République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université SAAD DAHLEB-BLIDA1
Faculté des Sciences
Département d'informatique

Mémoire de Fin d'Etude En vue de l'obtention du diplôme de

Master en Informatique

Option : Système Informatique et Réseau (SIR)

Thème

Une Solution de confidentialité compatible avec la blockchain dans les villes intelligentes

Réalisé par : Bouhouia Wiem
Boussadia Fatma Zohra

Les jurys :

Mme.Abed	USDB1	Présidente
Mme.Cherfa Imane	USDB1	Examinatrice
Mme.Midoun Khadidja	USDB1	Promotrice
M. Mouzaoui Abdeldjallil	CERIST	Encadreur

2022/2023

Remerciements

Tout d’abord nous tenons à remercier Allah pour nous avoir donné le courage, la force et la volonté pour réussir et de nous avoir éclaircir le chemin tout au long de notre vie.

Nos remerciements et nos profondes gratitudes vont à notre promotrice Madame **Midoun Khadidja** et notre encadreur Monsieur **Mouzaoui Abdeldjalli** pour leurs encadrements, leurs suivies et leurs conseils tout au long de cette période.

Nous tenons aussi à remercier les membres du jury pour leur précieux temps accordé à l’étude de notre mémoire.

Nos remerciements et notre gratitude vont aux professeurs et enseignants de département d'informatique ainsi que ses étudiants et son personnel côtoyés tout au long de notre cursus universitaire.

Que toute personne ayant œuvré de près ou de loin à la réalisation de ce projet basé sur la Blockchain par une quelconque forme de contribution, trouve ici le témoignage de notre plus profonde reconnaissance.

Dédicace

Nous dédions ce mémoire : À nos très chers parents pour leurs soutiens durant toute notre vie d'étudiants et sans eux nous ne serions jamais

Devenues ce que nous sommes.

A nos frères et sœurs

À toutes nos familles.

À tous nos amis sans aucune exception.

Bouhouia Wiem & Boussadia Fatma Zohra

Résumé

Les villes intelligentes génèrent d'énormes quantités de données sensibles, nécessitant des mécanismes de confidentialité solides pour le partage de données et les interactions. Afin de résoudre ce problème de confidentialité, ce projet vise à développer une Solution de confidentialité compatible avec la Blockchain dans les villes intelligentes. La solution proposée exploite la nature décentralisée et immuable de la technologie Blockchain, ainsi que des techniques renforçant la confidentialité, afin d'assurer des transactions de données sécurisées et privées au sein de l'écosystème de la ville intelligente. Il implique la conception et la mise en œuvre d'un mécanisme de partage de données préservant la confidentialité à l'aide de la Blockchain. Ce mécanisme garantit que les données sensibles partagées entre différentes entités au sein de la ville intelligente restent confidentielles et sécurisées. Des techniques cryptographiques sont utilisées pour chiffrer et stocker les données de manière décentralisée sur la Blockchain, permettant aux parties autorisées d'accéder et de valider les données tout en préservant la confidentialité.

الملخص

يهدف هذا المشرع الى تطوير حل يدعم تقنية بلوكشين والخصوصية للمدن الذكية للتعامل مع قضايا الخصوصية في مشاركة البيانات والتفاعلات. تعمل المدن الذكية، التي تعتمد على انترنت الأشياء والتقنيات المستندة الى البيانات، على انتاج كمية ضخمة من البيانات الحساسة، مما يستدعي ضرورة وجود اليات قوية للخصوصية، يتمثل في الحل المقترح وهو الطبيعة اللامركزية والثابتة لتقنية بلوكشين، بالإضافة الى تقنيات تعزز الخصوصية، لضمان تنفيذ صفقات بيانات امنة وخاصة داخل نظام المدن الذكية. يتضمن تصميم وتنفيذ آلية مشاركة بيانات تحافظ على الخصوصية باستخدام بلوكشين .تضمن هذه الآلية أن تظل البيانات الحساسة المشتركة بين الكيانات المختلفة داخل المدينة الذكية سرية وآمنة. تُستخدم تقنيات التشفير لتشفير البيانات وتخزينها بطريقة لامركزية على بلوكشين.

Abstract

This project focuses on developing a Blockchain-privacy enabled solution for smart cities to address privacy concerns in data sharing and interactions. Smart cities, powered by the Internet of Things (IoT) and data-driven technologies, generate vast amounts of sensitive data which require robust privacy mechanisms. The proposed solution based on the decentralized and immutable nature of Blockchain technology, along with privacy-enhancing techniques, to ensure secure and private data transactions within the smart city ecosystem. It involves designing and implementing a privacy-preserving data sharing mechanism using Blockchain. This mechanism ensures that sensitive data shared between different entities within the smart city remains confidential and secure. Cryptographic techniques are employed to encrypt and store the data in a decentralized manner on the Blockchain, allowing authorized parties to access and validate the data while preserving privacy.

Table des matières

Table des figures

Liste des tableaux

La liste des abréviations

- **IDO :** Internet des objets
- **ACL:** Access Control List
- **SC:** Smart City
- **CID :** content identifier
- **TIC :** Technologie de l'information et de la communication
- **SVM :** Support Vector Machine
- **ACP :** Analyse en Composantes Principales
- **CSP:** Content Security Policy
- **HCAI:** Human-Centered Artificial Intelligence
- **ML:** Machine Learning
- **PPSF:** Privacy-Preserving Smart Framework
- **OBPP:** On-Chain Blockchain Privacy-Preserving
- **PDFPSTC Smart City IE:** Privacy-aware Data Fusion and Prediction with Spatial-Temporal Context for Smart City Industrial Environment

Introduction Générale

Depuis quelques années, on assiste à une révolution numérique dans de nombreux domaines, la digitalisation de l'industrie, la digitalisation des administrations publiques, la digitalisation des personnes et des objets (Internet des Objets - IoT), et la digitalisation des villes dites villes intelligentes. La ville intelligente est un terme collectif pour les technologies et les concepts qui visent à rendre les villes efficaces, technologiquement plus avancées, plus vertes et plus inclusives socialement. La construction d'une ville intelligente nécessite une plus grande connectivité réseau pour promouvoir de nouvelles fonctionnalités avancées qui augmentent les préoccupations en matière de sécurité et de confidentialité afin d'économiser le temps et les ressources précieux. La grande quantité de données critiques stratégiques doit être protégée contre le vol de données. Le vol de données expose la confidentialité de l'organisation à des défis importants à mesure que le nombre de violations augmente, ce qui entraîne une augmentation des coûts liés à ce problème. Pour garantir la confidentialité des informations sensibles pour chaque fournisseur de données, la technologie Blockchain peut être envisagée pour construire une politique de partage de données fiable et sécurisée entre de nombreux fournisseurs de données, où les informations IoT sont encodées puis vérifiées sur des registres diffusés. Cependant la nature publique de la Blockchain pose un grand problème de préservation de la vie privée des utilisateurs et de confidentialité des données. En effet, de nombreux travaux de recherches ont pu mettre en avant les principale lacunes et faiblesses de cette technologie. Notre travail est d'étudier la problématique ainsi que les différentes solutions proposées et éventuellement proposer une méthode pour améliorer la protection de la vie privée dans la Blockchain.

Nous avons divisé notre mémoire en quatre chapitres. Dans le premier chapitre nous donnons un aperçu sur la ville intelligente et leur forces et limites. Nous avons donne aussi une présentation générale du Blockchain et énumérer les concepts de base technologiques de cette dernière. Puis nous avons introduit le concept de la vie privée dans la Blockchain, ensuite nous avons réalisé l'étude de différents travaux visant à améliorer la préservation de la vie privée avec la technologie Blockchain.

Dans le deuxième chapitre, nous présentons notre conception qui est un modèle qui stocke et partage les données dans un réseau Blockchain intégrer avec IPFS d'une manière sécuriser en préservons la vie privée et la confidentialité des données.

Dans le troisième chapitre, nous présentons l'implémentation et les outils utilisés dans notre approche avec les résultats obtenue.

Chapitre 1 : La technologie blockchain dans les villes Intelligentes

1. Introduction

Dans ce chapitre, nous allons essayer d'aborder les grandes lignes de la ville intelligente et la technologie Blockchain. Nous avons commencé par définir la ville intelligente et ses caractéristiques et les dimensions de la ville, puis nous avons défini la Blockchain et énumérer les prés requis technologiques de cette dernière et expliquer le principe de son fonctionnement, nous avons expliqué une vue générale sur la protection de la vie privée dans la Blockchain.

2. La ville intelligente

2.1.Définition

Le terme la ville intelligente [1] « **Smart City en Anglais** » désigne une ville moderne avancée qui utilise les TIC et d'autres technologies dès les années 1990, pour améliorer la qualité de vie, la compétitivité, l'efficacité opérationnelle des services urbains, tout en assurant la disponibilité des ressources pour les générations actuelles et futures en termes de facteurs sociaux, économiques et environnementaux [2].

Le concept de ville intelligente intègre les technologies de l'information et de la communication (TIC) ainsi que divers dispositifs physiques connectés au réseau, formant ainsi l'Internet des objets (IoT). Cette approche vise à optimiser l'efficacité des opérations et des services urbains tout en favorisant la connectivité entre les citoyens et leur environnement [3].

2.2. Caractéristique de la ville

Une ville intelligente se caractérise par plusieurs caractéristiques clés qui tirent parti de la technologie et des données. Les principales caractéristiques d'une ville intelligente sont la durabilité, la qualité de vie, l'intelligence et l'urbanisation (voir la figure 1).

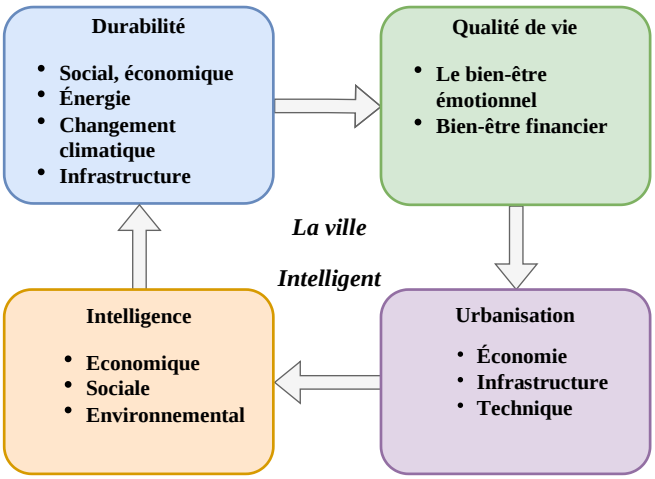


Figure 1: Caractéristiques d'une ville intelligente [4]

2.3. Les avantages de la ville intelligente

- Une ville efficace, rationalisée et leader : La ville serait plus efficace car elle serait rationalisée à travers le flux de données, ce qui la rendrait plus facile à contrôler, plus gérable et, surtout, plus réactive. En outre, les progrès technologiques permettent un fonctionnement plus efficace et efficace des administrations locales [6].
- Une ville plus stimulante : où il fait bon vivre L'objectif de la ville intelligente est, d'améliorer la viabilité, la gouvernance, le développement de la politique urbaine, etc. En outre, il est envisagé que la nouvelle technologie de l'information créera des citoyens plus intelligents qui adopteront finalement des comportements plus intelligents [6].
- Une ville durable : Grâce aux données, la ville intelligente permettra aux résidents d'adopter des comportements plus respectueux de l'environnement et aidera les sociétés urbaines à passer à un avenir économe en énergie [6].

2.4.Les limites de la ville intelligente

Les villes intelligentes offrent des transports intelligents, l'industrie, la santé intelligente, les maisons intelligentes et les services financiers intelligents. Ces applications doivent traiter les données avec une sécurité extrême afin d'améliorer la qualité de vie des citoyens. Nous pouvons utiliser la Blockchain pour activer des villes intelligentes avec une sécurité et une confidentialité renforcées [6].

3. Blockchain

Blockchain est un registre distribué basé sur un réseau pair à pair décentralisé construit sur une structure de données connue sous le nom de chaîne de blocs qui permet le stockage et l'échange d'informations. Les transactions d'un bloc sont organisées en arbres de Merkle, ces derniers utilisant le hachage cryptographique pour stocker les transactions de manière sûre et efficace. Le bloc inclut les transactions ainsi que l'héritage numérique du bloc précédent. Les blocs rassemblent et vérifient les heures et les séquences des transactions, qui sont ensuite enregistrées dans la Blockchain et affectées à un réseau unique soumis à des règles convenues par ses participants**.** Chaque bloc contient un hash. Le hash du bloc précédent relie les blocs et évite qu'un bloc ne soit modifié ou inséré entre deux blocs existants. Ainsi, chaque bloc consécutif renforce la vérification du précédent, et, par conséquent, l'ensemble de la Blockchain. Les blocs sont vérifiés selon des mécanismes de consensus.

