République Tunisienne
****
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Sfax

Ecole Nationale d'ingénieur de Sfax

PROJET FIN D'ANNÉE

Mise en place et déploiement d'une plateforme Blockchain appliquée au domaine de l'e-health

---

Elaboré par :

HASSINE SOUHA

FATNASSI SONIA

JALLELI NADINE

AYEDI AMINE

Encaré par : Frikha Tarek

Periode de Projet : ..... - .....

Année Universitaire : 2023 - 2024

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Etat de l'art

1.1 Introduction

Après avoir défini les objectifs et réalisé l'analyse nécessaire pour élaborer la solution finale dans le chapitre précédent, nous nous penchons sur l'état de l'art de notre projet comme une étape préliminaire à la réalisation de l'application. En effet, cette étape nous permet de décrire les concepts et les notions de base utilisés tout au long de notre implémentation, mettant en évidence nos technologies et d'outils nécessaires pour notre travail.

1.1.1 Présentation des concepts et des notions théoriques utilisés

A- Hypothèse de solution :

Dans le domaine des applications de santé, la technologie Blockchain offre une solution convaincante pour relever des défis critiques, dont certains sont suggérés dans la figure 2.1. Sa nature décentralisée et immuable fournit un cadre sécurisé pour protéger les données sensibles et atténuer les vulnérabilités de sécurité répandues dans les systèmes de santé.

FIGURE 1.1 – Exemples de domaines d'application de la blockchain

Cettte technologie innovante est extrêmement prometeuse pour révolutionner les opérations de santé , établir un écosystème plus sûr, comme dans notre cadre Hyperledger Aries joue un rôle vital dans l'intégration des technologies de la blockchain, offrant une architecture robuste pour la gestion des identités décentralisées et la communication sécurisée entre les participants.

B- Introduction à la technologie Blockchain :

La blockchain a été initialement introduite comme composant fondamental du bitcoin, une solution de cryptomonnaie décrite dans le livre blanc de Satoshi Nakamoto de 2009. Cette technologie vise à établir un consensus de confiance dans des scénarios où plusieurs rédacteurs, souvent inconnus et peu fiables, doivent stocker un état (transaction). Il est largement reconnu et acclamé comme une technologie disruptive qui exploite la vérifiabilité publique pour garantir l'immuabilité et la sécurité cryptographique des transactions effectuées par les utilisateurs en ligne, fournissant ainsi une piste vérifiable. Bien que Bitcoin soit l'application la plus connue de la Blockchain, elle peut être appliquée à diverses applications bien au-delà des crypto-monnaies. Puisqu'elle permet d'effectuer des paiements sans aucune banque ni intermédiaire,la Blockchain peut être utilisée dans divers services financiers, tels que les actifs numériques, les envois de fonds et le paiement en ligne.

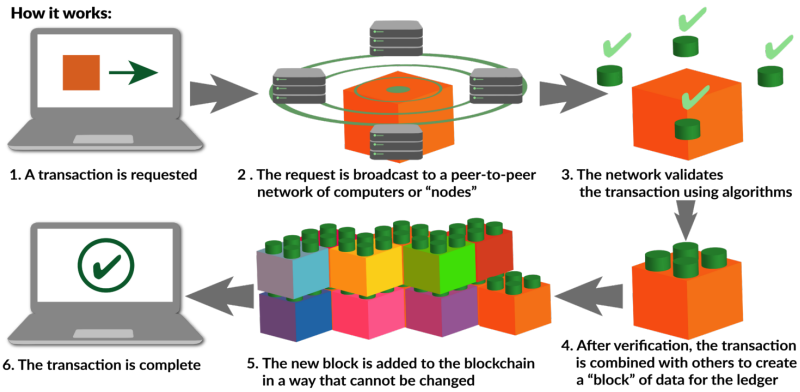

FIGURE 1.2 – Architecture de la chaîne de blocs

La blockchain elle-même a pris son envol et s'est infiltrée dans un large éventail d'applications dans de nombreux secteurs, notamment la finance, la santé, le gouvernement, l'industrie manufacturière et la distribution. La blockchain est sur le point d'innover et de transformer

diverses applications, telles que le suivi des marchandises (chaîne d'approvisionnement), la distribution de médias numériques (vente d'art), la prestation de services à distance (voyages et tourisme), ainsi que les plateformes de données et d'accréditation distribuées. Cette transformation est rendue possible grâce à sa structure de fonctionnement et à son architecture uniques, comme l'explique la figure 2.2. Les applications supplémentaires de la blockchain comprennent les ressources distribuées (production et distribution d'électricité), le financement participatif, le vote électronique, la gestion de l'identité et la gestion des archives publiques.

