un bloc en fonction du nombre de **tokens** qu'il possède et de la durée pendant laquelle il les détient.
3. **Caractéristiques** :
   (a) Diminue la consommation énergétique et la centralisation due aux puissances de calcul.
   (b) Augmente la sécurité en rendant les attaques coûteuses en capital.
   (c) Dans les versions avancées, la création de blocs ne nécessite plus de résolution de problème mathématique, mais repose uniquement sur le **staking** (mise en jeu des jetons).

1.7.3 Tolérance Pratique aux Pannes Byzantines (PBFT - Practical Byzantine Fault Tolerance)

1. Algorithme basé sur un mécanisme de **vote** qui permet à un groupe de nœuds de s'accorder même en présence de **nœuds malveillants**.
2. Conçu pour fonctionner efficacement dans des **blockchains de consortium** (ex : Hyperledger Fabric).
3. **Caractéristiques** :
   (a) Permet de parvenir à un consensus même si une partie des nœuds se comporte de manière malveillante.
   (b) Utilise un système de **nœud principal** (leader) et de **nœuds de sauvegarde** (backup) qui valident les transactions en plusieurs étapes.
   (c) Élimine le besoin de calculs intensifs comme dans le PoW, mais nécessite une **confiance accrue entre les participants** et une protection contre les attaques Sybil.

1.8 Règle de la chaîne la plus longue (Longest Chain Rule)

1. Lorsqu'il existe plusieurs chaînes en raison de la propagation différée des blocs ou de la compétition entre mineurs, cette règle permet de résoudre les conflits.
2. **Caractéristiques** :

(a) Les nœuds considèrent comme valide la chaîne qui a le plus de blocs.
(b) Cette règle garantit qu'à long terme, une seule chaîne domine et prévaut sur les autres.
(c) Assure la cohérence et la continuité du registre distribué.

1.9 Le principe de fonctionnement de la Blockchain

Le processus de fonctionnement de la blockchain repose sur plusieurs étapes clés, garantissant la sécurité, l'intégrité et la transparence des transactions. Voici une explication détaillée de chaque étape du processus :

1.9.1 Création et émission d'une transaction

Une transaction est une action initiée par un utilisateur sur la blockchain. Elle peut être un transfert de cryptomonnaie, l'exécution d'un contrat intelligent ou toute autre opération enregistrée dans la blockchain.

Informations requises pour une transaction

1. **Expéditeur** : L'adresse publique de l'utilisateur qui envoie l'actif numérique.
2. **Destinataire** : L'adresse publique de l'utilisateur qui reçoit l'actif.
3. **Montant** : La quantité de cryptomonnaie ou d'actif transférée.
4. **Signature numérique** : L'expéditeur signe la transaction avec sa clé privée pour prouver son authenticité.
5. **Frais de transaction (facultatif)** : Dans certaines blockchains, des frais sont nécessaires pour inciter les mineurs à valider la transaction.

Une fois remplie, la transaction est signée numériquement et envoyée au réseau.

1.9.2 Diffusion de la transaction dans le réseau

La transaction est transmise à tous les nœuds du réseau (ordinateurs participant à la blockchain). Ce processus est appelé *broadcast* et fonctionne selon un protocole peer-to-peer (P2P).

1. Les nœuds valident la structure de la transaction avant de la relayer au reste du réseau.
2. Les mineurs ou validateurs reçoivent ces transactions et les stockent temporairement dans une **mempool** (pool de mémoire contenant les transactions en attente de validation).
3. **Propagation rapide et décentralisée** : Plus il y a de nœuds sur le réseau, plus la propagation est rapide.

1.9.3 Validation de la transaction

Avant d'être ajoutée à un bloc, chaque transaction doit être vérifiée par les nœuds du réseau pour éviter les fraudes, comme la double dépense.

Vérifications effectuées par les nœuds

1. **Authenticité de la signature** : Vérifiée cryptographiquement à l'aide de la clé publique de l'expéditeur.
2. **Disponibilité des fonds** : L'expéditeur doit avoir un solde suffisant pour exécuter la transaction.
3. **Non-altération des données** : Vérification que les informations de la transaction n'ont pas été modifiées.
4. **Respect des règles du protocole** : Vérification des frais de transaction et d'autres paramètres spécifiques à la blockchain utilisée.

Si la transaction est jugée valide, elle est stockée temporairement dans la mempool en attente d'intégration dans un bloc.

1.9.4 Ajout de la transaction dans un bloc

Les mineurs ou validateurs regroupent plusieurs transactions valides dans un bloc candidat.

Composition d'un bloc

1. **En-tête du bloc** : Contient le hachage du bloc précédent, un horodatage, le nonce et d'autres métadonnées.
2. **Liste des transactions** : L'ensemble des transactions validées.
3. **Racine de Merkle** : Structure permettant d'assurer l'intégrité des transactions contenues dans le bloc.

Le bloc est ensuite soumis à l'algorithme de consensus pour être validé.