3.1.Les concepts de base de Blockchain

3.1.1. Architecture paire à pair P2P

C'est une architecture d'application distribuée qui divise les tâches en différentes paires, chacune ayant le même privilège. Le réseau se trouve pratiquement au- dessus du réseau physique et les liens entre les paires sont considérés comme des liens logiques. Le nœud du réseau P2P exécute volontairement Ensemble, Chaque nœud du réseau P2P exécute délibérément un logiciel pour fonctionner à la fois en tant que serveur et client tout en conservant les mêmes responsabilités et le même statut au sein du réseau [7].

3.1.2. Cryptographie asymétrique

La Blockchain utilise le principe de la cryptographie pour garantir l'intégrité, la confidentialité et l'authenticité des données.

3.1.3. Définition

La cryptographie asymétrique, également appelée cryptographie a clé publique, qui utilise des publique et privées pour chiffrer et déchiffrer des données. Ces clés sont simplement de grands nombres qui sont associes par paires, mais ils ne sont pas identiques. La clé publique peut être partagée avec tout le monde par contre la clé privée est tenue secrète. L'une ou l'autre de ces clés peut servir à chiffrer un message, donc la clé opposée a celle ayant servi au chiffrement qui est utilisée pour le déchiffrement [16].

3.1.4. Fonction de hachage

La fonction de hachage cryptographique génère une chaine de caractères de longueur fixe à partir d'un ensemble de données de n'importe quel volume. Le hachage d'un bloc est unique à ce bloc et il change si l'une de ses données sous-jacentes change. Le hachage transforme une sotie de données aléatoire (clés) en une chaine d'octets de longueur et structure fixes (valeur de hachage). Le hachage d'une transaction facilite l'identification de cette dernière sur la Blockchain. Une fonction de hachage favorable utilise un algorithme de hachage unidirectionnel. Blockchain utilise des algorithmes cryptographiques pour calculer le hachage. L'entrée de ces algorithmes cryptographiques est les données du bloc et sa valeur de hachage précédente [7].

3.1.5. Arbre Merkle

Utilisé pour obtenir des informations sur le bloc et pour recevoir une clé de hachage pour la racine de Merkle. L'arbre binaire est la définition d'un arbre de Merkle. Le nœud racine de l'arbre de Merkle contient toutes les paires hachées de l'arbre [4]. Pour vous aider à visualiser ce processus, regardez l'exemple d'une liste binaire d'un arbre haché illustré dans la figure 3.

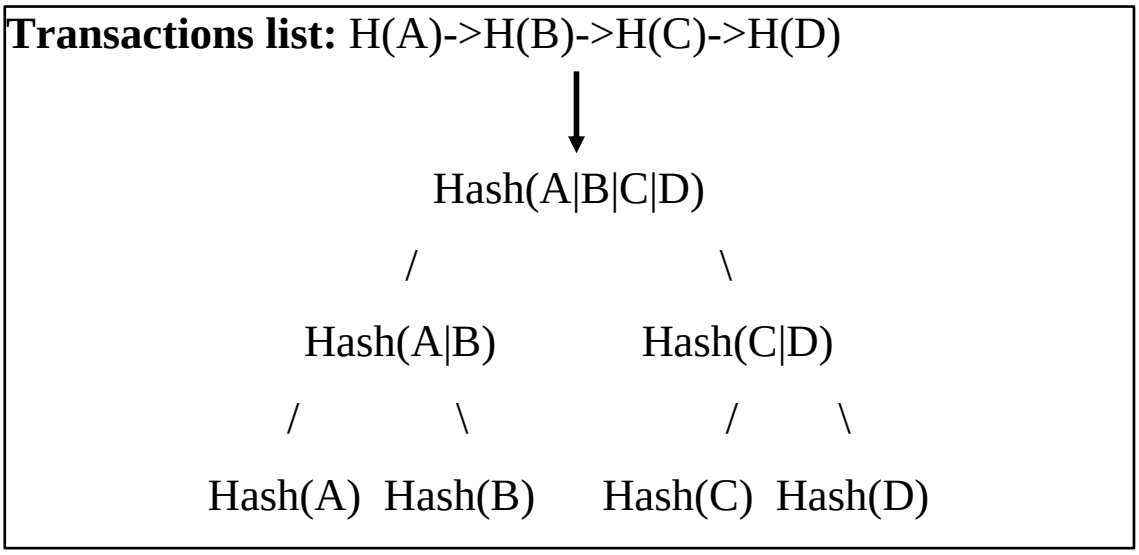


Figure 2 : Un exemple sur l'arbre de Merkle [4]

Les blocs descendants inclus dans ce Merkle sont une représentation de toutes les transactions de ce bloc à travers les en-têtes de bloc. La racine de Merkle est HASH(A|B|C|D). Toutes les opérations de ce bloc seraient hachées par chacun des éléments A, B, C et D. Dans notre exemple, nous n'avons qu'une seule transaction dans chaque bloc.

3.1.6. Le Block

C'est une structure de données sert à stocker toutes les transactions, distribuées à tous les nœuds présents dans le réseau Blockchain. Structure d'un bloc dans une Blockchain est généralement composée des éléments suivants :

1. En-tête du bloc : L'en-tête du bloc contient des informations essentielles sur le bloc lui-même. Ces informations comprennent généralement :

- **Version :** Le numéro de version du protocole utilisé.
- **Horodatage :** L'heure à laquelle le bloc a été créé.

- **Numéro de bloc :** Un identifiant unique qui indique la position du bloc dans la séquence de la chaîne de blocs.
- **Données de merkle root :** Une empreinte numérique (hash) des transactions contenues dans le bloc.

Hash de l'en-tête précédent : Le hash de l'en-tête du bloc précédent dans la chaîne, ce qui relie les blocs entre eux.

2. Liste des transactions : Cette partie du bloc contient les détails des transactions incluses dans le bloc. Chaque transaction peut inclure des informations telles que les adresses des expéditeurs et des destinataires, les montants transférés, les données supplémentaires, etc.

3. Nonce : Le nonce est un nombre aléatoire utilisé lors du processus de minage pour trouver une valeur de hachage satisfaisant certaines conditions définies par le protocole de consensus de la Blockchain. Il est utilisé pour prouver que du travail a été effectué pour créer le bloc.

4. Hash : Le hash est une valeur unique qui représente l'ensemble des données contenues dans le bloc. Il est calculé en utilisant une fonction de hachage cryptographique, généralement SHA-256 (Secure Hash Algorithme 256 bits) pour les Blockchains comme Bitcoin. Le hash sert à identifier de manière unique le bloc et est utilisé pour lier les blocs entre eux dans une séquence chronologique.

3.1.7. Transaction

Une transaction dans une Blockchain est un échange de données qui est enregistré de manière permanente et immuable sur la Blockchain. L'état actuel de Blockchain est représenté par ces transactions, qui sont générées en permanence par les nœuds, puis rassemblées en blocs. Tous les nœuds sont conscients du solde actuel à chaque adresse et conservent une copie de la Blockchain existante, qui est le journal contenant l'historique des transactions précédentes. L'état de la Blockchain change après chaque transaction. Avec un nombre considérable de transactions générées chaque seconde, il est très important de valider et de vérifier les transactions authentiques et d’éliminer le faux [17].

3.1.8. Mécanisme de consensus

3.1.8.1. Définition

Un consensus distribué signifie qu'un pool de pairs, géographiquement éloignés, s'accorde de manière décentralisée, au lieu d'un ordinateur maître (centralisé). Au lieu de réglementations, il existe des règles qui sont généralement définies dans un environnement open source au lieu d'être définies par une entité gouvernementale [7].

Dans les crypto-monnaies, le consensus/accord est de savoir si les blocs sont valides ou non. Si un bloc est valide, le bloc sera ajouté à la Blockchain. Si un bloc est invalide, il sera refusé d'être ajouté à la Blockchain. C'est là qu'une politique de consensus entre en jeu. La plupart des pairs dans le réseau détiennent les mêmes blocs dans leur meilleure Blockchain validée et suivent les mêmes règles. Il existe plusieurs types d'algorithmes de consensus, les algorithmes la preuve de travail et la preuve d'enjeu sont les plus connue [7].

3.1.8.2. La preuve de travail (POW)

La preuve de travail (proof of work) consiste à trouver le hachage du bloc tel qu'il soit inférieur au seuil fixé par la difficulté de minage actuelle du réseau Blockchain. Les mineurs modifient le nonce de l'en-tête du bloc pour trouver un tel hachage. Une fois qu'un tel hachage est trouvé par l'un des mineurs concurrents, les autres nœuds du réseau Blockchain vérifie son exactitude suivie de la validation des transactions dans le bloc nouvellement créé. Le principal inconvénient du Pow est l'exigence d'un équipement spécialisé coûteux avec un taux de hachage plus élevé. Pow exige non seulement une puissance de calcul, mais aussi implique une forte consommation d'électricité qui a des implications environnementales associées [7].

3.1.8.3. La preuve d'enjeu (POS)

La preuve d'enjeu (proof of stake) est un protocole informatique utilisé pour atteindre un consensus sur un réseau Blockchain basé sur la preuve de participation, il utilise la détention de jetons ou de crypto monnaies pour sécuriser le réseau. Les participants du réseau Blockchain détiennent des jetons ou des crypto monnaies spécifiques. Les détenteurs de jetons peuvent alors verrouiller une certaine quantité de jetons pour participer au processus de validation des transactions. Les nœuds qui ont verrouillé des jetons sont choisis aléatoirement pour valider ces transactions, les validateurs sélectionnés vérifient la validité des transactions et créent un

nouveau bloc de transactions. Les validateurs doivent alors s'accorder sur le contenu du bloc avant de le valider. Pour cela, ils peuvent utiliser différents mécanismes de consensus, tels que la preuve de possession ou la preuve de validité. Une fois que le bloc est validé, il est ajouté à la chaine de bloc, ce qui crée un consensus sur l'état du réseau [7].

3.1.8.4. Noeud

Dans une Blockchain, il existe différents types de nœuds qui participent au réseau et contribuent au fonctionnement de la Blockchain. Voici quelques-uns des types de nœuds courants :

1. **Nœud complet :** Un nœud complet est un type de nœud qui maintient une copie complète de la Blockchain. Il enregistre toutes les transactions, valide les nouvelles transactions et les blocs, et les propage à d'autres nœuds du réseau. Les nœuds complets jouent un rôle essentiel dans la sécurité et la décentralisation de la Blockchain, car ils vérifient toutes les règles du protocole et s'assurent que les transactions sont valides.

2. Nœud de minage : Un nœud de minage est un type de nœud qui participe au processus de minage dans les Blockchains basées sur la preuve de travail (Proof-of-Work). Les nœuds de minage effectuent des calculs intensifs pour résoudre des problèmes cryptographiques et ajouter de nouveaux blocs à la chaîne. Ils rivalisent pour trouver le nonce valide qui satisfait les conditions requises pour créer un bloc. Les mineurs sont récompensés par des crypto-monnaies pour leur travail de minage.

3. Nœud relais : Un nœud relais est un type de nœud qui facilite la propagation des transactions et des blocs à travers le réseau. Ils reçoivent les données provenant d'autres nœuds et les transmettent aux autres nœuds du réseau. Les nœuds relais jouent un rôle important dans la distribution efficace des informations et aident à maintenir la synchronisation de la Blockchain.

4. Nœud de porte d'entrée : Un nœud de porte d'entrée est un type de nœud qui agit comme une interface entre une Blockchain et d'autres réseaux externes. Ces nœuds permettent la communication entre la Blockchain et d'autres systèmes, tels que des réseaux privés, des services d'échange ou des applications tierces.

5. Nœud de validation : Un nœud de validation est un type de nœud qui participe au processus de validation des transactions dans les Blockchains basées sur la preuve d'enjeu (Proof-of-Stake). Ces nœuds sont sélectionnés en fonction de la quantité de crypto-monnaie qu'ils détiennent et engagent comme enjeu. Les nœuds de validation sont chargés de valider les transactions et de maintenir la sécurité de la Blockchain.