C- Evolution de Blockchain :

La blockchain a évolué de manière significative depuis son introduction où elle est associée à Bitcoin pour les transactions financières décentralisées, elle s'est transformée en une plateforme polyvalente utilisée dans divers secteurs.

Cette évolution a donné naissance à des plateformes comme Ethereum, pionnière dans les contrats intelligents, ouvrant ainsi la voie à de nombreuses applications décentralisées. Parallèlement, des projets comme Hyperledger Aries de la Fondation Linux se sont concentrés sur la gestion sécurisée des identités décentralisées, renforçant ainsi la confiance et la confidentialité des échanges d'informations sur la blockchain.

En somme, la blockchain a évolué pour répondre à divers besoins, intégrant des fonctionnalités avancées telles que l'évolutivité et la programmabilité. De plus, elle s'associe désormais à d'autres technologies émergentes telles que l'intelligence artificielle et l'Internet des objets, ouvrant ainsi de nouvelles perspectives d'applications et de collaborations dans différents domaines.

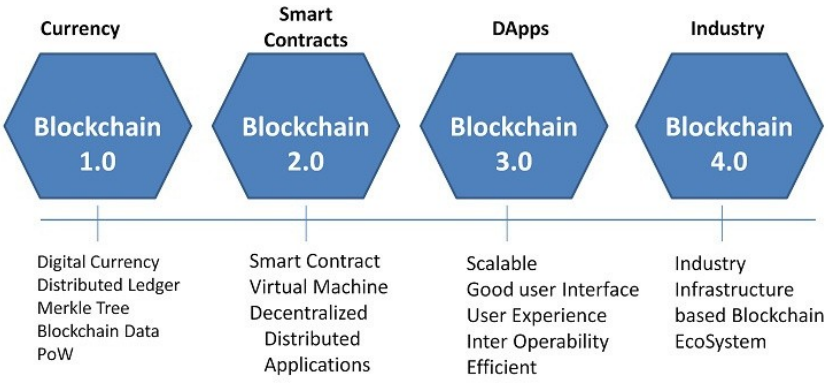

FIGURE 1.3 – Evolution de l'historique de blockchain

D- Mécanisme technologique de Blockchain :

La blockchain n'est pas un avènement unique, c'est une combinaison de trois technologies. Ils comprennent : Des clés cryptographiques, Un réseau peer-to-peer et Un registre numérique.

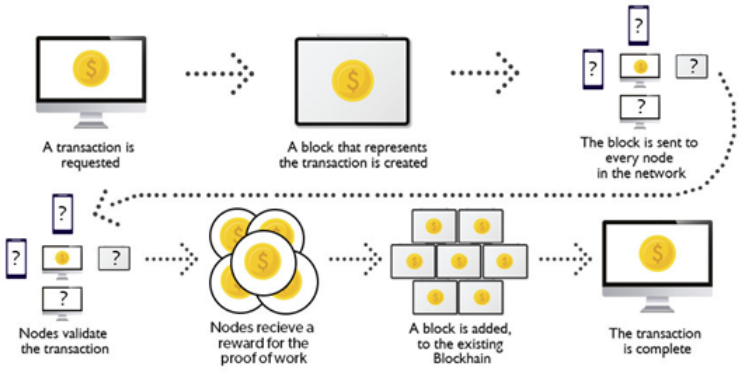

FIGURE 1.4 – Mécanisme de la blockchain

- Clés cryptographiques : sont une combinaison de clés privées et publiques utilisées pour créer une identité numérique unique et sécurisée pour chaque transaction. La clé privée est utilisée pour créer la signature, tandis que la clé publique est utilisée pour la vérifier.Ce processus repose sur la cryptographie à clé publique et est largement utilisé pour l'authentification et la sécurité des transactions, notamment dans des secteurs tels que la finance,la santé et les services juridiques. Les signatures numériques sont également utilisées pour identifier le signataire d'un document et garantir son intégrité, empêchant ainsi les modifications non autorisées

