MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHESCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et d'Informatique

Département de Mathématiques et informatique

Filière : Informatique

MEMOIRE DE FIN D'ÉTUDES

Pour l'Obtention du Diplôme de Master en Informatique

Option : **Ingénierie des Systèmes d'Information**

Présenté par :

MOSTEFAI Elhadja Hasnia & Zaoui Nour Elhouda

THEME :

La blockchain et ses applications dans le domaine de la santé

Devant le jury composé de :

BENHAMED Siham	MAA	Université de Mostaganem	Président
BENTAOUZA Chahinez Meriem	MCB	Université de Mostaganem	Examinateur
MIROUD Mohammed El Mustapha	MAA	Université de Mostaganem	Encadrant

Année Universitaire 2020-2021

Résumé

Dans ce projet de fin d'études, nous avons étudié la blockchain "bitcoin", les contrats intelligents et la plateforme Ethereum. Nous avons résolu le problème de partage d'informations dans le domaine médical électronique (E-santé), qui nécessite sécurité, confiance et transparence des données. Nous avons fourni une solution blockchain basée sur des contrats intelligents pour assurer la sécurité du partage des informations des patients entre les différents acteurs de l'industrie médicale. Nous avons développé trois contrats intelligents sur la plate-forme Ethereum avec une interface Web. Nous avons également évoqué les avantages de la blockchain ainsi que des contrats intelligents en termes de sécurité, deconfiance et de transparence.

Mots-clés

Blockchain, Cryptographie, Bitcoin, Transaction, Décentralisation, Réseau, Données, E-Santé, Contrats intelligents, Ethereum, Dapps, Solidity, Cryptomonnaies.

Abstract

In this document, we studied the bitcoin blockchain and how it accomplishes decentralization. In other words, how it removes central trust authority from a system. Then we studied Bitcoin transaction mechanics, and introduced smart contracts, which are a fundamental concept in blockchain use cases. Afterward, we studied blockchain application in healthcare system on the scientific literature, and how this technology is used for improving healthcare systems. Finally, we developed three smart contracts on the ethereum platform to handle data access right in a health database.

Keywords

Blockchain, Cryptography, Bitcoin, Transaction, Decentralization, Network, Data, E-Health, Smart contracts, Ethereum, Dapps, Solidity, data access rights, cryptocurrencies.

Dédicaces

Ce projet de fin d'étude est dédié à nos chers parents, qui nous ont toujours poussé et motivé dans nos études. Ce projet fin d'étude représente donc l'aboutissement du soutien et des encouragements qu'ils nous ont prodigués tout au long de notre scolarité. Qu'ils en soient remerciés par cette trop modeste dédicace.

C'est un moment de plaisir de dédier cet œuvre, à nos chers et adorable frères et sœur en signe d'amour, nous vous souhaitons une vie pleine de bonheur et de succès et que Dieu, le tout puissant, vous protège et vous garde.

A tous nos amis qui nous ont toujours encouragés, et à qui on souhaite plus de succès.

Finalement, à toutes les personnes qui ont participé à l'élaboration de ce travail.

Remerciements

Nous remercions d'abord ALLAH le tout puissant qui nous guidé et nous a donné la force et la volonté de réalisé ce mémoire.

En premier lieu, nous remercions notre encadrant Mr MIROUD Mohammed El Mustapha de nous avoir orientés avec ces précieux conseils et remarques.

Nos pensées vont vers nos parents, qui ont toujours cru en nous. C'est grâce à leur soutient et prières que nous avons accomplies ce travail, ils savent déjà combien nous leur devons.

A nos amis, qui ont contribué dans notre travail par leurs encouragements, merci !

Nos remerciements les plus sincères à toutes les personnes qui auront contribué de près ou de loin à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Enfin, nous tenons aussi à remercier les jurés pour avoir accepté d'examiner et de juger notre travail.

Liste des figures

Liste des tableaux

Liste des abréviations

Abréviation	Expression Complète	Page
E-Santé	Santé électronique.	5
DSE	Dossier de santé électronique.	22
PHR	Personal health record ou dossier personnel de santé.	23
FHIR	Healthcare Interoperability Resources.	23
IoT	Internet of Things ou Internet des objets	23
PoW	Proof of Work ou Preuve de travail.	26
PBTF	Practical Byzantine Fault Tolerance.	26
DME	Dossier médical électronique.	32
ABAC	Attribute-based access control.	32
UI	Interface utilisateur.	36
ETH	Ether.	46
EVM	Machine virtuelle Ethereum.	47
NPM	Node Package Manager.	49

Table des matières

Introduction Générale

Le concept de blockchain a pour la première fois été utilisé en 2008. Le mot blockchain est resté pendant des années l'apanage de petits groupes, très restreints, d'informaticiens et de mathématiciens, dont l'objectif était de développer des outils pour garantir le respect de la vie privée sur internet. Il faudra une petite dizaine d'années pour que ce concept arrive aux oreilles du grand public, notamment grâce à la médiatisation du Bitcoin [1] qui est à l'origine de cette technologie.

La technologie blockchain est une nouvelle façon de concevoir le stockage d'information, en abolissant la nécessité d'un tiers de confiance. En alliant plusieurstechniques, la blockchain permet à plusieurs entités non seulement de partager des données mais aussi de les modifier de manière collaborative, et surtout sécurisée. Elle permet également de créer de la confiance entre les différents utilisateurs de cette donnée.

La blockchain étant un nouveau moyen de stocker et gérer des données, cela en fait une technologie qui peut potentiellement devenir très répandue dans nos sociétés informatisées. C'est pourquoi, après avoir émergé avec les monnaies digitales, elle peut impacter et transformer potentiellement de nombreux secteurs d'activité. Bien sûr, les bénéfices que l'on peut en tirer sont variables selon le domaine auquel elle est appliquée. Cependant, il est à peu près certain que la finance, les assurances, l'immobilier, la logistique, et bien sûr la santé, sont des secteurs d'activité qui seront amenés à se transformer grâce à la technologie blockchain.

Quand une unique organisation veut contrôler l'accès à ses ressources, elle met en place un système d'authentification et d'autorisation centralisé. Lorsque plusieurs organisations veulent partager entre elles des ressources, le problème de la gestion de l'ensemble des identités et des règles de contrôle d'accès partagées se pose. Traditionnellement, ce problème est traité en confiant cette gestion à un seul acteur (interne ou externe) de sécurité ou en utilisant des mécanismes de fédération d'identité. Cependant, ces mécanismes nécessitent la mise en œuvre de relations de confiance souvent difficiles voire impossibles entre ces organisations. Une autre façon de résoudre ce problème est d'utiliser la Blockchain elle-même pour gérer les identités et les règles de contrôle d'accès aux ressources.