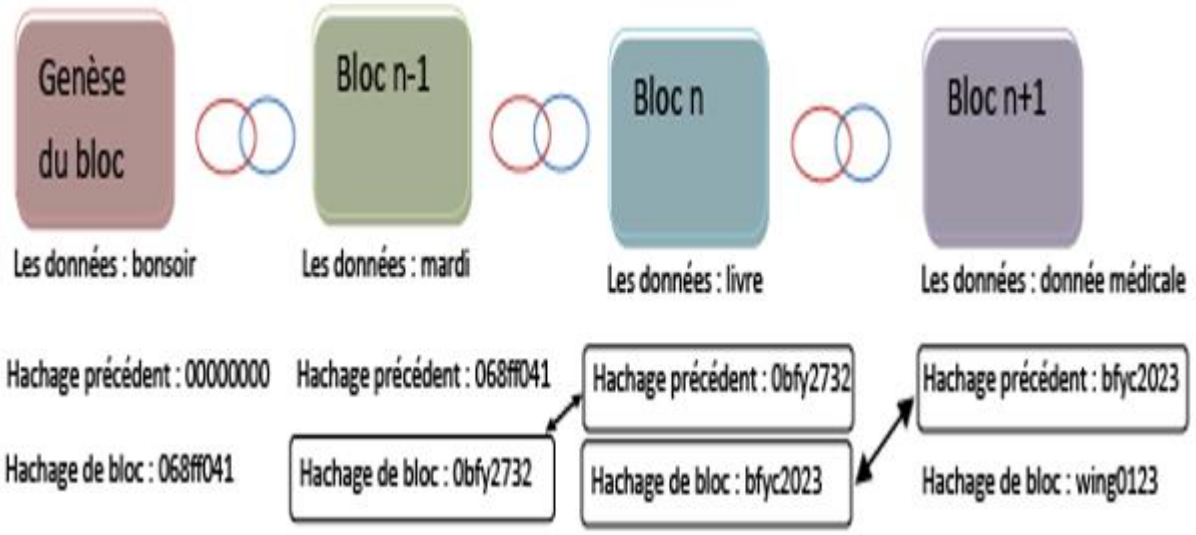


Figure 3 : Bloc cryptés avec opérations de hachage [22]

3.2. Fonctionnement de la Blockchain

Les utilisateurs possèdent des jetons, servant de monnaie au sein de la Blockchain, qu'ils peuvent s'échanger. Toutes les transactions sont regroupées dans des blocs, ensuite ajouter en plus dans chaque nouveau bloc l'empreinte cryptographique du bloc précédent. Pour éviter les intermédiaires chaque machine participant au réseau stocke sa propre chaîne, sur sa propre mémoire. Dans un réseau Blockchain, les transactions sont regroupées en blocs, et chaque bloc doit être vérifié avant de pouvoir être ajoute à la blockchain.les mineurs s'affrontent pour être les premiers a résoudre un casse-tête mathématique complexe qui leur permet d'ajouter le bloc suivant a la chaine. Ce processus s'appelle l'exploitation minière. Pour exploiter un bloc, un mineur doit d'abord vérifier toutes les transactions du bloc pour s'assurer

qu'elles sont valides. Ensuite, le mineur résoudre un casse-tête mathématique complexe qui nécessite une puissance de calcul importante. Le premier mineur à résoudre le puzzle et à ajouter le bloc à la chaine est récompense par une certaine quantité de crypto-monnaie. Une fois que le bloc est validé, il est ajouté à la chaine de blocs et devient donc visible de tous les utilisateurs. Voici un schéma qui vous permettra d'illustrer cette définition [18].

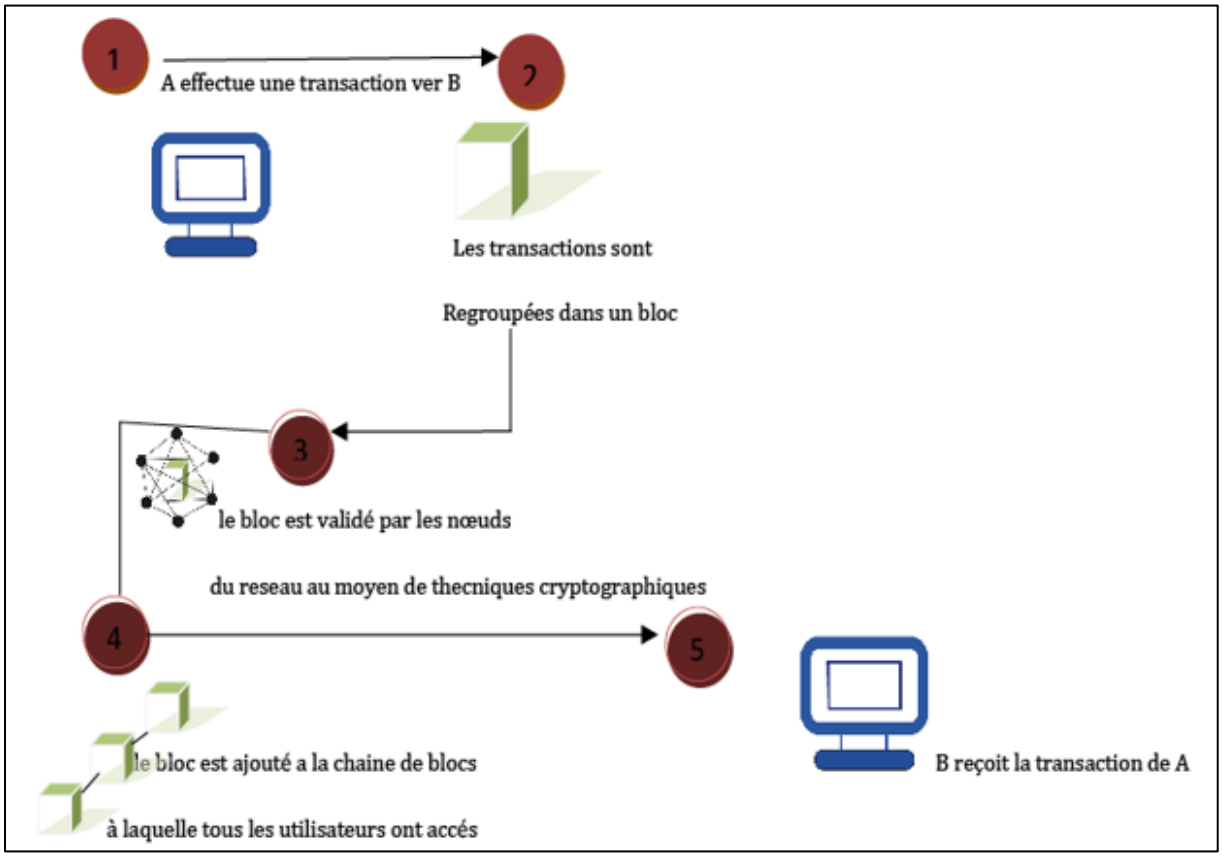


Figure 4 : Fonctionnement d'une Blockchain [18]

3.3. Signature numérique

La signature numérique est un schéma mathématique pour valider qu'une donnée numérique particulière est authentique. Signalisation numérique ture apporte au destinataire la preuve irréfutable qu'un message falsifié a été conçu par l'expéditeur correspondant. Le premier schéma de signature numérique a été introduit par Hellman et Diffie en 1976. En cryptographie symétrique, une clé secrète est partagée entre les parties communicantes pour le chiffrement et le déchiffrement. Cependant, Hellman a apporté la révolution de la cryptographie en introduisant l'asymétrie cryptographie qui est utilisée dans la technologie Blockchain. Chaque membre se voit attribuer une paire de clés cryptographiques dans le réseau Blockchain. La signature numérique a deux phases : la phase de signature et la phase de vérification [7].

3.3.1. La clé privée

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

3.3.2. La clé publique

Une fois qu'une transaction est reçue pour tous les nœuds, ces derniers possédant la clé publique, ils vont devoir procéder à l'authentification de l'auteur de la transaction.

3.4. Horodatage

L'horodatage est le moyen de garder une trace de la création ou l'heure de modification d'un document numérique. À travers l'horodatage, les parties concernées peuvent valider que le document particulier existait à une date et une heure donnée. Tout tierce partie peut vérifier la validité de l'horodatage qui est utilisé comme attribut dans chaque en-tête de bloc pour indiquer l'heure de création du bloc et de certifier que les transactions [7].

3.5. Les caractéristiques de Blockchain

Les caractéristiques principales de la technologie Blockchain sont :

1 **La désintermédiation**

La validation et l'ajout d'un bloc résultent d'un consensus entre les utilisateurs-validateurs, qui repose sur la possibilité de vérifier leur travail de validation et qui rend inutile le contrôle par une institution de référence. Tout est effectués sans l'intervention d'une autorité centrale, les utilisateurs opèrent la surveillance, et se contrôlent mutuellement, assurant la certification des sauvegardes et leur cohérence. La Blockchain est ainsi décentralisée, personne ne la contrôle et pas d'infrastructure centrale.

2 **La transparence**

Une fois qu'un document est inscrit sur la Blockchain, cela suffit à prouver que ce dernier existe bien à l'instant T et qu'il n'a pas été modifié.

3 **La sécurité**

Les données sont copiées dans les différents serveurs. Cela la rend résistante aux cyber-attaques ou au contrôle de l'État. En effet, s'il est possible de s'attaquer à un ou plusieurs ordinateurs, il est plus compliqué de s'attaquer aux blocs d'informations copiés dans l'ensemble des ordinateurs connectés au réseau.

4 **L'autonomie**

La puissance de calcul et l'espace d'hébergement sont fournis par les nœuds du réseau, c'est-à-dire les utilisateurs eux-mêmes. Il n'y a donc pas besoin d'infrastructures centrales.

3.6. Les types de la Blockchain

3.6.1 Blockchain publique

Une Blockchain publique est accessibles à tout le monde, tout utilisateur peut rejoindre le réseau sans condition et sans besoin d'une autorité centrale.

Les Blockchains principales sont des Blockchains publiques, comme Bitcoin, Ethereum, Monero, Litecoin, Dash [8].

3.6.2 Blockchain privée

Dans les Blockchain privée, les autorisations d'écriture sont strictement limitées, seuls les nœuds autorisés peuvent rejoindre une Blockchain privée pour lire, créer ou valider des transactions et des blocs, même si ses autorisations de lecture sont ouvertes au public ou limitées à un sous-ensemble de participants du réseau. Les Blockchains privées sont moins décentralisées que les Blockchains publique, mais l'information circule plus rapidement [8].

3.6.3 Blockchain consortium

Une Blockchain de consortium a des caractéristiques mixtes d'implémentations de Blockchain privées et publiques, sont généralement utilisées dans les cas où les membres du réseau veulent avoir un regard sur qui peut les rejoindre, mais sans utiliser un tiers de confiance où une autorité centrale [8]

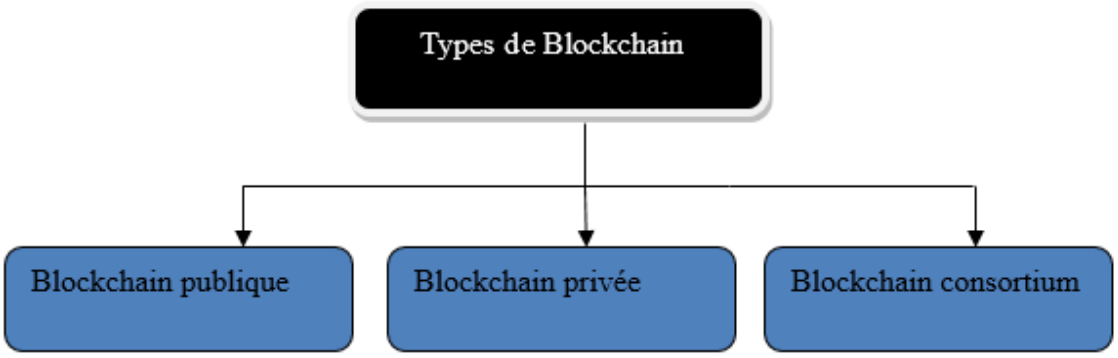


Figure 5 : Les types de la Blockchain [8]

3.7. Applications Blockchain

Le plus grand cas d'utilisation de la technologie Blockchain à ce jour est celui des crypto-monnaies. Cependant, la Blockchain ne s'arrête pas là - les banques et les institutions financières trouvent la Blockchain utile car elle les aide à traiter les transactions plus rapidement et à moindre coût [17].

3.7.1 Blockchain Crypto-monnaies

La crypto-monnaie est un actif numérique et de l'argent sécurisé par cryptographie et qui permet aux utilisateurs du réseau Blockchain de posséder, stocker, échanger et échanger de la valeur en toute sécurité. Contrairement aux dollars imprimés par le gouvernement, les euros et le yuan, le Bitcoin, Ethereum et plus de 5000 autres jetons cryptographiques et devises ne peuvent pas être contrôlés par une autorité centrale [9].

3.7.1.1 Bitcoin

Bitcoin est une monnaie numérique décentralisée qualifie de crypto-monnaie car il utilise des techniques cryptographiques pour sécuriser les transactions et contrôler la création de nouvelles unités .Ces transactions Bitcoin sont effectuées directement entres les utilisateurs sans avoir besoin d'intermédiaires comme les banques. Bitcoin est la première implémentation open source de la Blockchain été créée en 2009 [10].

3.7.1.2 Ethereum

Ethereum est une plateforme Blockchain décentralisée et open source qui permet la création et l'exécution des contrats intelligents [10].