- Un réseau peer-to-peer : fait référence à un grand groupe d'individus agissant en tant qu'autorités et parvenant à un consensus sur des transactions. Alors que les clés cryptographiques créent une signature numérique, le réseau peer-to-peer autorise la transaction en utilisant une vérification mathématique dans le réseau peer-to-peer.
- Un registre numérique : est une structure qui héberge toutes les transactions. Il fonctionne comme une feuille de calcul contenant chaque nœud d'un réseau et enregistrant chaque achat effectué par ce nœud. La signature numérique protège les informations du grand livre numérique contre la falsification et garantit leur sécurité exceptionnelle. Une caractéristique intrigante de ce grand livre est que, bien que tout le monde puisse consulter les données, elles ne peuvent pas être modifiées d'une autre manière

E- Caractéristiques des systèmes Blockchain :

De manière générale et comme présenté dans la figure 1.5, la Blockchain présente les caractéristiques clés suivantes :

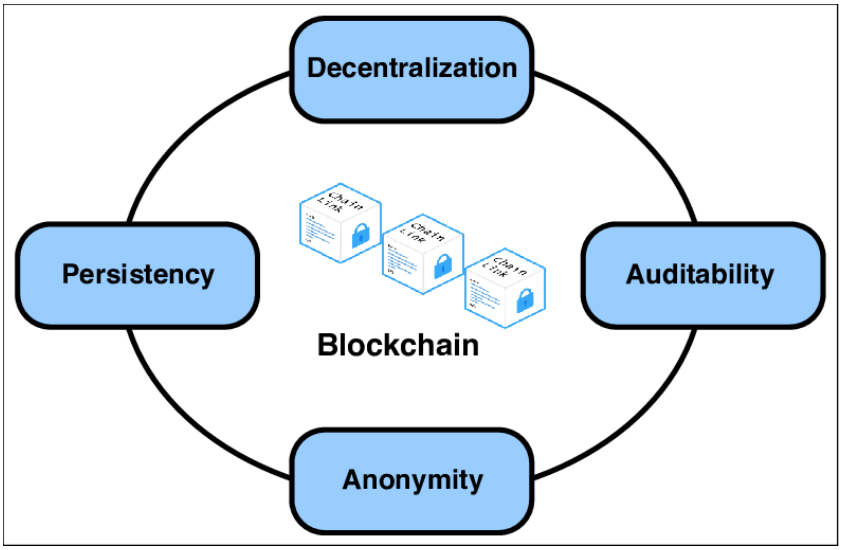

FIGURE 1.5 – Caractéristiques de la blockchain

• Décentralisation : Dans les systèmes de transactions centralisés conventionnels, chaque transaction doit être validée par l'agence centrale de confiance (par exemple, la banque centrale), ce qui entraîne inévitablement des goulots d'étranglement en termes de coûts et de performances

au niveau des serveurs centraux. D'une manière différente, une transaction dans le réseau Blockchain peut être effectuée entre deux pairs (P2P) sans authentification par l'agence centrale. De cette manière, Blockchain peut réduire considérablement les coûts du serveur (y compris les coûts de développement et les coûts d'exploitation) et atténuer les goulots d'étranglement des performances du serveur central.

• Persistance : Étant donné que chacune des transactions réparties sur le réseau doit être confirmée et enregistrée dans des blocs répartis sur l'ensemble du réseau, il est presque impossible de la falsifier.

• Un registre numérique : est une structure qui héberge toutes ces transactions. En clair, le grand livre numérique fonctionne comme une feuille de calcul qui contient chaque nœud d'un réseau et enregistre chaque achat effectué par ce nœud. La signature numérique protège les informations du grand livre numérique contre la falsification et garantit qu'elles sont exceptionnellement sécurisées. La caractéristique la plus intrigante de ce grand livre est que même si tout le monde peut consulter les données, elles ne peuvent pas être modifiées.De plus, chaque bloc diffusé serait validé par d'autres nœuds et les transactions seraient vérifiées. Ainsi, toute falsification pourrait être facilement détectée.