Un contrôle d'accès basé sur la blockchain permet d'établir la confiance entre des organisations différentes et de partager de l'information tout en conservant le contrôle de cette information sans pour autant recourir à un unique acteur de sécurité. L'information partagée peut alors être les attributs d'identité pour les utilisateurs et les règles d'accès pour gérer les autorisations sur les ressources.

Nous avons, au cours de ce travail de fin d'études de master en informatique, fourni une solution blockchain basée sur des contrats intelligents pour assurer la sécurité du partage des informations des patients entre les différents acteurs de l'industrie médicale. Nous avons développé trois contrats intelligents sur la plate-forme Ethereum avec une interface Web. Nous avons également évoqué les avantages de la blockchain ainsi que des contrats intelligents en termes de sécurité, de confiance et de transparence. Ce document est divisé en quatre chapitres :

Au cours du premier chapitre, nous allons aborder les notions de cryptomonnaies pour en comprendre le principe de fonctionnement, Ceci nous permettra également d'illustrer les problèmes de double dépense ainsi que la dépendance d'un système à une autorité centrale. Nous introduisons par la suite comment la blockchain Bitcoin a réussi à supprimer cette autorité de confiance, tout en garantissant que le système reste fonctionnel.

Lors du second chapitre, nous allons étudier l'état de la recherche en matière de blockchain utilisée pour la E-santé ainsi que du control d'accès aux données médicales.Par la suite, nous allons exposer les possibles applications et enjeux d'une telle technologie, et les possibles innovations qu'elle pourrait apporter au monde de la santé.

Dans le troisième chapitre nous allons aborder les Dapps (applications décentralisées) ainsi que leurs caractéristiques et présenter la problématique traitée dans notre travail. Enfin nous allons exposer la conception et la modélisation de notre application.

Enfin, lors du quatrième chapitre, nous allons présenter l'application de gestion de contrôle d'accès que nous avons développé, ainsi que ces différentes interfaces graphique.

Chapitre 1

Introduction à Bitcoin

1.1 Introduction

Bitcoin est une cryptomonnaie. Ce n'est pas la première cryptomonnaie à avoirété conçue, cependant c'est la première à avoir vraiment pris son essor. La principale raison pour que toutes les cryptomonnaies avant bitcoin aient échouées, est le fait qu'elles se reposaient en général sur une autorité centrale pour être gérées. Cette autorité centrale veillait principalement à ce que les règles du système ne soient pas enfreintes. Notamment, elle évitait la double dépense, qui constitue le danger principal dans ce genre de système.

La principale innovation du concepteur de bitcoin est qu'il ait réussi à supprimer cette autorité centrale, tout en concevant un système opérationnel, qui fonctionne. Au cours de ce chapitre, nous allons présenter comment cette innovation a été mise en œuvre.

En premier lieu, nous donnerons deux exemples simples de cryptomonnaies, afin que le lecteur puisse comprendre leur concept et mieux comprendre les menaces qui pèsent sur ce genre de système, ainsi que le pouvoir dont jouit une autorité centrale enleur sein. Ceci nous amènera à bitcoin est à comment Satoshi Nakamoto (le concepteur deBitcoin), a réussi à concevoir un système décentralisé, fonctionnel, se reposant sur la cryptographie ainsi que sur une politique incitative.

1.2 Exemples de Crypto-monnaie

1.2.1 GoofyCoin

Bitcoin est une cryptomonnaie, afin de comprendre le concept derrière cette appellation, nous allons présenter un exemple de cryptomonnaie qui suit à peu près le principe de fonctionnement de bitcoin, mais qui souffre néanmoins d'un défaut majeur. Les deux exemples de cryptomonnaies qui vont suivre sont expliqués beaucoup plus en détails dans la référence [2]. Cette cryptomonnaie se nomme Goofycoin et elle constitue la cryptomonnaie la plus simple que l'on puisse imaginer. Elle ne possède que deux règles très simples :

1ère règle dans Goofycoin: Une entité centrale désignée sous le nom de Goofy, peut créer de nouveaux coins (peut émettre de la monnaie) à chaque fois qu'elle le désire,et cette monnaie nouvellement créée lui appartiendra.

Pour créer de la monnaie, Goofy génère un identifiant de jeton unique (**uniqueCoinID),** qu'il n'a jamais généré auparavant et construit un string **CreatCoin [UniquecoinID]**.

Ensuite, Goofy calcule la signature électronique de ce string à l'aide de sa clé privée.

Le String + la signature électronique de Goofy = une pièce (un coin, un jeton).

Tout le monde peut vérifier que le jeton contient bien la signature de Goofy et que c'est bien un jeton valide (un jeton qui a bien été créé par Goofy)[2].
La figure 1 ci-dessous illustre cette première règle.

Figure 1 - Règle 1 de Goofycoin : Goofy peut créer des coins[2].

2ème règle : Toute personne possédant un coin, **peut transférer** la propriété de cecoin à quelqu'un d'autre. Mais ce transfert ne consiste pas seulement à transférer cette structure de données au bénéficiaire (au destinataire). Ce transfert s'effectue en utilisant des opérations cryptographiques.

Supposons que Goofy veuille transférer un coin à Alice :

Pour se faire, il va créer un nouveau communiqué (une déclaration) qui stipule : « **versez ceci à Alice »** où **« ceci » est un pointeur de hachage vers le coin en question**.

Nous allons supposer que les identités dans le système sont représentées par les clés publiques des utilisateurs. Par conséquent, **Alice sera représentée par sa clé publique dans le système**. Enfin, Goofy signe le string correspondant à la déclaration.

Étant donné que c'est lui le propriétaire original du jeton, il doit signer n'importe quelle transaction qui va dépenser ce jeton. Une fois cette structure de donnée représentant la déclaration de Goofy signée, Alice devient la nouvelle détentrice du jeton. Elle peut le prouver à tout le monde puisqu'elle peut leur montrer la structure de données (**la déclaration de Goofy lui donnant le coin + une signature valide de Goofy pour cette déclaration**). En plus, **cette transaction pointe vers un coin valide qui a vraimentappartenu à Goofy**. Par conséquent, la validité et la propriété des jetons sont évidentes dans le système.

Une fois qu'Alice entre en possession du jeton, elle pourra le dépenser à son tour. Pour se faire, elle va faire la déclaration suivante : **"Payez ce jeton à la clé publique de Bob"** où **« ceci » est un pointeur (pointeur de hachage) vers le jeton qui lui appartient.** Alice devra bien sûr signer cette déclaration. Toute personne à qui l'on va présenter ce jeton pourra vérifier que Bob est vraiment son propriétaire. Elle pourra suivrela chaîne de pointeur de hachage jusqu'à la création du jeton. Elle pourra également vérifier qu'à chaque étape, le vrai propriétaire du jeton a vraiment signé la déclaration quia transmis le jeton à la personne suivante.