1.9.5 Consensus et ajout du bloc à la chaîne

Le consensus est le mécanisme permettant aux nœuds du réseau de s'accorder sur l'ajout d'un bloc valide. Différents algorithmes sont utilisés selon la blockchain.

Principaux algorithmes de consensus

1. **Preuve de Travail (PoW - Proof of Work)**
   — Utilisé par Bitcoin.
   — Les mineurs doivent résoudre un puzzle cryptographique complexe.
   — Nécessite une forte puissance de calcul, mais assure la sécurité du réseau.
2. **Preuve d'Enjeu (PoS - Proof of Stake)**
   — Utilisé par Ethereum 2.0 et Cardano.
   — Les validateurs sont sélectionnés en fonction de la quantité de cryptomonnaie détenue.
   — Moins énergivore que le PoW et plus rapide.
3. **Preuve d'Autorité (PoA - Proof of Authority)**
   — Utilisé pour des blockchains privées.
   — Un ensemble restreint de nœuds de confiance valident les blocs.
4. **Preuve de Participation Déléguée (DPoS - Delegated Proof of Stake)**
   — Utilisé par EOS et TRON.
   — Les détenteurs de jetons votent pour élire des validateurs.

Une fois le consensus atteint, le bloc est ajouté à la blockchain.

1.9.6 Mise à jour du registre

Après validation, le bloc est diffusé à tous les nœuds du réseau pour mise à jour :

1. Les nœuds ajoutent le bloc validé à leur copie locale de la blockchain.
2. Les transactions incluses dans le bloc sont considérées comme confirmées et irréversibles.
3. La chaîne la plus longue est toujours considérée comme valide en cas de divergence entre plusieurs versions de la blockchain (principe de la *Longest Chain Rule* dans PoW).

Sécurisation et immuabilité

1. Chaque bloc contient le hachage du bloc précédent, formant une chaîne inaltérable.
2. Modifier une transaction nécessiterait de réécrire tous les blocs suivants, ce qui est quasiment impossible en raison du consensus décentralisé.

1.10 Applications de la Blockchain

La blockchain est une technologie révolutionnaire qui a transformé plusieurs secteurs grâce à ses caractéristiques de décentralisation, d'immutabilité et de transparence. Initialement utilisée pour les crypto-monnaies, son champ d'application s'est élargi à de nombreux autres domaines, notamment la finance, la santé, la gouvernance, l'Internet des objets (IoT) et les systèmes de contrôle de fichiers[1][3][4].

1.10.1 Secteur de la Santé

La blockchain est utilisée pour **sécuriser et partager les dossiers médicaux** entre les différents acteurs de la santé (médecins, hôpitaux, patients). Elle permet de garantir **l'intégrité et la confidentialité** des données tout en assurant un accès sécurisé et contrôlé aux professionnels de santé.

1.10.2 Secteur Financier et Cryptomonnaies

Les cryptomonnaies, comme **Bitcoin et Ethereum**, sont les premières applications de la blockchain. Elles permettent des transactions **sécurisées, transparentes et sans intermédiaire**. De plus, les **contrats intelligents** facilitent l'automatisation des accords financiers et réduisent les risques de fraude.

1.10.3 Collaboration Inter-Entreprises

La blockchain est utilisée pour **optimiser les processus métiers** et la **collaboration entre entreprises**. Grâce aux **contrats intelligents**, les accords commerciaux peuvent être exécutés de manière **automatique et sécurisée**, sans intermédiaire. Cette application est particulièrement bénéfique pour la gestion des **chaînes d'approvisionnement, la logistique et le commerce international**.

1.10.4 Internet des Objets (IoT)

L'intégration de la blockchain dans l'**IoT** permet de renforcer la **sécurité et la gestion des objets connectés**. Dans les architectures **multi-tiers**, la blockchain est utilisée pour **authentifier les dispositifs IoT, sécuriser les communications et améliorer la scalabilité des réseaux**. Un modèle basé sur les **nœuds gateway** a été proposé pour renforcer la fiabilité des interactions entre les objets connectés.

1.10.5 E-Gouvernance et Vote Électronique

Les gouvernements explorent l'usage de la blockchain pour **renforcer la transparence et la confiance dans les processus électoraux**. Elle peut être utilisée pour **l'authentification des votes**, réduisant ainsi les risques de fraude et garantissant un système électoral plus fiable.

1.10.6 Systèmes de Contrôle de Fichiers

Un système de fichiers blockchain avec traçabilité des modifications permet d'assurer une gestion transparente et sécurisée des fichiers tout en enregistrant chaque modification sur un registre immuable. Elle joue egalement un rôle clé dans la gestion sécurisée des fichiers et des données :

1. Authentification et traçabilité : garantit l'intégrité des documents en conservant un historique immuable des modifications.
2. Stockage décentralisé : remplace les serveurs centralisés traditionnels par un réseau distribué pour éviter les points uniques de défaillance.
3. Protection contre les manipulations : Assure la non-répudiation des documents et prévient toute modification non autorisée.