3.7.1.3 Contrat intelligent

Est un contrat auto-exécutable dans lequel les termes de l'accord entre l'acheteur et le vendeur sont directement écrits dans des lignes de code sur la Blockchain Ethereum. Les contrats intelligents permettent l'automatisation d'accords financiers et juridiques complexes et peuvent être utilisés à des fins très diverses, allant des simples transferts de jetons à des instruments financiers plus complexes comme les options et les contrats à terme [9].

3.8. Technologies complémentaires à la Blockchain

La Blockchain est une technologie prometteuse qui offre de nombreux avantages en termes de sécurité, de transparence et de décentralisation.

Cependant, il existe également d'autres technologies qui peuvent compléter et améliorer l'utilisation de la Blockchain dans différents domaines. Voici un exemple de ces technologies :

IPFS : (système de fichiers interplanétaire) est un protocole de partage de fichiers décentralisé qui vise à créer un système de stockage et de distribution de contenu plus résilient et plus efficace que les solutions traditionnelles basées sur les serveurs et utilise un système de hachage pour identifier de manière unique chaque fichier et permet de les stocker de manière décentralisée sur un réseau pair- à -pair. Lorsqu'un fichier est ajouté à IPFS, il est divisé en petits morceaux appelés "chunks", qui sont distribués sur le réseau et peuvent être récupérés à partir de n'importe quel nœud qui les détient donc il facilite la mise en cache des fichiers et la réduction de la duplication, ce qui peut améliorer les performances et l'efficacité du partage de contenu sur Internet [19].

3.9. Sécurité de la technologie Blockchain

L'architecture de la Blockchain derrière les crypto-monnaies modernes, et les applications décentralisées possède d'importantes fonctionnalités de sécurité intégrées. Une fois les blocs de données ajoutés à la base de données Blockchain, ils sont immuables. Un pirate ne peut pas les modifier pour détourner des fonds. Les blocs sont vérifiés selon des mécanismes de consensus qui éliminent les transactions frauduleuses et protègent contre le piratage. L'accès à la base de données est protégé par un cryptage à clé publique de qualité financière. Ces fonctionnalités font de l'architecture Blockchain une place parmi les bases de données les plus sécurisées jamais créées [20].

3.10. Vie privée et la Blockchain

La protection de la vie privée a été étudié dans les Blockchains, en tant que type de base de données distribuée, la technologie Blockchain a des avantages significatifs en matière de protection de la vie privée. Voici quelque unes des approches utilisées pour protéger la vie privée des données.

Cryptographie : utilisée pour chiffrer les données avant d'être ajouté à la Blockchain, seules les personnes disposant de la clé de déchiffrement appropriée peuvent accéder aux données.

Hachage : les données sont transformées en une empreinte numérique unique à l'aide d'une fonction de hachage, cela permet de vérifier si les données ont été modifiées sans révéler les données elle-même.

Blockchain privée : utilisée pour limiter la visibilité des informations uniquement aux participants autorises, cela permet de protéger la vie prive des données. Il existe d'autres approches qui visent à améliorer la confidentialité des données dans la Blockchain. Par exemple, partage sélectif de données, solutions de confidentialité tierces [10].

3.11. Menaces sur la vie privée

Les menaces sur la vie privée des données dans la Blockchain peuvent inclure :

- **Révélation d'informations sensibles :** certaines informations peuvent être sensibles et révéler des détails personnels ou confidentiels, par exemples si des

données médicales sont enregistrées sur la Blockchain, leur divulgation peut compromettre la vie privée des individus concernés.

- **Données d'identification personnelles :** si les noms, les adresses, les numéros de sécurité sociale, etc., sont associées a des transactions sur la Blockchain, il existe risque que ces informations soient exposées être utilisées a des fins malveillantes [11].

3.12. Problématique

La problématique du partage de données privées médicales entre les cliniques ou les hôpitaux est un sujet délicat et complexe qui soulève plusieurs préoccupations en matière de confidentialité, de sécurité et d'éthique.

3.13. Confidentialité des données

Les données médicales sont hautement sensibles et personnelles, contenant des informations sur la santé des individus, telles que les antécédents médicaux, les résultats d'examens, les traitements, etc. Le partage de ces données entre les établissements de santé nécessite des mesures strictes pour garantir la confidentialité et le respect de la vie privée des patients.

3.14. Consentement éclairé

Le partage des données médicales devrait se faire avec le consentement éclairé des patients. Les patients doivent être informés des finalités du partage, des entités impliquées, des types de données partagées et des mesures de sécurité mises en place. Ils devraient également avoir le droit de refuser ou de limiter le partage de leurs données.

3.15. Sécurité des données

Les établissements de santé doivent mettre en place des mesures de sécurité robustes pour protéger les données médicales contre les accès non autorisés, les fuites ou les cybers attaques. Cela comprend l'utilisation de technologies de cryptage, de pare-feu, de contrôles d'accès et de pratiques de gestion des risques.

3.16. Interopérabilité des systèmes

Les cliniques et les hôpitaux utilisent souvent des systèmes informatiques différents pour gérer leurs données médicales, ce qui peut rendre difficile le partage efficace des informations. L'interopérabilité des systèmes et l'adoption de normes communes sont essentielles pour faciliter l'échange de données tout en préservant leur intégrité et leur sécurité.

Brièvement, le partage de données privées médicales entre les cliniques ou les hôpitaux est un enjeu complexe qui nécessite une approche équilibrée, tenant compte à la fois des bénéfices potentiels pour les soins de santé et de la protection de la vie privée des patients. Il est crucial d'établir des politiques et des pratiques solides pour garantir la confidentialité, la sécurité lors du partage de telles données.

3.17. Travaux connexes

PPSF [12] Dans ce travail vise à proposer un cadre de Blockchain intelligent qui intègre la technique d'apprentissage automatique pour protéger la confidentialité et la sécurité dans les villes intelligentes axées sur l'IoT qui utilise une approche à deux niveaux pour préserver la confidentialité des données et propose une architecture intégrée IoT-brouillard-Cloud avec Blockchain-IPFS. Dans la préservation de la vie privée, une technique Pow pour vérifier l'intégrité des données basée sur la Blockchain et les contrats intelligents et ACP (Analyse en Composantes Principales).

PrivySharing [13], Bien qu'ils proposent un mécanisme qui partage des données d'une manière sécurisée et préservant la confidentialité basée sur la Blockchain de consortium autorisée pour les villes intelligentes et basé aussi sur les règles ACL définies par l'utilisateur et intégrées dans les contrats intelligents. De plus, les résultats ont validé que le réseau Blockchain multi canaux est plus évolutive par rapport à une Blockchain mono canaux. À l'avenir, l'étude de ce travail sera à intégrer le concept des nœuds de brouillard basés sur les stations BTS mobiles existantes et également à concevoir un mécanisme d'intégration sécurisée des appareils IoT avec le réseau Blockchain.

Tableau 1. Tableau d'étude détaillée entre deux approches distinctes

Méthode	Titre	Description	Technologie
Avec Blockchain	**[12] PPSF**	Le PPSF proposé est basé sur deux mécanismes clés : • Un schéma de confidentialité à deux niveaux en intégrant un module Blockchain et ACP. • Un schéma de détection d'intrusion ; Détecteur (GBAD).	• Architecture Fog-Cloud. • Internet des objets. • PoW • ACP • Apprentissage automatique. • Blockchain.
Sans Blockchain	**[13] PrivySharing**	• Un mécanisme qui partage des données d'une manière sécurisé et préservant la confidentialité basée sur la Blockchain de consortium. • Autorisée pour les villes intelligentes et basé aussi sur les règles ACL définies par l'utilisateur et intégrées dans les contrats intelligents. Cette stratégie garantit que les données utilisateurs restent confidentielles et sécurisé	Blockchain de consortium. Les contrats intelligents.

4. Conclusion

Depuis quelques années, on assiste à une révolution numérique dans de nombreux domaines, la mise en œuvre de mesures de sécurité, telles que le chiffrement, l'authentification, le contrôle d'accès, la sécurité du réseau et la sécurité des applications, pour les appareils IOT et leurs vulnérabilités inhérentes est inefficace, et a cette fin. Dans le chapitre suivant, nous avons essayé d'écrire un modèle qui est base sur un réseau Blockchain pour le partage et l'accès aux données dans une manière sécurisée, nous avons intégré cette technologie avec un système de fichier interplanétaire (IPFS) pour le stockage des données.

Chapitre 2 : Notre solution de confidentialité compatible avec la Blockchain dans les villes Intelligentes

1. Introduction

Dans le but de renforcer la vie privée et la confidentialité dans la ville intelligente, la Blockchain peut être un moyen efficace, surtout s'il est renforcé par d'autres moyens cryptographiques, comme nous l'avons fait pour réaliser notre modèle. L'objectif de notre modèle est de présenter une approche proposée pour la gestion sécurisée des données médicales des patients à l'aide de l'identité numérique et de la technologie de la Blockchain, IPFS et les contrats intelligents pour permettre le partage sécurisé des données médicales entre les cliniques et les hôpitaux. L'utilisation de notre modèle entre plusieurs cliniques médicales est basée sur le stockage des données dans un IPFS intégré par un réseau Blockchain et le partage sécurisé des données médicales à l'aide des contrats intelligents. L'objectif principal est de garantir la sécurité, la confidentialité et la traçabilité des données tout en offrant un système décentralisé et transparent.

2. Description de notre approche

Dans notre approche nous avons intégré Blockchain et IPFS qui sont deux technologies distinctes mais complémentaires, l'intégration de ces derniers ce qui est très utile pour une application de partage des données privées entrent les cliniques ou les hôpitaux parce que la traçabilité de partage et la sécurité, confidentialité des données privées sont garantie.

La plateforme Ethereum nous permet d'écrire des codes exécutables en mode Turing complet dans une Blockchain qui est sécurisée, immutable, privé. Le code sera exécuté dans la machine virtuelle de manière décentralisée et se chargera de la lecture, de l'écriture des données, du transfert de la valeur, de la prise des décisions. C'est là qu'on définit la logique de cette application. C'est très important pour une application de partage et d'accès aux données parce que cela signifie que les règles ne changeront pas toute en gardant la transparence du partage, ce code est appelé un Smart contrat car il représente une sorte d'alliance ou accord de notre partage.

L'accord de notre contrat intelligent est présenté comme suit :

- **Autorisations d'accès**

Les cliniques peuvent créer un smart contrat qui spécifie les conditions d'accès et de partage des données privées. Les autorisations d'accès peuvent être définies de manière granulaire, en précisant quelles données peuvent être partagées, avec qui et dans quelles circonstances.

- **Consentement du patient**

Avant de partager des données privées, le consentement du patient peut être enregistré sous forme d'un smart contrat. Cela garantit que le patient a donné son consentement éclairé et que les données ne sont partagées qu'avec son autorisation.

- **Contrôle d'accès**

Nous avons utilisé les smart contrats pour contrôler l'accès aux données partagées. Ils permettent de mettre en place des règles strictes concernant qui peut accéder aux données, pour combien de temps et à quelles fins. Cela renforce la confidentialité et limite les risques de mauvaise utilisation des données.

- **Adaptabilité**

Étant donné que les transactions sur une Blockchain sont immuables et transparentes, l'utilisation de smart contrats permet de suivre et d'auditer toutes les activités de partage de données. Cela facilite la vérification de la conformité et renforce la confiance entre les cliniques.

- **Sécurité renforcée**

Les données partagées sont cryptées et stockées de manière sécurisée sur un IPFS intégrer sur un réseau Blockchain, ce qui réduit les risques de violation de la sécurité et de piratage.

Notre solution dans ce travail est une application décentralisée en tous sens :

- Un réseau décentralisé présenté en p2p.
- Les données sont décentralisées car elles sont partagées entre tous les nœuds.
- Le code est décentralisé car il est également partagé et exécuté sur tous les nœuds.

Nous allons aussi concevoir une application coté client sous forme d'un site web (html, java script, css) et au lieu d'une connexion a un serveur web, on aura une connexion à une Blockchain privée.

On a choisi de déployer notre Smart contrat dans une Blockchain consortium car il y a un nombre restreint et choisi de nœuds peut lire le grand registre et peut participer à la validation des blocs ce qui renforce la sécurité et confidentialité du réseau.

La preuve de travail Ethash est le type de minage actuel de la Blockchain Ethereum fournir un consensus sécurisé et décentralisé au sein du réseau, qui s'appuie sur des calculs de hash successives d'un bloc pour atteindre une valeur de hash qui correspond à la difficulté du bloc, c'est couteux en termes de ressources mais garanti un niveau de sécurité élevée. En bref le travail doit être difficile a réalisé par les mineurs car utilisent leur puissance de calcul pour résoudre des problèmes mathématiques complexes. Le temps moyen de la validation d'un bloc est de 15 secondes avec Ethash ce temps peut varier en fonction de plusieurs facteurs, tel que la puissance de calcul déployée par les mineurs sur le réseau, la difficulté de l'algorithme de preuve de travail, ainsi que le nombre de transactions à inclure dans le bloc.