La figure 2 ci-dessous illustre la deuxième règle de Goofycoin.

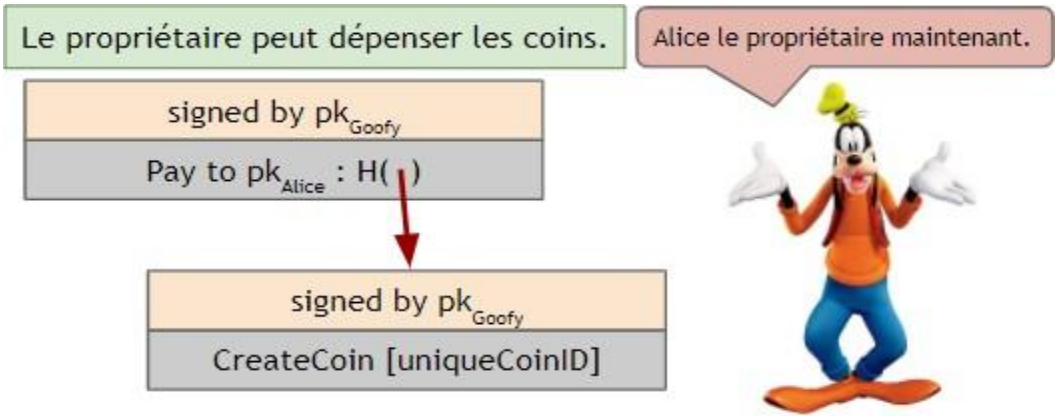

Figure 2 - Règle 2: transmission de jetons dans de GoofyCoin [2].

Donc, pour résumer ce que l'on vient de dire dans les paragraphes précédents à propos de cette cryptomonnaie :

- Goofy peut créer de nouvelles pièces avec une simple déclaration ;
- Chaque nouveau jeton possède une identité unique ;
- Celui qui possède un jeton, peut la transmettre à quelqu'un d'autre en signant une déclaration de transmission de propriété ;
- Il est possible de vérifier la validité d'un jeton, en suivant simplement la chaîne de pointeurs de hachage, et en vérifiant toutes les signatures en cours de route, jusqu'à remonter à la première transaction dans laquelle Goofy a créé ce jeton.

La figure 3 ci-dessous illustre les quatre points que nous venons de résumer.

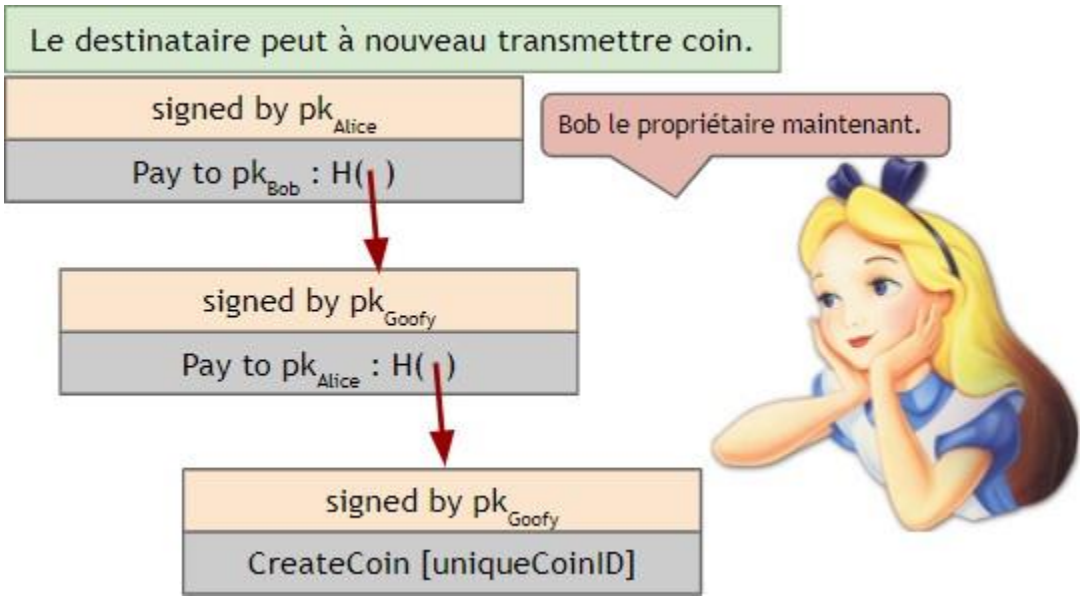

Figure 3 - GoofyCoin [2].

1.2.2 Problème de double dépense

Cependant, il y a un problème de sécurité fondamental avec **Goofycoin**. Supposons que Bob transmette un jeton à Alice en signant sa déclaration mais en omettantde le dire aux autres utilisateurs du système. Il pourra alors effectuer une autre déclaration, dans laquelle il va payer le même jeton à Anna. En apparence, il va sembler à Anna que ceci est une transaction parfaitement valide. Alice et Anna auront toutes lesdeux des prétentions valides sur ce jeton, parce qu'elles peuvent toutes les deux fournir une chaîne de transactions valides entre la transaction que Bob leur a faite et celle dans laquelle Goofy a créé le jeton dépensé. Ceci est appelé **DOUBLE-SPENDING ATTACK (attaque par double dépense)**. Bob est en train de dépenser la même pièce deux fois, et nous savons qu'une monnaie n'est pas censée fonctionner de la sorte (voir la figure 4). Ce genre d'attaque est l'un des principaux problèmes que doit résoudre une cryptomonnaie. Goofycoin n'arrive cependant pas à le résoudre et par conséquent, cette cryptomonnaie n'est pas sécurisée. Le mécanisme de transfert de jeton que nous venons deprésenter ici pour Goofycoin est en fait **le même que celui utilisé par Bitcoin**.

Cependant, étant donné qu'il n'est pas sécurisé, Goofycoin ne peut pas être considérécomme une cryptomonnaie **utilisable**.