• Anonymat : Chaque utilisateur peut interagir avec le réseau Blockchain avec une adresse générée. De plus, un utilisateur pourrait générer de nombreuses adresses pour éviter de révéler son identité. Il n'existe plus de partie centrale qui conserve les informations privées des utilisateurs. Ce mécanisme préserve une certaine confidentialité sur les transactions incluses dans la Blockchain. Notez que la Blockchain ne peut garantir la parfaite préservation de la vie privée en raison de la contrainte intrinsèque.

• Auditabilité : Étant donné que chacune des transactions sur la Blockchain est validée et enregistrée avec un horodatage,les utilisateurs peuvent facilement vérifier et retracer les enregistrements précédents en accédant à n'importe quel nœud du réseau distribué.Dans Bitcoin Blockchain, chaque transaction peut être retracée de manière itérative aux transactions

précédentes. Il améliore la traçabilité et la transparence des données stockées dans la Blockchain.

E- Classification des systèmes Blockchain :

Il existe trois types de Blockchain : publique, privée (autorisée) et consortium (fédérée).Pour cela dans notre projet nous avons choisi d'utiliser une blockchaine privée ou autorisée. Cette décision découle de notre besoin d'assurer le contrôler strictement l'accès aux données médicales sensibles et de maintenir une certaine confidentialité. Ainsi elle permet un groupe sélectionné d'entités ou d'organisations de gérer le réseau, ce qui peut être bénéfique pour assurer la conformité aux réglementations en matière de confidentialité des données.Alors nous avons mentionné ces types qui sont présentés et brièvement expliqués dans le tableau ci-dessous :

Blockchain publique	Un réseau Blockchain public ou sans autorisation est un réseau auquel tout le monde peut participer sans restrictions. La plupart des types de crypto-monnaies fonctionnent sur une blockchain publique régie par des règles ou des algorithmes de consensus.
Blockchain autorisée ou privée	Une Blockchain privée ou autorisée permet aux organisations de définir des contrôles sur les personnes pouvant accéder aux données de la Blockchain. Seuls les utilisateurs disposant d'autorisations peuvent accéder à des ensembles de données spécifiques.
Blockchain fédérée ou consortium	Un réseau blockchain où le processus de consensus (processus de minage) est étroitement contrôlé par un ensemble présélectionné de nœuds ou par un nombre présélectionné de parties prenantes.

TABLE 1.1 – Types de Blockchain

Ces systèmes peuvent être comparés en utilisant différentes perspectives comme décrit ci-dessous :

• Détermination par consensus : Ce mécanisme préserve une certaine confidentialité sur les transactions incluses dans la Blockchain. Notez que la Blockchain ne peut garantir la parfaite préservation de la vie privée en raison de la contrainte intrinsèque.

• Auditabilité : Tous les nœuds peuvent participer au processus de consensus dans la Blo-

ckchain publique, telle que Bitcoin,tandis que seuls quelques ensembles sélectionnés de nœuds sont responsables de la confirmation d'un bloc dans la Blockchain du consortium. Dans la Blockchain privée, une autorité centrale décidera des délégués qui pourront déterminer le bloc validé. Étant donné que chacune des transactions sur la Blockchain est validée et enregistrée avec un horodatage, les utilisateurs peuvent facilement vérifier et retracer les enregistrements précédents en accédant à n'importe quel nœud du réseau distribué.

• Autorisation de lecture : La blockchain publique accorde une autorisation de lecture aux utilisateurs, le secteur privé et le consortium pouvant restreindre l'accès au grand livre distribué. Par conséquent, l'organisation ou le consortium peut décider si les informations stockées doivent rester publiques pour tous ou pas.

• Autorisation de lecture : La blockchain publique accorde une autorisation de lecture aux utilisateurs, le secteur privé et le consortium pouvant restreindre l'accès au grand livre distribué. Par conséquent, l'organisation ou le consortium peut décider si les informations stockées doivent rester publiques pour tous ou pas.

• Immuabilité : Dans le réseau Blockchain décentralisé, les transactions sont stockées dans un grand livre distribué et validées par tous les pairs, ce qui rend presque impossible toute modification dans la Blockchain publique. En revanche, le consortium et le registre privé de la Blockchain peuvent être altérés par le désir de l'autorité dominante.