3. Description détaillée de l'approche proposée

Chaque clinique crée une identité numérique unique qui lui est associée, et stocke les données médicales de ses patients. Ces données peuvent inclure des informations telles que les antécédents médicaux, les résultats de laboratoire, les prescriptions, etc. Chaque transaction de données est sécurisée et liée à l'identité numérique de la clinique selon les mécanismes de sécurité de la Blockchain, tiennent compte du fait que les données n'ont pas été altérées et avérées. Lorsqu'un patient se rend dans une autre clinique, la clinique d'origine peut partager les données médicales spécifiques du patient avec la nouvelle clinique de manière sécurisée et transparente, Cela peut être réalisé en utilisant des contrats intelligents, où les paramètres de confidentialité et les autorisations d'accès sont définis par l'administration de la clinique. Voici le schéma suivant qui résume le fonctionnement du notre modèle.

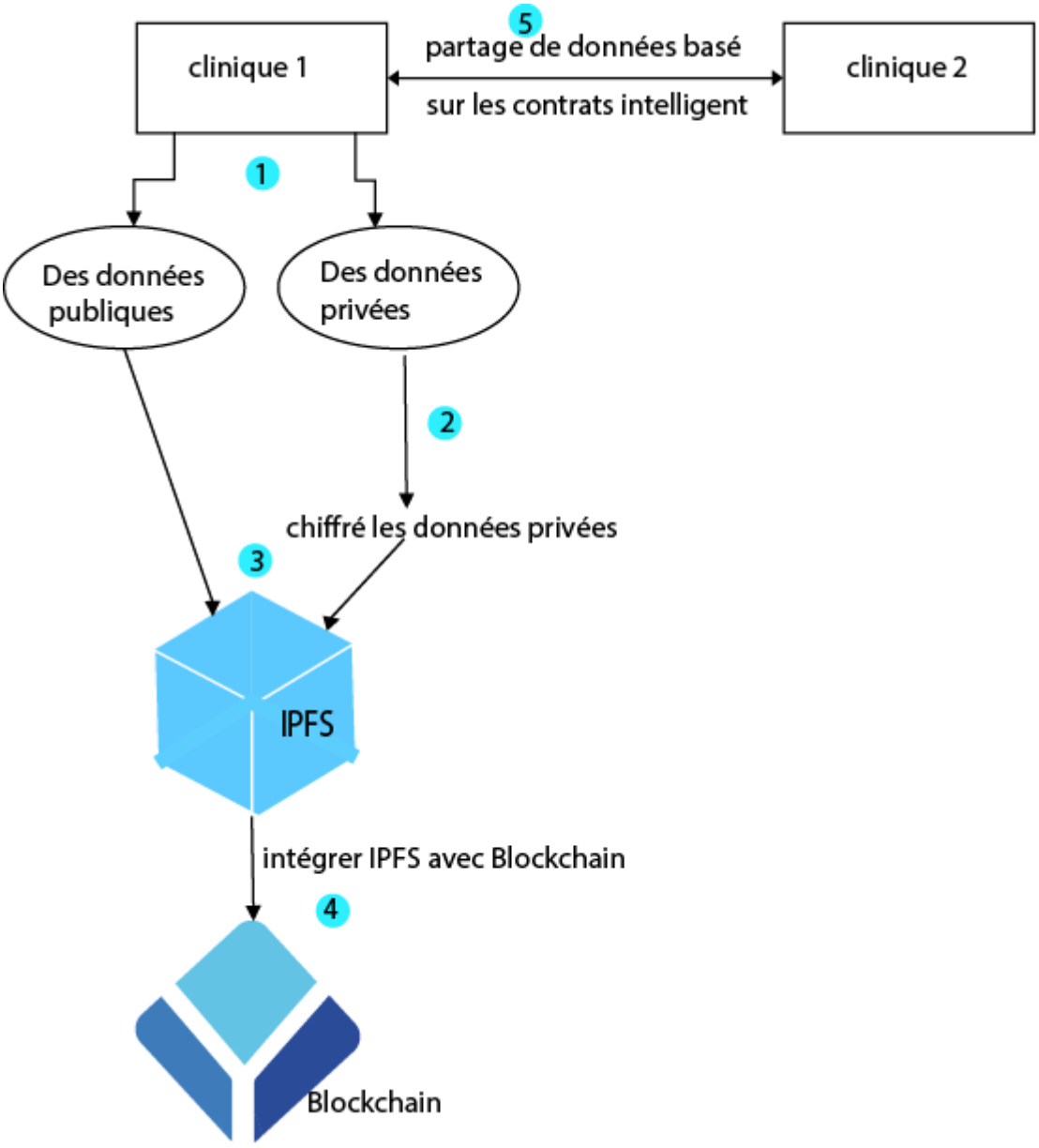


Figure 6 : Schéma de fonctionnement du modèle

4. Fonctionnement de notre modèle

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

- **Cryptage des données**

Chaque clinique contient deux types de données, des données publiques et des données privées. Les données publiques dans le contexte des analyses médicales et des radios se réfèrent généralement aux informations non confidentielles et dépersonnalisées. En revanche, les données privées agissent des informations personnelles identifiables telles que le nom de patient, l'adresse la date de naissance du résultat des tests médicaux et pour sécuriser les

données privées en doit chiffré ses données par l'algorithme de cryptage solide AES. Le cryptage des données privées avant de les stocker dans IPFS est une bonne pratique pour assurer la confidentialité et la sécurité des informations.

- **L'algorithme de cryptage AES**

L'algorithme de cryptage AES (Advanced Encryption Standard) fonctionne en utilisant une clé de chiffrement pour transformer les données originales en données chiffrées et vice versa. Voici comment il fonctionne en général :

1. **Clé de chiffrement** : Cette clé est essentielle pour chiffrer et déchiffrer les données. Elle peut être de différentes longueurs, comme 128, 192 ou 256 bits, en fonction du niveau de sécurité souhaité.
2. **Substitution :** L'algorithme AES utilise une technique de substitution. Il divise les données en blocs de 128 bits (16 octets) et applique une série de substitutions à chaque octet de ces blocs, en utilisant la clé.
3. **Permutation :** Ensuite, il effectue une permutation des octets dans le bloc, ce qui signifie qu'il réorganise les octets d'une manière spécifique, également basée sur la clé.
4. **Mélange :** Enfin, l'algorithme mélange les octets dans le bloc de données d'une manière déterminée par la clé. Ce processus est répété un certain nombre de fois, en fonction de la longueur de la clé et du niveau de sécurité souhaité.

Le résultat final est un bloc de données chiffrées qui est extrêmement difficile à décrypter sans la clé de chiffrement appropriée. Pour déchiffrer les données, le même processus est inversé en utilisant la clé de déchiffrement correspondante.

L'utilisation de l'AES pour chiffrer des données privées avant de les stocker dans IPFS est une mesure de sécurité importante pour protéger la confidentialité des informations médicales personnelles. Cela garantit que seules les personnes autorisées avec la clé appropriée peuvent accéder aux données sensibles.

Figure 7 : Illustration sur le chiffrement [21]

- **Stockage des données**

Les deux types de données sont stockés dans IPFS qui est intégré avec un réseau Blockchain. IPFS fournit un système de fichiers distribué et adressable par le contenu, permettant de stocker et de récupérer des fichiers en fonction de leur contenu plutôt que de leur emplacement, en revanche la Blockchain utilisée pour stocker les identifiants de contenu IPFS (cid) en chaîne. Cette intégration permet un stockage de fichiers décentralisé, où les fichiers sont stockés sur IPFS et leurs références ou métadonnées sont stockées sur la Blockchain.

- **L'accès et le partage de données**

Le partage de données sera utilisé par des contrats intelligents et l'accès à ces données sera grâce à l'application distribuée D'App. Lorsque nous avons stocké des données dans IPFS, chaque fichier ou ensemble de données est identifié par un Content Identifier (CID) unique. Ce CID est utilisé pour référencer les données et les récupérer ultérieurement. Dans notre application DApp, nous avons conservé les CID associés aux données que nous souhaitons accéder et partager.

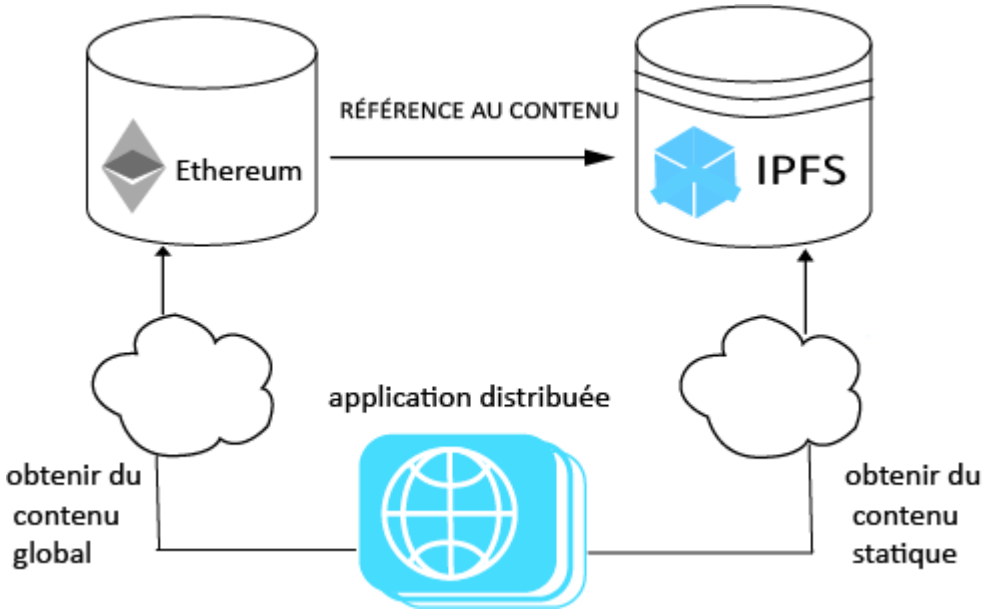


Figure 8 : schéma représente l'intégration de l'IPFS avec Ethereum [14]

- **Sécurité et confidentialité des données**

Le contrat intelligent contrôle les accès aux données qui autorise l'accès seulement aux médecins et aux administrateurs de la clinique, et spécifie les types de données qui peuvent être partagées et les cliniques qui y ont accès. Par exemple, il peut être configuré pour autoriser l'accès uniquement aux informations pertinentes pour le traitement d'un patient spécifique, et cet accès se fait l'aide d'un identifiant de contenu IPFS (cid) qui est définit dans le contrat intelligent.

5. Validation et exécution des transactions

Les transactions sont exécutées après vérification de leur validité. Voici les tests initiaux de la vérification :

- Une transaction doit être bien formée et codée RLP sans octets supplémentaires.
- La signature numérique utilisée pour signer la transaction est valide.
- Le nonce de transaction doit être égal au nonce courant du compte de l'expéditeur.
- La limite de gaz ne doit pas être inférieure au gaz utilisé par la transaction.
- Le compte de l'expéditeur contient un solde suffisant pour couvrir les frais d'exécution.

6. Le mécanisme de validation des blocs

Un bloc Ethereum est considéré comme valide s'il réussit les contrôles suivants :

- Cohérent avec les oncles et les transactions, le terme ‘oncles’ fait référence a des blocs qui étaient en compétitions pour être ajoutés à la Blockchain, mais qui n’ont pas été sélectionnés comme le bloc principal. La cohérence avec les oncles signifie que le bloc doit également être compatible avec d’autres blocs qui ont été extraits en même temps. Cela signifie que tous les Oncles satisfait la propriété qu'ils sont effectivement des oncles et aussi leurs preuves de travail est valide. Cela garantit la sécurité du réseau Ethereum.
- Si le bloc précédent (parent) existe et est valide.
- Si l'horodatage du bloc est valide. Cela signifie essentiellement que l’horodatage du bloc courant doit être supérieur à celui du bloc parent. Tous les temps de bloc sont calculés en temps Unix. Si l'un de ces contrôles échoue, le bloc sera rejeté.

7. La combinaison d'IPFS et de Blockchain peut offrir plusieurs avantages

Au lieu de stocker des fichiers volumineux directement sur la Blockchain, IPFS peut stocker les fichiers et fournir leurs identifiants de contenu (hachages IPFS) sur la Blockchain. Cela réduit la charge de stockage sur la Blockchain tout en maintenant l'immuabilité et l'intégrité des données stockées.

Au lieu de stocker toutes les données sur la Blockchain, seul le hachage IPFS est stocké, qui agit comme un pointeur vers le contenu. Cela garantit une utilisation efficace des ressources de la Blockchain.