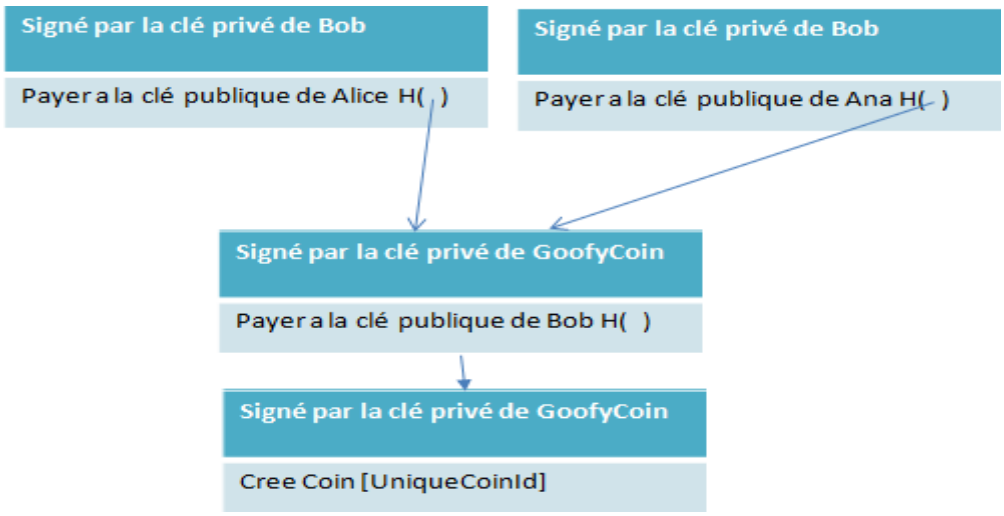

Figure 4 – Problème de double dépense.

Nous pouvons toutefois résoudre ce problème. Les auteurs de [2] fournissent une illustration précise de la méthode à suivre pour résoudre ce problème. Nous allons cependant en donner un bref aperçu dans la section qui suit.

1.2.3 ScroogeCoin

Pour résoudre le problème de double dépense, nous allons concevoir une autre cryptomonnaie appelée **ScroogeCoin**. ScroogeCoin est construite de façon identique à **Goofycoin,** cependant, elle est un peu plus compliquée en termes de structure de données. La première idée de Base est qu'une entité nommée **Scrooge,** publie un registre appelé **append-only ledger (un registre de transactions),** qui va contenir l'historique de toutes les transactions effectuées.

Remarque : La propriété **Append-only** veut dire que toute information écrite sur ce registre, sera enregistrée de façon définitive (on ne pourra pas la supprimer).

Si cette propriété est réalisée, nous pourrons nous protéger contre les doubles dépenses d'un jeton, en requérant que toute transaction ne peut être validée qu'après avoir été inscrite sur le registre. Ceci va nous permettre de nous assurer que le jeton n'a pas été dépensé lors d'une transaction antérieure, et que son propriétaire légitime est bien celuiqui tente de le dépenser. Pour implémenter ce registre de transactions, Scrooge peut construire une blockchain (une chaîne de blocs), qu'il signera numériquement. Cette blockchain consistera en une série de blocs de données, chacun contenant une transaction (en pratique, dans un souci d'optimisation, nous mettrons de multiples transactions dans un même bloc, comme dans Bitcoin). Chaque bloc contiendra :

- L'identifiant de la transaction ;
- Le contenu de la transaction ;
- Un hash pointer vers le bloc précédent.

Scrooge signera numériquement l'empreinte finale du dernier bloc (le pointeur de hachage du dernier bloc), ce qui aura pour effet de signer et lier toutes les données dans la structure. Scrooge publiera la signature en même temps que la blockchain.

Remarque : Signer numériquement le pointeur de hachage du dernier bloc d'une blockchain, équivaut à signer l'ensemble des données de la blockchain. La figure 5 ci- dessous illustre le schéma de ScroogeCoin.

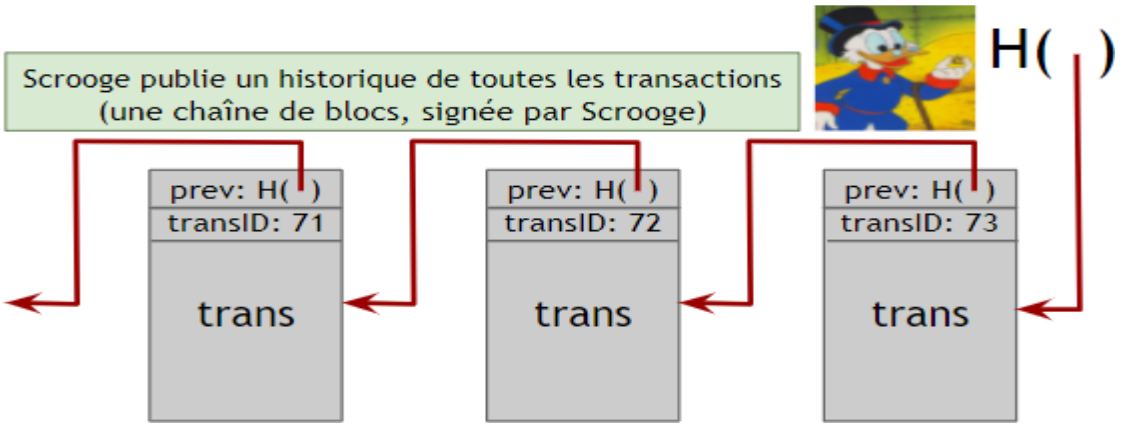

Figure 5 – Scroogecoin Blockchain [2].

Dans le système ScroogeCoin, une transaction ne compte que si elle est contenue dans la blockchain et qu'elle a été signée par Scrooge. Ceci va impliquer que **tout le monde pourra vérifier qu'une transaction a été approuvée par lui, en vérifiant la signature dans le bloc dans lequel la transaction à été inscrite**. Scrooge quant à lui, devra vérifier que la transaction n'est pas en train d'utiliser un jeton qui avait déjà été dépensé, avant de l'inscrire dans le registre. (Il devra vérifier que ce n'est pas une tentativede double dépense). Une question que nous pourrions nous poser c'est : **Pourquoi avons- nous besoin d'une blockchain, alors que toutes les transactions ont déjà été signées par Scrooge ?** Ceci en fait, garantit la propriété de append-only à laquelle nous avons fait mention au début de la section :

- Si Scrooge tente de supprimer ou d'ajouter une transaction ou d'en modifier une déjà existante, ceci va affecter toutes les autres transactions suivant celle-ci ;
- Grâce à la blockchain, et tant que quelqu'un surveille le dernier pointeur de hachage publié par Scrooge, tout changement devient évident et facilement détectable.

La figure 6 ci-dessous illustre le paragraphe précédent.