• Efficacité : Dans la Blockchain publique, n'importe quel nœud peut rejoindre ou quitter le réseau, ce qui le rend hautement évolutif. Cependant, avec la complexité croissante du processus d'exploration de données et l'accès flexible des nouveaux nœuds au réseau, cela entraîne un débit limité et une latence plus élevée.Cependant, avec moins de validateurs et de protocoles de consensus électifs, les blockchains privées et de consortium peuvent faciliter de meilleures performances et une meilleure efficacité énergétique.

• Centralisé : La différence significative entre ces trois types de blockchain est que ce der-

nier publique est décentralisée, tandis que le consortium est partiellement centralisé et que la Blockchain privée est contrôlée par une autorité centralisée.
La Blockchain publique étant ouverte sur le monde, elle peut attirer de nombreux utilisateurs. Les communautés sont également très actives. De nombreuses Blockchains publiques émergent chaque jour.

• Le consortium :la blockchain, elle, pourrait être appliquée à de nombreuses applications métiers. Actuellement, Hyperledger développe des frameworks Blockchain de consortium d'entreprises. Ethereum a également fourni des outils pour créer des blockchains de consortium. Pour la Blockchain privée, de nombreuses entreprises la mettent encore en œuvre pour des raisons d'efficacité et d'auditabilité.

1- Chaîne de blocs Ethereum :

Ethereum a commencé comme un moyen de créer une blockchain à usage général qui pourrait être programmée pour diverses utilisations. Mais très rapidement, la vision d'Ethereum s'est élargie pour devenir une plate-forme de programmation de dApps.

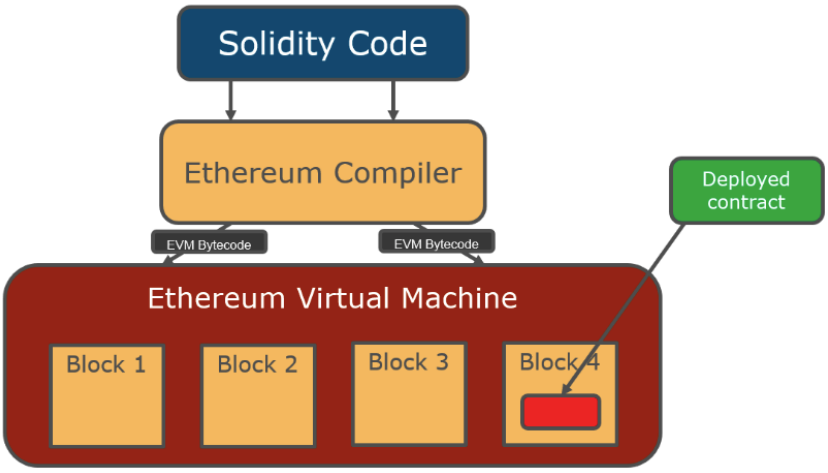

FIGURE 1.6 – Architecture d'Ethereum

Les dApps représentent une perspective plus large que les contrats intelligents. Une dApp est, à tout le moins, un contrat intelligent et une interface utilisateur Web. Plus largement, une dApp est une application Web construite sur des services d'infrastructure ouverts, décentralisés et peer-to-peer. Une dApp est composée d'au moins :

- Contrats intelligents sur une Blockchain.
- Une interface utilisateur Web frontale.

De plus, de nombreuses dApp incluent d'autres composants décentralisés, tels que :

- Un protocole et une plateforme de stockage décentralisés (P2P)
- Un protocole et une plateforme de messagerie décentralisée (P2P)

2- Contrats intelligents :

L'essor de la technologie Blockchain ces dernières années soutient également d'autres concepts suggérés dans la littérature. Le concept de « **Smart Contract** » ou bien contrat intelligent est un contrat auto-exécutable dont les termes de l'accord sont directement écrits dans des lignes de code. Ces contrats sont mis en œuvre sur des plateformes Blockchain, généralement à l'aide de langages de programmation de contrats intelligents. Les smart contracts permettent d'automatiser l'exécution d'un contrat en utilisant des protocoles informatiques et des interfaces utilisateur. Grâce à la Blockchain, les contrats intelligents sont de plus en plus populaires car ils peuvent être utilisés plus facilement en appliquant des Blockchains par rapport à la technologie disponible au moment de leur invention il y a 20 ans. Cette approche innovante pourrait remplacer les avocats et les banques qui ont été impliqués dans des contrats de transactions d'actifs en fonction d'aspects prédéfinis parmi les langages de programmation de contrats intelligents nous :