Créer une application distribuée décentralisée DApp. La Blockchain peut gérer les aspects consensuels et transactionnels, tandis que IPFS peut fournir une couche de stockage distribuée et résiliente pour les données et les fichiers de l'application. Cela permet le développement de DApp avec une évolutivité, une résistance à la censure et une disponibilité des données améliorées.

IPFS peut être utilisé pour les plates-formes décentralisées de partage de fichiers et de distribution de contenu. Des incitations basées sur la Blockchain et des contrats intelligents peuvent être utilisés Pour encourager un écosystème autonome pour la distribution de contenu.

8. La différence entre notre application D'App et une application centralisée classique

Les deux principales différences entre les applications ordinaires et les DApps sont les suivantes :

1. Au lieu que l'interface utilisateur interagisse avec un programme traditionnel, ils interagissent avec des contrats intelligents.

2. Au lieu que le backend de l'App soit hébergé sur un seul ordinateur personnel ou sur les serveurs centralisés d'une seule entreprise quelque part, les DApps sont hébergées sur de nombreux ordinateurs à travers le monde via un réseau peer-to-peer et leurs données sont enregistrées sur une blockchain publique.

3. Une DApp peut faire tout ce qu'une application ordinaire peut faire, mais notamment elle aussi, au moins le backend a les qualités d'être « distribué et décentralisé ».

4. Les DApp peuvent être sur les réseaux cryptographiques, mais elles ne sont pas seulement destinées aux jetons.

5. Ethereum et d'autres plateformes de ce type permettent des types d'applications sans confiance autres que financières.

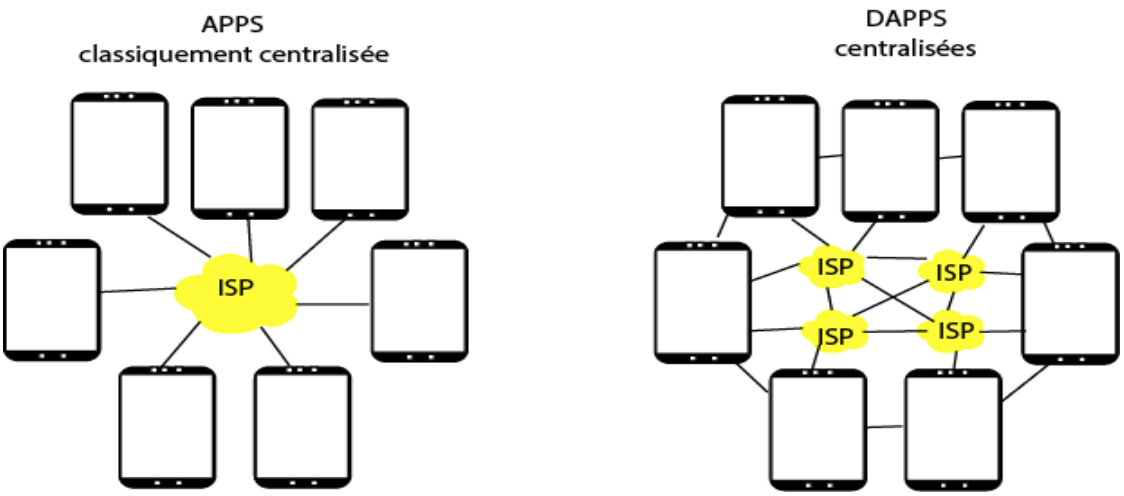


Figure 9 : Schéma représente la différence entre notre application DAPP et une application classique [15]

9. Conclusion

Dans ce chapitre nous avons proposé notre solution pour avoir un maximum de transparence, d'intégrité, d'immutabilité et de traçabilité des données sans autorité intermédiaire. Nous avons implémenté notre solution qui est un contrat intelligent, puis nous avons déployé notre contrat intelligent dans un réseau de test pour mieux tester son comportement.

Dans le chapitre suivant nous parlerons des outils utilisés dans notre modèle avec les résultats obtenue et l'évaluation de notre travail.

Chapitre 3 : Implémentation

1. Introduction

2. Environnement de développement

Langages de programmation des contrats intelligents

Les contrats peuvent être programmés dans une variété de langages. Nous avons utilisé le langage solidity parce qu'est le sécurisé para port aux autres langages.

Solidity

C'est un langage à typage statique, ce qui signifie que la vérification du type de variable en Solidity est effectuée au moment de la compilation. Chaque variable, qu'elle soit d'état ou locale, doit être spécifiée avec un type lors de la compilation. C'est un avantage aux sens que toute validation et vérification est terminée au moment de la compilation et que certains types de bugs, tels que l'interprétation des types de données, qu'elles peuvent être détectés dans le cycle de développement plutôt qu'au moment de l'exécution, ce qui pourrait être coûteux, les autres fonctionnalités du langage incluent l'héritage, les bibliothèques et la possibilité de définir des types de données composites. La syntaxe de Solidity est très similaire à C et JavaScript, et il est assez facile à programmer avec le concept orienté objet avec des notions et des mots clés spéciaux, compréhensible par la machine virtuelle Ethereum. Ce langage est l'objet de ce chapitre.

Compilateur

Les compilateurs sont utilisés pour convertir le code source des Smart contrats de haut niveau au format compris par l'environnement d'exécution Ethereum. Solc est le compilateur de Solidity qui convertit un code de haut niveau en un bytecode Ethereum Virtual Machine (EVM) afin qu'il puisse être exécuté sur la Blockchain par l'EVM.

Développement et déploiement d'un Smart contrat

Dans cette partie nous allons voir les outils de développement des Smart contrats sur la plateforme Ethereum, quand et comment nous avons utilisé. Diverses étapes doivent être franchies pour développer et déployer des Smart contrats. En gros, elles peuvent être

divisées en quatre étapes : écriture, test, vérification et déploiement. L'étape d'écriture consiste à écrire le code source du contrat. Cela peut être fait dans n'importe quel éditeur de texte. Les tests sont généralement effectués par des moyens automatisés comme Truffe, qui utilise le cadre Mocha pour tester les contrats.

Cependant, des tests manuels peuvent également être effectués. Une fois que le contrat est vérifié, fonctionne et testé sur un environnement simulé (Private Net), il peut être déployé sur le Test Net Ropsten ou Kovana et enfin, sur le Main Net.

Installation des outils de développement

Tout d'abord, nous allons installer et configurer une Blockchain privée pour développer un Smart contrat localement.

La Blockchain personnelle Ganache

Ganache est une Blockchain personnelle de développement local. Cela nous permettra de déployer des Smart contrats, de développer des applications et d'exécuter des tests. Nous avons choisi Ganache car il nous fournit 10 comptes Ethereum avec une balance de 100 ether (du faux ether) pour chaque compte, ainsi une interface graphique qui nous permet d'examiner tout ce qui se passe dans cette Blockchain.

Node.JS

Nous devons configurer notre environnement pour développer des Smart contrats.

La première dépendance dont nous aurons besoin est Node Package Manager, où NPM, fourni avec Node.js.

Framework Truffle

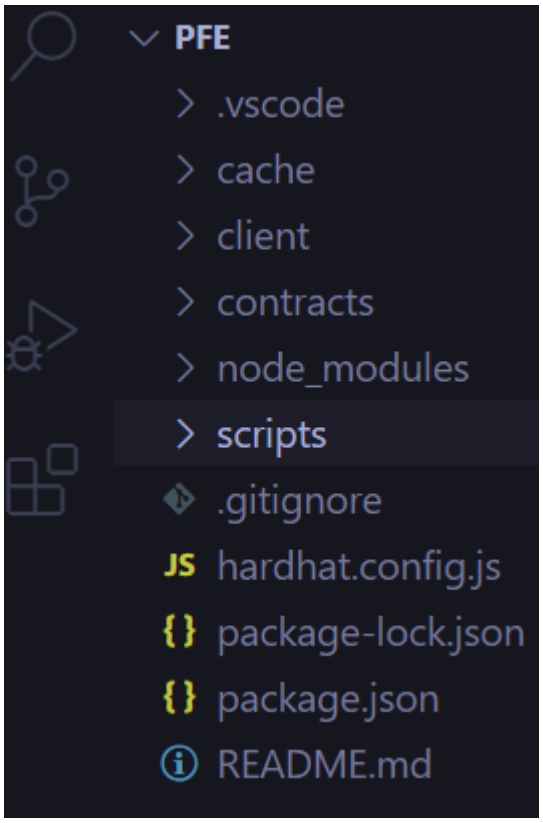
Truffle est un Framework qui fournit une suite d'outils permettant de développer des Smart contrats Ethereum avec le langage de programmation Solidity.

Nous avons choisi Truffle pour le développement de notre application car c'est un Framework puissant qui nous facilite l'interaction avec notre Smart contrat et il nous permet d'effectuer des tests, développer une interface coté client de notre Smart contrat, la déployé dans n'importe quel réseau Ethereum. Voici un aperçu de toutes les fonctionnalités du Framework Truffle.

Framework Hardhat

Hardhat est un cadre de développement populaire pour les contrats intelligents Ethereum. Il fournit un ensemble complet d'outils et de fonctionnalités qui simplifient le développement,

les tests et le déploiement de contrats intelligents.



Gestion des Smart contrats

Rédiger des Smart contrats avec Solidity et les compiler en bytecode pour exécuter sur Ethereum Virtual Machine (EVM).

Tests automatisés

Écrire des tests sur les Smart contrats pour assurer qu'ils se comportent comme convenu. Ces tests peuvent être écrits en JavaScript ou Solidity, et peuvent être exécutés sur n'importe quel réseau configuré par Truffle.

Déploiement et Migration

Écrire des scripts pour migrer et déployer des Smart contrats sur n'importe quel réseau Ethereum.

Gestion du réseau

Se connecter à n'importe quel réseau public Ethereum, ainsi qu'à tout réseau Blockchain personnel pour des fins de développement.

Console de développement

Interagir avec des Smart contrats dans un environnement d'exécution JavaScript avec la console Truffle. Pour ce faire, il suffit de se connecter à n'importe quel réseau de Blockchain

spécifié dans la configuration du réseau.

Développement côté client

Configurer le projet Truffle pour héberger des applications côté client qui communiquent avec les Smart contrats déployés dans la Blockchain

Le portefeuille Metamask

La plupart des principaux navigateurs Web ne se connectent pas aux réseaux décentralisés, le plugin Metamask vous permet de transformer un navigateur Web en un navigateur Blockchain, nous avons choisi Metamask car il permet également la gestion des comptes Blockchain, ainsi que les fonds Ether pour payer les transactions.

Pinata

Est un service tiers populaire utilisé pour le stockage décentralisé de fichiers sur la blockchain Ethereum. Il permet de télécharger des fichiers, de les héberger de manière décentralisée et de générer des liens permanents (hash) pour accéder à ces fichiers.

Configuration d'environnement

Nous allons d'abord créer un répertoire qui va contenir les fichiers de notre projet comme ceci :

```
mkdir MonApplication
cd MonApplication
```

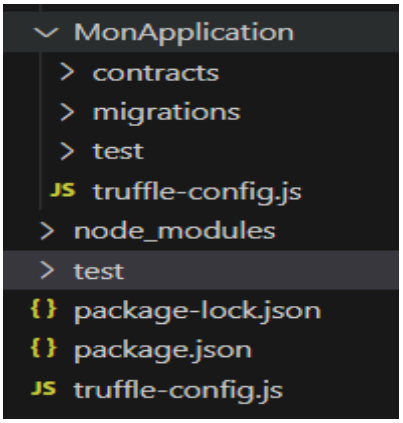
Maintenant, nous initialisons un nouveau projet de truffe pour développer notre projet comme ceci :

```
truffle init
```

Après il faut installer les dépendances par cette commande :

```
npm install
```

Maintenant que les dépendances sont installées, examinons la structure de répertoire de projet que nous venons de créer :



Répertoire des contrats

C'est là que se trouve tous les Smart contrats. Nous avons déjà un contrat de migration qui gère nos migrations vers la Blockchain.

Répertoire migrations

C'est là que résident tous les fichiers de migration. Ces migrations sont similaires aux autres infrastructures de développement Web qui nécessitent des migrations pour modifier l'état d'une base de données. Chaque fois que nous déployons des Smart contrats sur la Blockchain, nous mettons à jour l'état de la Blockchain et nous avons donc besoin d'une migration.

Répertoire Node modulés

C'est le répertoire de toutes nos dépendances de node que nous venons d'installer.

Répertoire de test

C'est là que nous allons écrire nos tests pour notre Smart contrat.

Fichier truffle-config.js

Il s'agit du fichier de configuration principal de notre projet Truffle, dans lequel nous allons gérer des tâches telles que la configuration réseau.