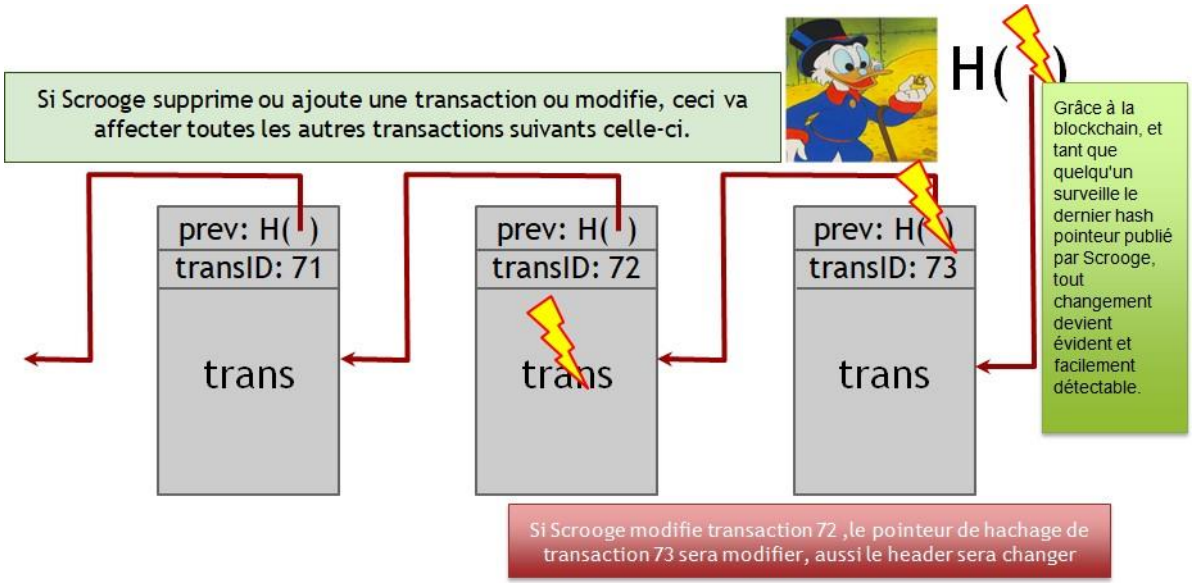

Figure 6 - Modification dans ScroogeCoin Blockchain[2].

Dans un système où Scrooge signerait chaque bloc individuellement, nous aurions besoin de garder une trace de chaque transaction de Scrooge jamais signée. Utiliser la

blockchain rend la surveillance de l'historique de transactions beaucoup plus facile à mettre en œuvre. Cette cryptomonnaie est tout à fait utilisable dans le sens où :

- Les utilisateurs peuvent voir quel jeton est valide.
- La double dépense n'est pas possible, parce que tout le monde pourra regarderdans la blockchain et constater que chaque jeton n'est consommé qu'une seule fois.

Cependant, le problème dans le système ScroogeCoin, malgré le fait qu'il soit tout à fait fonctionnel, est justement Scrooge. Il possède un immense pouvoir, il possède trop de pouvoir dans le système. Il ne peut certes pas créer de fausses transactions, parce qu'il ne peut pas falsifier les signatures des autres. Cependant, il peut :

1. Arrêter d'approuver les transactions de certaines personnes, les priver de serviceet rendre leurs jetons inutilisables ;
2. Il peut refuser de publier des transactions, sauf si des frais de transaction lui sont payés pour chacune d'entre elles ;
3. Bien entendu, Scrooge peut créer autant de jetons pour lui-même qu'il le désire ;
4. Enfin, Scrooge peut en avoir assez de tout ça et arrêter de mettre à jour la Blockchain, et paralyser par conséquent tout le système.

Le problème dans ce système c'est la **centralisation.** Malgré le fait que Scrooge soit satisfait par lui. Les utilisateurs pourraient ne pas l'être. Toutes les cryptomonnaies utilisant une autorité centrale n'ont pas réussi à prendre leur envol en pratique. Parconséquent, le challenge technique le plus important que nous devons relever pour améliorer ScroogeCoin et créer un système fonctionnel et qui puisse marcher est : **Peut- on supprimer Scrooge du système ?** Peut-on nous débarrasser de cette figure d'autorité (Scrooge)? Peut-on avoir une cryptomonnaie qui opère de la même façon que ScroogeCoin dans la plupart des aspects, mais qui n'a besoin d'aucune autorité centrale ? Si nous pouvions résoudre ces problèmes, alors, nous pourrions construire une cryptomonnaie semblable à Scroogecoin mais sans autorité centrale. A vrai dire, un tel système existe déjà, et c'est le Bitcoin [2].

1.3 La décentralisation dans Bitcoin

Lors de la section précédente, nous avons vu un exemple de cryptomonnaie tout à fait utilisable. Néanmoins, cette cryptomonnaie avait un principal défaut : elle reposait surune autorité centrale qui devait valider l'ensemble des transactions. Ceci constituait également le principal frein à l'adoption des cryptomonnaies avant la conception de bitcoin. La vraie innovation de Bitcoin a été de supprimer cette autorité de confiance, et d'arriver à implémenter un système **de cryptomonnaie totalement décentralisé (qui n'avait besoin d'aucune autorité de confiance pour fonctionner).**

Lors de la section qui suit, nous allons tenter de présenter très brièvement comment Satoshi Nakamoto est parvenu à implémenter un système totalement décentralisé.

Définition de la décentralisation : La décentralisation est l'un des termes les plus fréquemment utilisés dans la sphère crypto-économique, et cette notion est souvent perçue comme la seule raison d'être de la blockchain, mais c'est aussi l'une des moins bien définies.

La **décentralisation** est essentielle au fonctionnement et à la sécurité du réseau Bitcoin [3]. Elle signifie que le réseau fonctionne d'utilisateur à utilisateur.

Les aspects de la décentralisation dans Bitcoin sont les suivants :

- **Le Peer-to-peer network** : Cette caractéristique s'appuie sur un réseau pair-à- pair, ouvert à tous et facilement accessible (la barrière d'entrée est assez faible).
- **Le Mining (le minage)** : La capacité de créer des bitcoins et de vérifier des transactions est aussi ouverte à n'importe qui. Seule la concentration de cette capacité de création est un risque identifié pour bitcoin.
- **Mise à jour du logiciel/protocole** : Les core développeurs qui peuvent apporter des modifications au logiciel client [2]. Étant donné que le protocole est open source, tout le monde est censé pouvoir implémenter et utiliser sa propre version du client bitcoin.

Si Bitcoin est décentralisé dans sa gestion des transactions, c'est grâce à deux facteurs :

1. Un algorithme de Consensus distribué ;
2. Une politique d'incitation aux mineurs (politique de récompense).

1.4 Le Consensus distribué

Concept : Le concept de consensus distribué est le suivant :

- Nous avons « n » nœuds dont chacun a une valeur d'entrée (input) ;
- Certains de ces nœuds sont malicieux ou contiennent des erreurs ;
- Le protocole de consensus distribué possède deux propriétés :

    - Le protocole doit se terminer avec tous les nœuds honnêtes en accord sur la même valeur de sortie ;
    - Cette valeur doit avoir été proposée par un nœud correct.