L'un des principaux exemples de gestion sécurisée des fichiers via la blockchain est le stockage des certificats et diplômes, permettant de prévenir la falsification des documents académiques.

1.11 La blockchain dans les systèmes de contrôle de fichiers

1.11.1 Introduction

Avec l'augmentation exponentielle des données numériques, la sécurité et l'intégrité des fichiers deviennent des enjeux cruciaux pour les entreprises et les particuliers. Bien que les systèmes de fichiers traditionnels soient robustes, ils présentent certaines limites en matière de protection contre la falsification, la perte de données et l'accès non autorisé.

Dans ce contexte, la blockchain, une technologie initialement développée pour les cryptomonnaies, apparaît comme une solution prometteuse pour combler ces lacunes. Grâce à son registre immuable, sa transparence et son approche décentralisée, elle offre un moyen efficace de sécuriser et de tracer les modifications apportées aux fichiers.

1.11.2 Le système de fichiers

Un système de fichiers est une structure qui permet d'organiser, de stocker et de gérer des fichiers sur un support de stockage. Il repose sur plusieurs éléments clés, notamment la hiérarchie des fichiers, les permissions d'accès et les mécanismes de lecture et d'écriture.

Parmi les systèmes de fichiers les plus courants, on retrouve NTFS, FAT32, ext4 et HFS+. Pour le transfert de fichiers, diverses techniques sont utilisées, telles que SFTP et SSH, qui assurent l'échange de données entre les nœuds d'un réseau. Cependant, bien que ces outils soient essentiels à l'efficacité du transfert, ils présentent certaines vulnérabilités susceptibles de compromettre l'intégrité des fichiers.

1.11.3 Les limites des systèmes de fichiers

Malgré leur omniprésence, les systèmes de fichiers traditionnels souffrent de plusieurs limitations :

Sécurité et intégrité des données : Les fichiers stockés peuvent être modifiés ou supprimés sans laisser de trace, ce qui pose des problèmes de traçabilité.

1. Accès non autorisé : Les permissions peuvent être contournées par des utilisateurs malveillants ou des attaques informatiques.
2. Centralisation des données : La plupart des systèmes de fichiers sont centralisés, rendant les données vulnérables aux pannes et aux attaques sur un serveur unique.
3. Faible transparence : Il est souvent difficile d'auditer les modifications apportées à un fichier.

1.11.4 La blockchain comme une solution de sécurité dans les systèmes de fichiers

Grâce la blockchain et à ses caractéristiques décentralisées et immuables, constitue une solution innovante pour renforcer la sécurité des systèmes de Fichiers. Voici comment la blockchain garantit la sécurité des fichiers :

Immutabilité des données

1. Chaque transaction (modification ou enregistrement d'un fichier) est stockée dans un bloc.
2. Une fois ajouté à la chaîne, un bloc ne peut plus être modifié ni supprimé, garantissant l'intégrité des enregistrements.
3. Toute tentative de modification nécessiterait la modification de tous les blocs suivants, ce qui est pratiquement impossible en raison du consensus décentralisé.

Hachage cryptographique

1. Chaque fichier est associé à une empreinte unique (hash) générée par un algorithme cryptographique (ex : SHA-256).
2. Si un fichier est modifié, son empreinte change complètement, rendant toute altération immédiatement détectable.
3. Le hash du fichier est stocké sur la blockchain, garantissant que le fichier original reste inchangé.

Consensus distribué

1. Toutes les modifications des fichiers doivent être validées par un réseau de nœuds via un mécanisme de consensus (Proof of Work, Proof of Stake, etc.).
2. Cela empêche une entité unique de modifier les données de manière frauduleuse.

Historique et traçabilité des modifications

1. Chaque action (ajout, modification, suppression) est enregistrée sous forme de transactions sur la blockchain.
2. Un historique complet des modifications est conservé, permettant d'identifier qui a modifié quoi et quand.

Authentification et contrôle d'accès

1. L'accès aux fichiers est sécurisé par des signatures numériques et des clés cryptographiques.
2. Seuls les utilisateurs autorisés peuvent apporter des modifications validées sur la blockchain.

Réplication décentralisée

1. Les données sont stockées sur plusieurs nœuds du réseau, empêchant toute corruption ou perte en raison d'une panne unique.
2. Toute tentative de modification malveillante sur un nœud est immédiatement détectée par les autres.

Bibliographie

[1] Yasmine Bachi. *Sélection des nœuds gateway dans une architecture Blockchain multi-tiers pour l'IoT*. 2021.

[2] Ying-Chang Liang. *Blockchain for Dynamic Spectrum Management*. 2020.

[3] Aktouche Sadek Rayan and Righi Sylia. *Intégration de la technologie Blockchain dans les systèmes de collaboration inter-entreprises*. 2021.

[4] Habibeche Sakina and Fartas Hesna. *Conception et réalisation d'un système sécurisé de gestion des Dossiers Médicaux Utilisant la blockchain*. 2024.