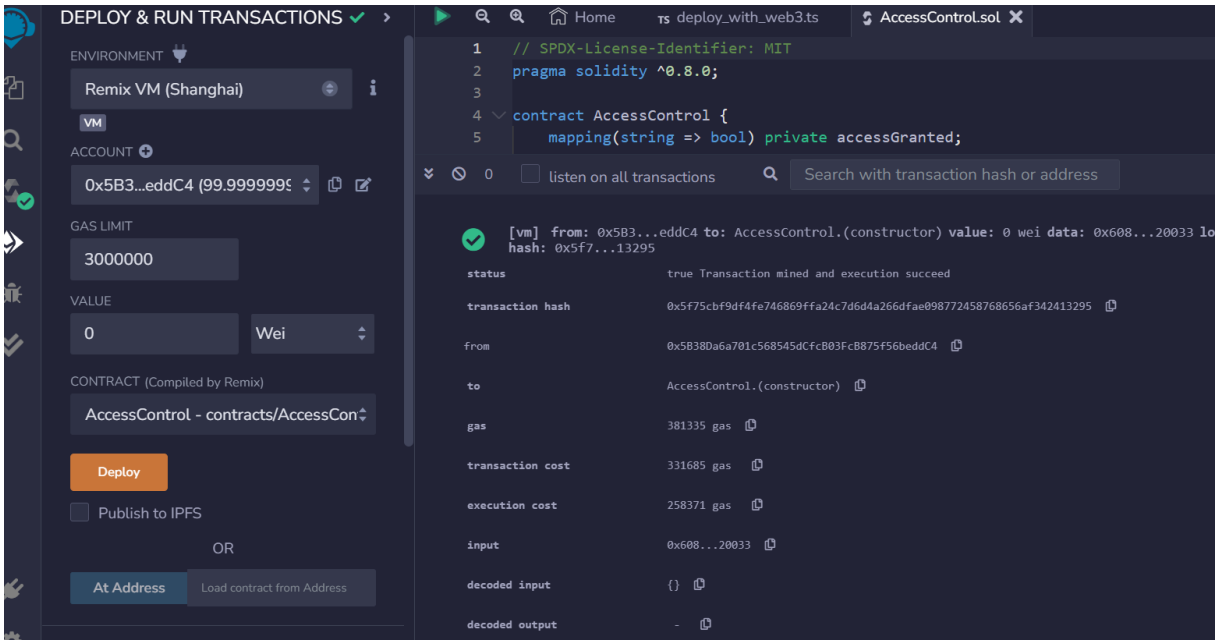
Maintenant on peut créer notre contrat intelligent par la création d'un fichier ContratStorage.sol dans le répertoire 'contracts '. On doit spécifier la version de notre compilateur Solidity comme suite :

```
pragma solidity 0.8.9;
```

3. Réalisation du modèle

➢ Créer un contrat intelligent et le déployer sur Remix

Le principe du contrôle d'accès dans un contrat intelligent repose sur l'utilisation de mots-clés et de fonctionnalités spécifiques pour limiter l'accès à certaines parties du contrat à des utilisateurs autorisés



➢ Déployer un contrat intelligent sur vs code

Une transaction est créée avec comme destinataire l'adresse du contrat intelligent. Cette transaction est soumise au réseau Ethereum pour être incluse dans un bloc.

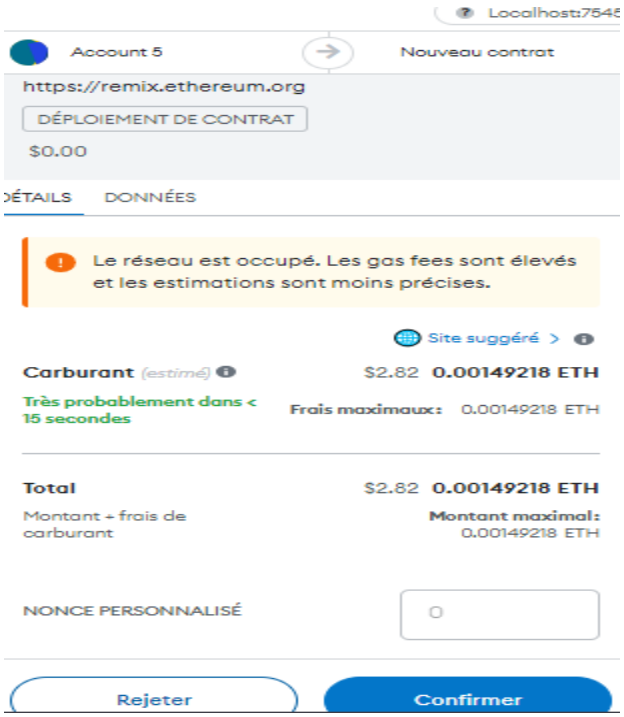
```
Deploying 'AccessControl'
-------------------------
> transaction hash:    0x93560f4e1900d7b48b8e0673a2e8c9c1bdd1add687f96c5572de88ea96485f11
> Blocks: 0            Seconds: 0
> contract address:    0x5D4d05E4B1c7C83339ee5A10Eacca75197d1a13c
> block number:        7
> block timestamp:     1687696078
> account:             0xB740E99D3033AeB6bbB8329291d1c45D97Dee62f
> balance:             99.957589400358354996
> gas used:            314562 (0x4ccc2)
> gas price:           3.155588211 gwei
> value sent:          0 ETH
> total cost:          0.000992628138828582 ETH

> Saving artifacts
-------------------------------------
> Total cost:     0.000992628138828582 ETH
```

➢ Choisir l'environnement

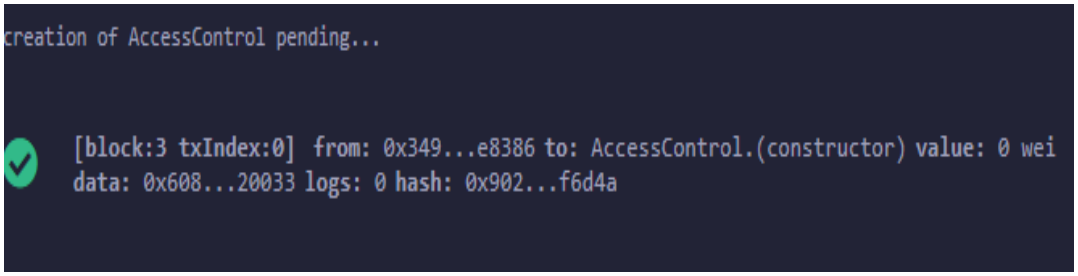
On choisit le réseau Ethereum, y compris des réseaux de test tels que Ropsten, Rinkeby et Kovan, ainsi que le réseau principal Ethereum (Mainnet). Une fois l'environnement

sélectionné, Remix utilisera les paramètres spécifiques à cet environnement, tels que l'URL du nœud de ce réseau, pour compiler, déployer et tester les contrats intelligents.

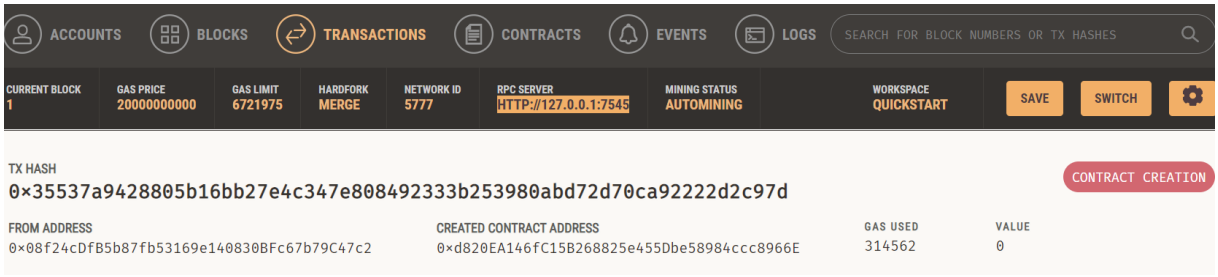
- Choisir l'adresse à laquelle on souhaite envoyer une transaction
- Se connecter avec le réseau localhost dans Metamask et confirmer la transaction



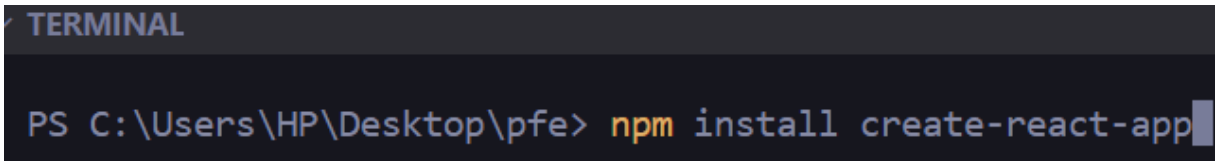
- Après la validation de la transaction : Les mineurs du réseau Ethereum vérifient la validité de la transaction. Cela implique de s'assurer que l'expéditeur a suffisamment de fonds pour payer les frais de gaz et que la transaction respecte les règles du protocole Ethereum.
- Après le déploiement d'un contrat intelligent dans Remix, un nouveau block est ajouté à la Blockchain pour enregistrer cette action. On obtient différents résultats et informations, notamment le résultat du déploiement lui-même et le hash de la transaction associée.



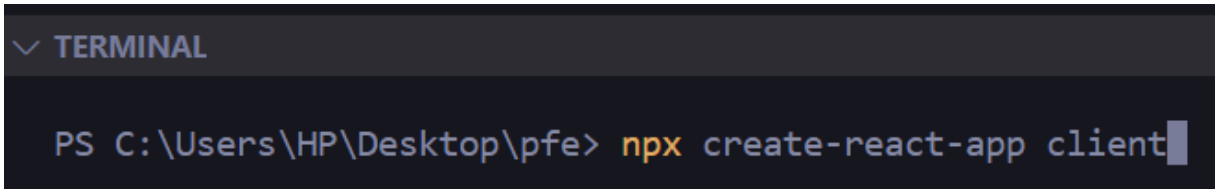
- Dans l'interface graphique Ganache, il y a une liste de comptes générés par Ganache avec leurs adresses et soldes associés. Chaque compte est accompagné d'une liste des transactions associées. Une fois qu'on identifie l'adresse de la transaction, affiche la liste des transactions dans l'interface graphique Ganache.



- Pour afficher l'interface d'un contrat intelligent à l'aide de React :



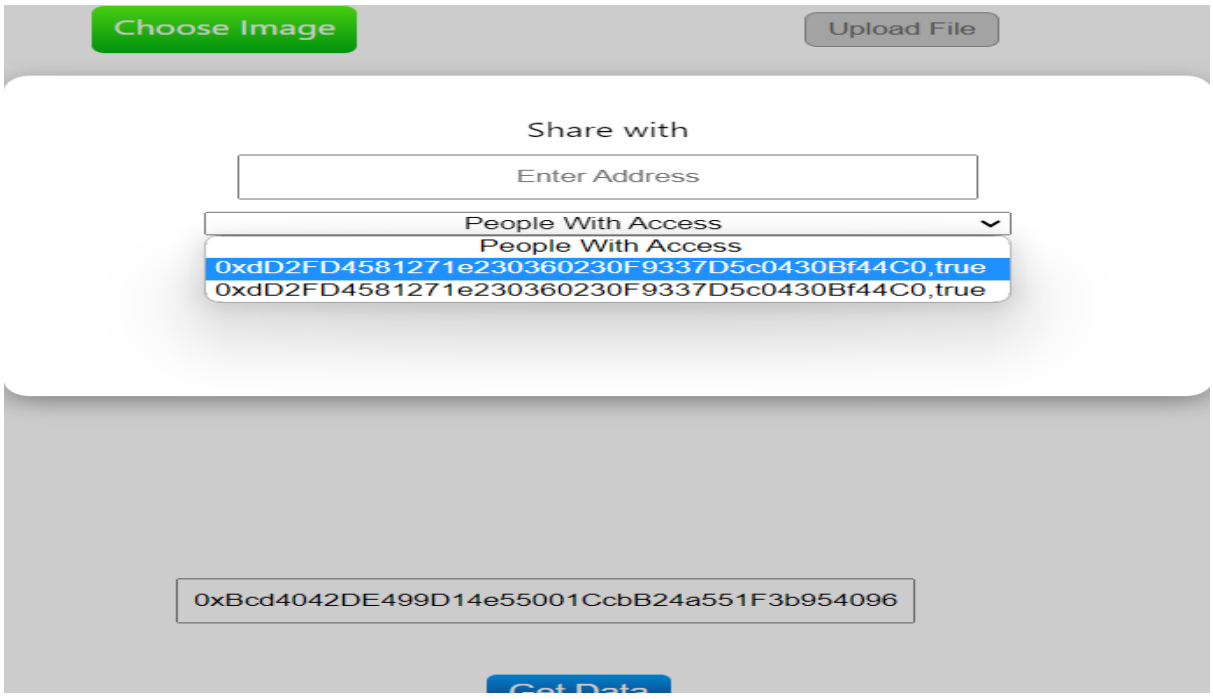
- Le fichier Client, contient le code qui définit le composant React responsable de l'affichage de l'interface utilisateur d'un contrat intelligent.