Algorithme de consensus dans Bitcoin

- Les nouvelles transactions sont diffusées sur tous les nœuds ;
- Chaque nœud collecte de nouvelles transactions dans un bloc ;
- À chaque tour, un nœud aléatoire parvient à diffuser son bloc ;
- Les autres nœuds n'acceptent le bloc que si toutes les transactions qu'il contientsont valides (signatures non dépensées et valides) ;
- Les nœuds expriment leur acceptation du bloc en incluant un pointeur de hachagevers lui dans le bloc suivant qu'ils créent [2].

1.5 Récompense et incitation

La deuxième propriété du protocole de consensus est un concept qui n'est possible que parce que bitcoin est une cryptomonnaie : **L'incitation**. Par convention, la première transaction d'un bloc est une transaction spéciale, qui crée de la nouvelle monnaie (de nouveaux bitcoin) attribuée au créateur du bloc. Cela incite les nœuds à participer au réseau, et fournit un moyen d'introduire de la monnaie en circulation, car il n'existe pas d'autorité centrale pour émettre cette monnaie. Cette participation constamment monnayéeest analogue à la démarche des chercheurs d'or qui affectent des ressources pour introduire de l'or en circulation. Dans notre

cas, c'est l'électricité et le temps de calcul qui sont affectés. L'incitation peut aussi être financée avec des frais de transaction. Lorsque la valeur résultante d'une transaction est inférieure à sa valeur émise, la différence correspond à des frais de transaction ajoutés au montant d'incitation de création du bloc contenant la transaction. Une fois qu'un montant prédéterminé de monnaie est entré en circulation, l'incitation peut être convertie entièrement en frais de transaction, évitant une inflation (Le nombre total de bitcoin qui devraient être mis en circulation sera de 21 millions de bitcoin). L'incitation peut encourager les nœuds à rester honnêtes,

Récompense

Trouver comment inciter les nœuds à agir de façon honnête, est un problème difficile, puisque dans le réseau Bitcoin, les nœuds sont pseudo anonymes (sans identité). Par conséquent, nous ne pouvons pas pénaliser ceux qui agissent mal (qui nuisent au réseau). Pour remédier à cela, Bitcoin a choisi de récompenser, au contraire, les nœuds quiagissent de façon honnête. Le fait que bitcoin utilise une cryptomonnaie, lui confère la possibilité de récompenser les utilisateurs agissants honnêtement. Ceci aurait été difficile sans cryptomonnaie incluse dans le système. Pour récompenser les utilisateurs, Bitcoin possède deux mécanismes : la récompense de bloc (Bloc reward) et les frais de transactions (transaction fees).

1.5.1 Récompenser par bloc (Block reward)

Ce mécanisme permet au créateur du bloc de :

- Y inclure une transaction spéciale. Cette transaction est une transaction de créationde pièces, analogue à CreateCoins dans ScroogeCoin ;
- Choisir l'adresse du destinataire de cette transaction, ce nœud choisira généralement une adresse lui appartenant.

À partir de 2021, la valeur de la récompense de bloc est fixée à 6,25 BTC. Elle est divisée par deux chaque 210 000 blocs créés. Sur la base du taux de création de blocs, le taux diminue de moitié environ tous les quatre ans. Le créateur du bloc ne sera récompensé que si

le bloc aboutit sur la branche du consensus à long terme, car comme toute autre transaction, la transaction de création de pièces ne sera acceptée par les autres nœuds, que si elle aboutit sur la chaîne de consensus. C'est l'idée clé de ce mécanisme d'incitation. C'est une astuce subtile mais puissante. Cela incite les nœuds à se comporter de la manière dont ils pensent que la conséquence sera que d'autres nœuds étendront leurs blocs. Ainsi, si la majeure partie du réseau suit la règle « de la branche valide la plus longue », cela incite tous les nœuds à continuer à suivre cette règle. C'est le premier mécanisme d'incitation de Bitcoin.

1.5.2 Les frais de transaction (Transaction Fees)

Le créateur d'une transaction peut choisir de mettre une valeur de sorties (output), inférieure à la valeur des entrées (input), La différence entre les deux sera considérée par les mineurs comme des frais de transactions. Les frais de transaction sont purement volontaires, mais elles tendent à devenir pratiquement obligatoires. Le mineur choisit quelle transaction il va mettre dans un bloc. Étant donné que les frais de minage sont toujours en augmentation, Le mineur ayant investi énormément en matériel et ressources énergétique, voudra prendre la meilleure récompense possible pour son travail. Quelques problèmes subsistent avec le mécanisme de consensus que nous venons de décrire :

Le premier élément majeur est : comment choisir un nœud aléatoirement pour qu'il propose un bloc. Deuxièmement, nous avons créé un nouveau problème en donnant aux nœuds ces incitations à la participation. Le système peut devenir instable car les incitations provoquent un free-for-all, où tout le monde veut gérer un nœud Bitcoin dans l'espoir de bénéficier de certaines de ces récompenses. Un troisième problème est qu'un adversaire pourrait créer un grand nombre de nœuds Sybil pour essayer de renverser le processus de consensus en sa faveur[2].

1.6 Minage et preuve de travail

Tous les problèmes avec le mécanisme de consensus que nous venons de citer sont liés. Et ils ont tous la même solution : **la preuve de travail.** L'idée clé de la preuve de travail est que nous approximons la sélection aléatoire d'un nœud, en sélectionnant des nœuds proportionnellement à une ressource que nous espérons, personne ne pourra monopoliser. Si, par exemple, cette ressource est la puissance de calcul, alors c'est un système de preuve de travail (Proof of work). Alternativement, cela pourrait être proportionnelle à la propriété de montant en monnaie, qui est connue sous le nom de preuve de participation (Proof of stake), cette dernière n'est pas utilisée dans Bitcoin mais l'est dans d'autres crypto-monnaies.

1.7 Mécaniques de bitcoin

1.7.1 Transactions Bitcoin

Les transactions sont la base sur laquelle se construit la blockchain Bitcoin, ils sont les résultats d'un brillant mélange entre cryptographie, structures de données et un langage de script. Nous allons dans cette partie, donner un bref aperçu de la structure d'une transaction.

Structure d'une transaction

1. **Les metadata** : hash de la transaction et des informations en plus (nombred'inputs, outputs, taille totale, etc.);
2. **Les inputs** : un tableau avec le détail des inputs;
3. **Les outputs** : un tableau avec le détail des outputs.

En réalité, les transactions dans Bitcoin sont écrites sous forme de script. Afin de rester le plus concis possible, nous n'avons pas inclus une partie qui traite du script Bitcoin dans le document. De nombreuses ressources sont disponible sur le langage script utilisé par Bitcoin.

1.8 Les différents types de blockchain

Les systèmes de Blockchain actuels peuvent être grossièrement classés en trois types :

1. **Les Blockchains publiques :** ce sont des grands réseaux distribués accessibles, ouvertsà tous et à tous les niveaux, Ils ont également un code source ouvert, que leur communauté maintient à jour. Comme exemple de blockchain publique, nous pouvons citer Bitcoin.