• Solidité (pour Ethereum) : Solidity est le langage de programmation le plus utilisé pour créer des contrats intelligents sur la plateforme Ethereum. Il s'agit d'un langage à typage statique, orienté contrat, présentant des similitudes avec JavaScript et C++. Solidity prend en charge des fonctionnalités telles que l'héritage, les bibliothèques et les types complexes définis par l'utilisateur.

• Vyper : Vyper est un autre langage développé pour les contrats intelligents Ethereum. Il se concentre sur la sécurité et la simplicité, dans le but de minimiser les vulnérabilités potentielles en limitant les constructions de programmation complexes et en favorisant la lisibilité et la facilité d'audit.

• Code de chaîne (Go) : Les codes de chaîne, également connus sous le nom de contrats intelligents, sur la plateforme Hyperledger Fabric sont généralement écrits en Go (Golang). Go est un langage typé statiquement connu pour son efficacité et sa simplicité. Les contrats intelligents Chaincode dans Go sont exécutés dans des conteneurs sur le réseau Fabric.
• Cadence : Cadence est un langage de programmation orienté ressources développé pour les contrats intelligents sur la Flow Blockchain. Flow est conçu pour les applications décentralisées et les actifs numériques. Cadence fournit des fonctionnalités telles que la gestion des ressources, le contrôle d'accès et des types de ressources flexibles.

• Michelson : Michelson est un langage pour les contrats intelligents sur la blockchain Tezos. Il s'agit d'un langage de bas niveau basé sur une pile qui se concentre sur la vérification formelle et la sécurité. La conception de Michelson facilite l'exécution sécurisée de contrats intelligents et permet l'analyse du code pour identifier les problèmes potentiels.

• Plutus : Plutus est le langage de programmation pour les contrats intelligents sur la Blockchain Cardano. C'est un langage de programmation fonctionnel basé sur Haskell. Plutus permet aux développeurs de rédiger des contrats intelligents avec des capacités de vérification formelle intégrées. Les contrats intelligents exécutent automatiquement les conditions prédéfinies et les actions qu' y sont spécifiées une fois que les événements ou conditions déclencheurs sont remplis. Ils fonctionnent sur un réseau décentralisé d'ordinateurs (nœuds) et sont transparents, inviolables et irréversibles une fois déployés sur la Blockchain.

a) Les principales caractéristiques des contrats intelligents :

Parmi les avantages que les smarts contracts possédent :