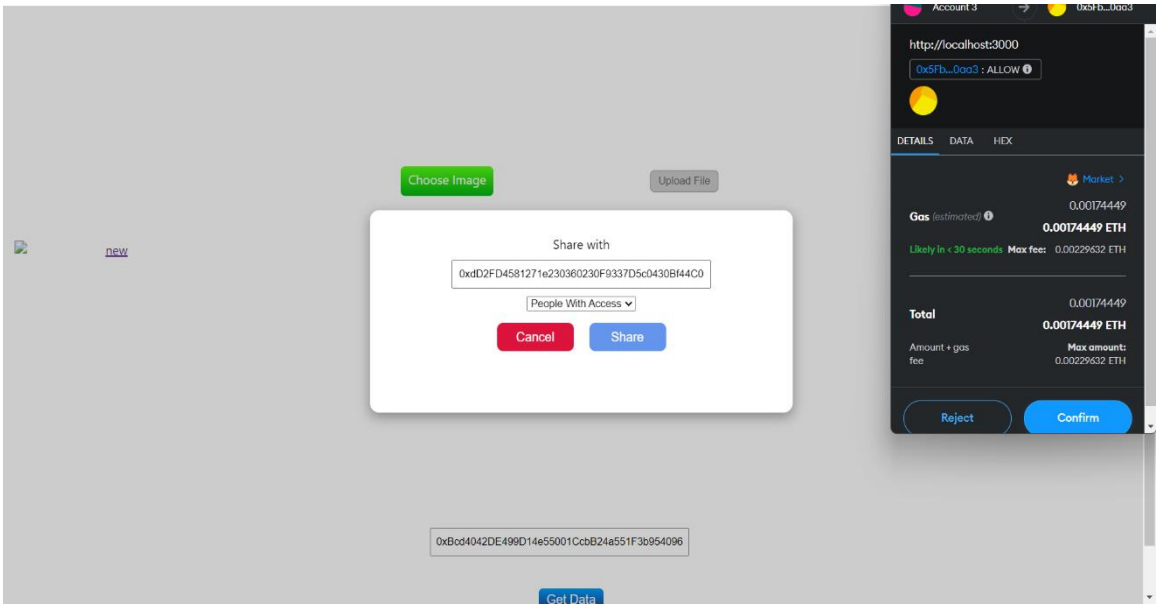
- L'interface

- Cette interface permet à un utilisateur d'ajouter des URL (adresse de ressources) et de partager l'accès des URL avec d'autre utilisateur

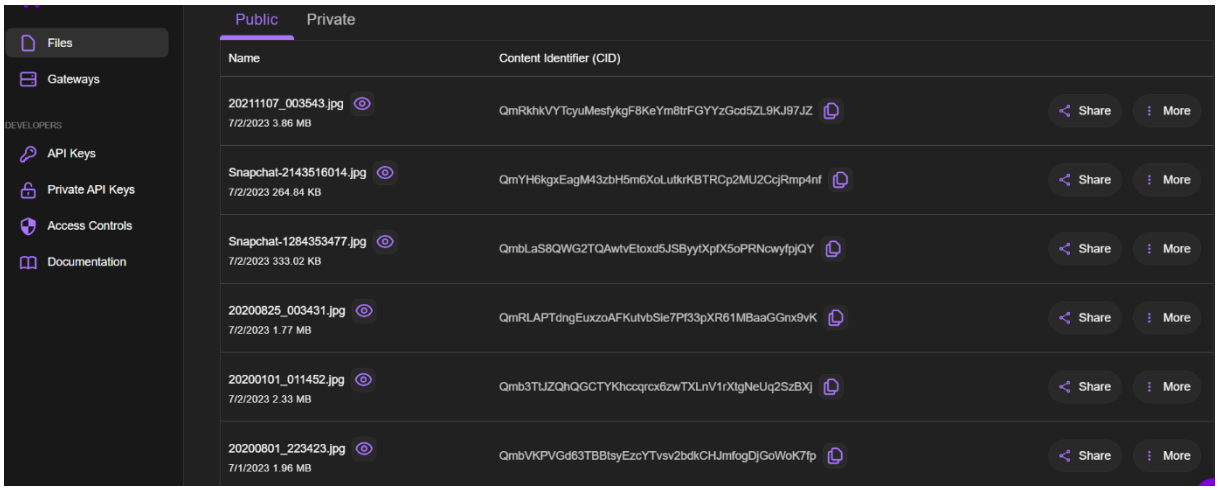
- Lorsqu'un utilisateur souhaite donner l'accès à un autre utilisateur, il appelle la fonction "allow" du contrat en spécifiant l'adresse de l'utilisateur auquel il souhaite donner l'accès. Cette fonction modifie l'état du contrat en mettant à jour les mappings et "accessList" correspondants. Chaque action nécessite une transaction pour donner l'accès à certains utilisateurs



- Chaque fois qu'un utilisateur souhaite donner l'accès à un autre utilisateur, il doit envoyer une transaction Ethereum pour exécuter la fonction "allow" du contrat. Cela garantit que toutes les modifications de l'accès sont enregistrées de manière immuable dans la blockchain Ethereum.



- Dans le contrat intelligent, on ajoute des fonctions qui utilisent le hash IPFS pour récupérer les données stockées sur Pinata. Créer une fonction qui prend le hash IPFS en tant que paramètre et renvoie les données correspondantes stockées sur Pinata. De cette manière, le contrat intelligent peut interagir avec les données stockées sur Pinata en utilisant les hash IPFS comme identifiants.



4. Analyse générale des différentes solutions pour la protection de la vie privée

Voici le tableau :

Tableau 2: Tableau d'analyse de notre approche avec d'autres solutions

	Notre solution	**Binder**	**IPFS**
Utiliser Blockchain	Oui	Oui	Oui
Utiliser IPFS	Oui	Non	Oui
Intégrité	Oui	Oui	Oui
Confidentialité	Oui	Oui	Oui
Rapidité	Oui	Non	Non
Problème de stockage	Oui	Non	Oui
Modèle souple	Oui	Oui	Non

5. Discussion

Dans cette étude, une approche est présentée pour renforcer la protection des données privées lors de leur partage en utilisant les mécanismes de sécurité de la Blockchain. Le problème de stockage des données est résolu en créant plusieurs canaux pour différents types de données. Cependant, cette solution s'avère moins efficace pour gérer des données similaires. De plus, diverses technologies d'apprentissage automatique sont explorées pour l'analyse des données et la détection de modèles, notamment l'utilisation de techniques telles que le boosting de gradient. Ces données sont stockées dans une Blockchain intégrée à IPFS après avoir été soumises à une technique de réduction de dimensionnalité, appelée PCA.

Néanmoins, l'emploi de multiples techniques et technologies a introduit une complexité et une charge supplémentaires dans la conception et la mise en œuvre du système. Par conséquent, un modèle de partage de données plus souple, rapide et fonctionnel est proposé, spécifiquement conçu pour gérer des données du même type, simplifiant ainsi le processus tout en maintenant l'intégrité et la confidentialité des données.

Conclusion Générale

La sécurité est l'un des problèmes critiques d'une ville intelligente, la Blockchain a prouvé son efficacité dans le domaine de la sécurité et la décentralisation dans diffèrent secteurs d'application dans le monde. Elle a apporté beaucoup de nouveaux concepts et d'idées dans le domaine de la recherches, proposant ainsi une nouvelle façon de concevoir les choses sans autorité intermédiaire, en s'appuyant sur les transactions et la cryptographie pour garder le système cohérant et sécurisé par l'ensemble des nœuds du réseau qui disposent d'une copie de la Blockchain et communiquent entre eux.

Notre travail consiste à étudier la technologie Blockchain et les villes intelligentes ainsi que la plateforme Ethereum, et de concevoir et implémenter une solution qui puisse parvenir à améliorer la protection de la vie privée dans les réseaux Blockchain dans les villes intelligentes à travers cette technologie pour garantir la transparence, l'intégrité, l'immutabilité des données.

Nous avons développé et déployer un Smart contrat dans la plateforme Ethereum qui assure le partage des données en toutes sécurité et confidentiel, nous avons aussi développé une interface graphique pour l'interaction des utilisateurs avec notre Smart contrat. Le futur travail de notre modèle serait axé sur l'évaluation, l'amélioration, l'extension et la sensibilisation de la solution développée pour renforcer la protection de la vie privée dans les réseaux Blockchains des villes intelligentes.

Bibliographie

[1] Suha Alawadhi, Armando Aldama-Nalda, Hafedh Chourabi, J Ramon Gil-Garcia, Sofia Leung, Sehl Mellouli, Taewoo Nam, Theresa A Pardo, Hans J Scholl, and Shawn Walker. Building understanding of smart city initiatives. In *International conference on electronic government*, pages 40–53. Springer, 2012.

[2] Aissani, Okba, Djahid Mekideche, and Ahmed Encadreur Alioua. *Vers un Système de Signalement Anonyme des Anomalies dans les Villes Intelligentes : une approche d'incitation basée sur la technologie de Blockchain*. Diss. Université de jijel, 2021.

[3] Meijer, Albert, and Manuel Pedro Rodríguez Bolívar 1. "La gouvernance des villes intelligentes. Analyse de la littérature sur la gouvernance urbaine intelligente." *Revue internationale des sciences administratives* 82.2 (2016) : 417-435.

[4] Edward O'Dwyer, Indranil Pan, Salvador Acha, and Nilay Shah. Smart energy systems for sustainable smart cities: Current developments, trends and future directions. *Applied energy*, 237 :581–597, 2019.

[5] Djamel Saba, Youcef Sahli, Brahim Berbaoui, and Rachid Maouedj. Towards smart cities: challenges, components, and architectures. In *Toward Social Internet of Things (SIoT): enabling technologies, architectures and applications*, pages 249–286. Springer, 2020.

[6] Breux, Sandra, and Jérémy Diaz. "La ville intelligente : origine, définitions, forces et limites d'une expression polysémique." (2017).

[7] Majeed, Umer, Latif U. Khan, Ibrar Yaqoob, SM Ahsan Kazmi, Khaled Salah, and Choong Seon Hong. "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges." *Journal of Network and Computer Applications* 181 (2021): 103007.

[8] Chinnasamy, P., Vinothini, C., Arun Kumar, S., Allwyn Sundarraj, A., Annlin Jeba, S. V., & Praveena, V. (2021). Blockchain technology in smart-cities. In *Blockchain Technology: Applications and Challenges* (pp. 179-200). Cham: Springer International Publishing.

[9] Tandon, Aditya. "Challenges of integrating blockchain with internet of things." *International Journal of Innovative Technology and Exploring Engineering* 8, no. 9s3 (2019): 1476-1489.

[10] El Majdoubi, D., El Bakkali, H., & Sadki, S. (2020, November). Towards smart blockchain-based system for privacy and security in a smart city environment. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)* (pp. 1-7). IEEE.

[11] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.

[12] Kumar, Prabhat, Randhir Kumar, Gautam Srivastava, Govind P. Gupta, Rakesh Tripathi, Thippa Reddy Gadekallu, and Neal N. Xiong. "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities." IEEE Transactions on Network Science and Engineering 8, no. 3 (2021): 2326-2341.

[13] Makhdoom, Imran, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." *Computers & Security* 88 (2020): 101653.

[14] https://steemit.com/ipfs/@admiboss/simple-decentralized-app-architecture

[15] https://www.crypto-sous.fr/quest-ce-quune-dapp-et-a-quoi-cela-sert/

[16] https://whatis.techtarget.com/fr/definition/cryptographie-asymetrique-cryptographie-acle-publique, (consulté le 22 avril 2021).

[17] D. Puthal, N. Malik, P. Saraju Mohanty, E. Kougianos, and G. Gautam

Das. Everything You Wanted to Know About the Blockchain: Its Promise,

Components, Processes, and Problems, 2018

[18] https://coinjournal.net/fr/crypto-monnaies/apprendre/blockchain/

[19] https://fr.wikipedia.org/wiki/InterPlanetary_File_System

[20] https://www.ibm.com/fr-fr/topics/blockchain-security

[21]https://www.google.com/imgres?imgurl=https%3A%2F%2Flibrecours.net%2Fmodule%2Fculture%2Fintro-chiffrement%2Fres%2Fprincipe_chiffrement.png&tbnid=x11oaQY459FP3M&vet=1&imgrefurl=https%3A%2F%2Flibrecours.net%2Fmodule%2Fculture%2Fintro-chiffrement%2Fprincipe-chiffrement.xhtml&docid=o7lmLHx58D1l0M&w=455&h=180&hl=fr-FR&source=sh%2Fx%2Fim%2Fm5%2F4&shem=uvafe1

[22] https://www.innovauto.org/systemes-embarques/la-securite-des-donnees-le-blockchain