2. **Les Blockchains consortium :** ce sont des réseaux distribués qui contrôlent les rôles de chaque nœud dans les réseaux, le code source peut être ouvert ou non. Comme exemple, nous pouvons citer la blockchain Ripple.

3. **Les Blockchains privées** elles sont plus petites que les autres types, leur accès est complètement contrôlé.

1.9 Conclusion

Dans ce premier chapitre, nous avons tout d'abord introduit les notions de cryptomonnaie, autorité centrale, et double dépense. Ensuite, nous avons pu étudier le procédé technique sur lequel repose Bitcoin et de comment elle apportait une solution simple aux problèmes de double dépense tout en supprimant les autorités de confiance. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne. Leprincipe de base de Bitcoin repose sur la notion de preuve de travail, et a recours aux techniques de la cryptographie. Nous avons mentionné dans la dernière partie du chapitre, que Bitcoin utilise un langage de script afin de représenter les transactions. Malgré le fait que Bitcoin ait été dans un premier temps conçu afin de permettre d'effectuer des paiements au travers d'internet sans passer par une autorité centrale, de nombreuses autresapplications de la blockchain sont en train de voir le jour et font l'objet de recherches etde publications scientifiques. Nous allons au cours du chapitre suivant présenter quelques-unes de ces applications dans le domaine de la santé

Chapitre 2

Les applications de la blockchain dans le domaine de la santé

2.1 Introduction

Au cours du chapitre précédent, nous avons défini les différents principes de base de la blockchain et de son fonctionnement.

La blockchain peut être envisagée pour de multiples usages dans de nombreux domaines : finance, assurance, immobilier, santé, etc. Nous allons au cours de ce chapitre, donner des exemples d'applications de la blockchain dans le domaine de la santé. Nous commencerons par faire un point sur la recherche scientifique en la matière. Par la suite, nous dresserons un tableau récapitulatif des différentes applications possibles.

2.2 Etat de la recherche scientifique en matière de blockchain et de santé

Le domaine de la santé est parmi les domaines qui vont selon certains experts être les plus impactés par la technologie blockchain. En effet, plusieurs études ont été menées et publiées sur le sujet. Cependant, étant donné le large spectre du domaine de la santé, il est difficile de prédire quel sous-domaine est le plus prometteur. Les auteurs de [3] ont publié une étude sur le sujet, l'étude a sélectionné un ensemble de 39 publications scientifiques (qu'ils ont jugé les plus pertinentes) parmi un nombre beaucoup plus élevé d'articles. La figure 7 ci-dessous résume les solutions proposées dans la littérature scientifique utilisant la technologie blockchain.

Health Information system	Process that is to be improved	Main challenge that is addressed
Electronic health records	Shared decision making	Interoperability, access control, data integrity
Electronic health records	Health data recording, storing and sharing	Access control, interoperability
Knowledge infrastructures	Aid decision-making by presenting knowledge	Data integrity, repudiation
Electronic health records	Sharing of healthcare information for clinical and research purposes	Access control, interoperability
Personal health records	M-health data recording, storing and sharing	Data integrity, data provenance
Picture archiving and communications systems	Exchange of medical images	Access control
IoT data management/Personal health data	Remote collection and storage of health data	Data integrity, access control
Personal health records	Sharing healthcare data between health institutions	Interoperability, data provenance
Personal health records	Automatic collection, storage and patient-controlled sharing of personal health data	Access control, interoperability
Personal health records	Sharing of health data for use by more than one healthcare institution	Access control, interoperability
Automated diagnostic service for patients	Collection and storage of data about symptoms of dyslexia for the purpose of automated diagnostics, decision-support and research.	Access control, data integrity, interoperability
Electronic health records	Sharing healthcare data between health institutions	Data integrity
Electronic health records	Sharing healthcare data between health institutions	Data integrity, access control
Administrative systems	Sharing healthcare information for administrative or economic purposes	Data integrity, data provenance
Electronic health records	Sharing healthcare data for clinical and research purposes. Recording and sharing of contracts/agreements.	Access control, interoperability, data integrity
Electronic health records	Sharing healthcare (health record) information for clinical, research and administrative [economic] purposes.	Access control, interoperability
Personal health records	Collecting and sharing [health-related] sensor data for clinical purposes.	Interoperability
Electronic health records	Sharing healthcare data for clinical and research purposes.	Access control, interoperability
Electronic health records/ Administrative system	Sharing healthcare data for administrative or economic purposes	Identity management, access control
Electronic health records	Patient data management and storage in a cloud environment	Access control, data integrity, data provenance
Population health management system	Collection and storage of sensor data for remote patient monitoring purposes	Data integrity, data provenance
Personal health data/Electronic health records	Managing access to personal health data and electronic health records	Access control, data integrity
Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, data integrity, interoperability
Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Interoperability, access control
Pharma supply-chain	Monitoring the distribution of drugs in a pharmaceutical supply chain.	Data integrity, data provenance
Clinical Trial Support Systems	Recruitment of patients to clinical trials	Data integrity, data provenance
Electronic health records	Sharing healthcare data for clinical and research purposes	Interoperability, data provenance
Clinical Trial Support Systems	Sharing healthcare information for research purposes	Data integrity, data provenance
Research support systems	Establishing a patient-controlled marketplace for selling and buying of healthcare information for research purposes	Access control, interoperability
Personal health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, privacy, data integrity
Electronic health records	Health record storing	Data integrity, privacy
Infectious disease surveillance system	Public health management (monitoring the outbreak of infectious diseases)	Data integrity, data provenance
Telemedicine system	Finding the patient in the context of telemedicine services	Data integrity
Electronic health records	Retrieving information in the EHR	Access control, data integrity
Electronic health records	Sharing healthcare data for clinical and research purposes	Access control, security, interoperability
Personal health records	Patient-controlled collection and sharing of sensor data	Access control, data integrity
Electronic health records	Sharing healthcare data between health institutions	Data provenance
Electronic health records	Patient-controlled sharing of health data between healthcare providers	Access control, interoperability
Electronic health records	Exchange of healthcare data for clinical and research purposes	Access control, interoperability

Figure 7 – Résumé des solutions proposées dans la littérature scientifique utilisant la technologie blockchain [3].

2.2.1 Répartitions des publications selon le système de santé visé

Selon les auteurs de [3], Le système le plus fréquemment ciblé était le DSE (le dossier de santé électronique), 43% des publications traitant de ce sujet. Les autres systèmes de

concentration étaient les PHR (personal health record ou dossier personnel desanté) (15%) et les systèmes de soutien aux essais cliniques (5%). Les processus au sein des systèmes cibles étaient pour la plupart axé sur le partage, le stockage, l'échange et l'accès aux données médicales. Plus de la moitié des publications (62%) traitaient de certains processus de partage des données sur la santé. De nombreux PHR ont été proposés comme contrôlés par le patient et non liés à un établissement ou un système de santé en particulier [3] .