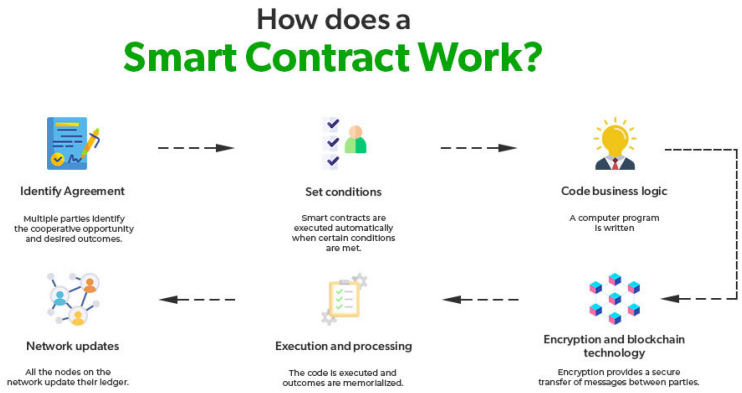

FIGURE 1.7 – Mécanisme de contrat intelligent

- Autonomie : Les contrats intelligents éliminent le besoin d'intermédiaires, tels que des avocats ou des courtiers, car ils appliquent automatiquement les termes de l'accord sans faire appel à des tiers.
- Transparence : Le code et l'exécution d'un contrat intelligent sont enregistrés sur la Blockchain, la rendant transparente et visible pour tous les participants du réseau.
- Sécurité : Les contrats intelligents sont construits sur la Blockchain, qui fournit des fonctionnalités de sécurité inhérentes telles que l'immuabilité, des algorithmes cryptographiques et des mécanismes de consensus qui garantissent l'intégrité et la sécurité du contrat.
- Efficacité : En automatisant l'exécution des contrats, les contrats intelligents réduisent le besoin de processus manuels, de paperasse et de rapprochement, conduisant à des transactions plus rapides et plus efficaces. D'autre part il y a aussi des inconvénients liés à l'utilisation des contrats intelligents sont les suivants :
- La possibilité de failles, une réalité inhérente à tout programme informatique. Plus les contrats intelligents sont complexes, plus le risque de vulnérabilités augmente. L'absence totale de régulation, ce qui soulève des questions tant sur le plan moral que juridique. Cette carence en encadrement légal peut engendrer des dilemmes éthiques et des litiges juridiques.

1.1.2 Utilisation de Blockchain dans les soins de santé :

L'intégration de la blockchain dans notre travail concernant le domaine de la santé électronique représente une avancée révolutionnaire et indispensable. Notre projet embrasse cette

technologie novatrice afin de sécuriser et rendre transparents les échanges de données médicales sensibles.En intégrant la blockchain dans notre système, notre objectif est de garantir la confidentialité, la sécurité et l'intégrité des informations cruciales pour la prise en charge médicale. Cette utilisation de la blockchain crée une infrastructure décentralisée dans notre environnement e-health, éliminant ainsi le besoin d'intermédiaires et assurant une traçabilité transparente des données médicales, renforçant ainsi la confiance des patients dans la qualité des services de santé.

De plus, ce domaine decentralisé facilite la mise en œuvre de contrats intelligents qui automatisent les processus de gestion des données médicales, réduisant les risques d'erreurs humaines et améliorant l'efficacité opérationnelle dans la prestation des soins de santé. En alignant les principes de sécurité et de décentralisation de la blockchain avec les exigences de confidentialité et de transparence de l'e-health moderne, notre projet ouvre de nouvelles perspectives pour une gestion des données médicales efficace et éthique, contribuant ainsi à des pratiques de soins de santé intelligentes et responsables.

1.2 Conclusion

Ce chapitre a donné l'occasion de présenter les concepts et les notions utilisé et indispensables pour notre étude théorique qui concerne les démarches de développement et de conception de notre solution que nous présenterons dans le chapitre qui suit.

Conclusion Générale

En résumé, notre projet dans le domaine de la santé, intégrant la technologie blockchain, s'est concentré sur la conception et le déploiement d'une plateforme dédiée à la sécurisation des données médicales. Nous avons examiné de près les méthodes d'intégration de cette technologie émergente afin d'améliorer la confidentialité, la sécurité et l'accessibilité des dossiers médicaux.

Cette plateforme offre de nombreux avantages pour les professionnels de la santé et les patients. Elle leur permet de gérer, partager et stocker les données médicales de manière sécurisée et transparente, facilitant ainsi la coordination des soins et la prise de décision éclairée. Pour les patients, elle garantit une confidentialité accrue et une implication dans leur processus de soins.L'intégration de la technologie blockchain renforce la confiance et la transparence dans la gestion des données médicales, assurant ainsi la précision et la fiabilité des informations essentielles.

Notre projet nous a permis d'explorer en profondeur les nombreuses possibilités offertes par la technologie blockchain dans le domaine de la santé. Nous avons développé des solutions e-health innovantes, répondant ainsi aux besoins évolutifs de ce secteur en constante mutation.

Malgré les défis rencontrés tout au long du processus de développement, de conception et de mise en œuvre, nous avons réussi à atteindre nos objectifs. Ce projet nous a offert l'occasion de mettre en pratique les concepts théoriques appris et d'appliquer nos connaissances dans un contexte concret. De plus, la réalisation de cette plateforme nous a permis d'acquérir de nouvelles compétences et de maîtriser divers outils.

Nos prochaines étapes de notre projet s'inscrivent dans la lignée de nos efforts actuels, mettant un accent particulier sur l'optimisation des fonctionnalités déjà en place. Ainsi la sécurité des données demeure une préoccupation majeure pour éviter toute vulnérabilité potentielle.

Bibliographie