Les défis que la blockchain vise à améliorer dans le domaine de la santé :

La figure 7 illustre également les problèmes traités dans la littérature scientifique, la blockchain a été suggérée comme une amélioration du contrôle d'accès dans 35% des publications incluses. Par exemple, dans l'article [3], l'accès aux données (images médicales) a été fourni en demandant et en approuvant les transactions des données (stockées hors chaîne de blocs) avec des clés privées et publiques. Une autre approche a été suggérée par les auteurs de [4], dans laquelle l'accès est accordé en interrogeant les données sur la blockchain et en les récupérant avec les URL FHIR (Healthcare Interoperability Resources)[5] une fois localisées. Le service d'adhésion Hyperledger Fabric a été utilisé par les auteurs de [6] pour l'émission d'un certificat d'inscription et d'uncertificat de transaction pour le contrôle d'accès [3].

Les solutions blockchain pour les défis d'interopérabilité ont été discutées dans plusieurs articles (27%, figure 7). Par exemple, l'interopérabilité a été obtenue en référençant les ressources FHIR (URL) dans certaines solutions. Une autre approche consistait à fournir un composant traducteur comme passerelle des blocs de données, traduction de formats utilisant une norme différente [3].

La capacité d'améliorer la provenance a été ciblée dans 12% des publications incluses (figure 7). Dans un concept de blockchain pour les chaînes d'approvisionnement médicales, la provenance des données a été améliorée par l'utilisation d'appareils IoT de confiance qui exécutent des contrats intelligents sur la blockchain. D'autres exemples ont été trouvés dans les concepts relatifs aux essais cliniques, où les problèmes de provenancedes données sont ciblés en fournissant un système de suivi des données utilisées dans les essais [3].

Pour augmenter l'intégrité des données, une solution blockchain a été proposée dans 28% des publications incluses dans [3] . Généralement, l'intégrité des données a été maintenue par la propriété d'immuabilité de la blockchain. L'intégrité des données a été améliorée en stockant des données médicales hachées ou un pointeur de hachage sur la chaîne. Une autre approche d'utilisation de la blockchain pour maintenir l'intégrité des données a été trouvée dans les essais cliniques où des contrats intelligents et l'intégration avec des appareils IoT de confiance sont utilisés [3]. Le tableau 1 ci-dessous résume également les catégories de systèmes d'informations traités dans les recherches. Nous pouvons constater que le dossier de santé électronique représente 43 % des publications, le dossier de santé personnel 15% et les systèmes de soutient au essaies cliniques 5%, les autres domaines ne sont pas encore très bien représentés.

Tableau 1 – Systèmes d'information de santé impactés par la technologie blockchain[3].

Catégorie de système d'information	Nombre de publication sur les 39 sélectionnés	Proportion des articlespris en charge par [3]
Dossier de santé électronique	17	43%
Dossier de santés personnelles	6	15%
Systèmes de soutien aux essais cliniques	2	5%
Infrastructure de données	1	3%
Archivage d'images et systèmes de communication	1	3%
Gestion de données IoT/Données de santé personnelles	1	3%
Service de diagnostic automatisé pour les patients	1	3%
Systèmes administratifs	1	3%
Dossier de santé électronique / Système administratifs	1	3%
Système de gestion de la santé de la population	1	3%
Chaîne d'approvisionnement pharmaceutique	1	3%
Total général	39	

2.2.2 Types de Blockchain utilisées dans les solutions proposées

Une blockchain de consortium (38%) était le type préféré parmi les publications incluses dans l'étude [3] . Bien que plusieurs des articles n'aient pas défini leur approche (26%), Les blockchains privées (10%) et publiques (15%) semblent moins utilisées dans le domaine de la santé [3] (Voir figure 8).

2.2.3 Plateformes blockchain utilisées dans la santé

Ethereum a été utilisé dans onze (28%) des 39 publications incluses, Hyperledger Fabric [7] quatre fois (10%) et Exonum [8] une fois (4%) (Figure 8). 14 études (36%) ontdéveloppé une nouvelle blockchain pour leurs concepts respectifs. Huit (21%) des études incluses n'ont pas précisé une plate-forme ou un cadre pour leur concept (la figure 8 illustre ces proportions) [3].

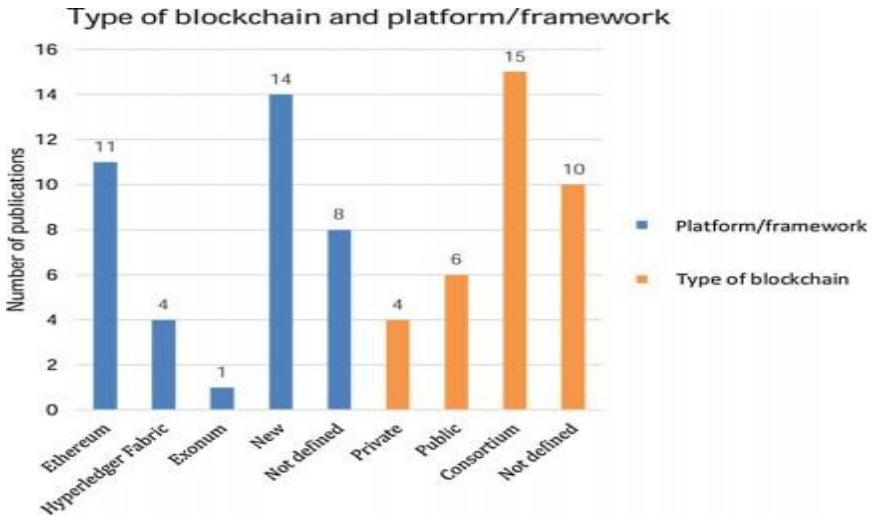

Figure 8 – Les types de blockchain et les plateformes [3].

2.2.4 Algorithme de consensus dans les projets de santé

Les résultats résumés dans [3] indiquent qu'une variété d'algorithmes de consensusest utilisée pour les concepts de blockchain dans le domaine de la santé (tableau 2). L'algorithme

de consensus le plus fréquemment utilisé dans les publications incluses était PoW (preuve de travail), représentant 21% des cas. En plus, il convient également de noter que tous les concepts construits à l'aide de la plate-forme Ethereum ou des protocoles Ethereum n'utilisaient pas de PoW. Le deuxième algorithme de consensus le plus fréquemment utilisé était le PBTF (Practical Byzantine Fault Tolerance) (15%). Plusieurs (41%) des publications n'ont pas indiqué quel protocole de consensus leurconcept entendait appliquer[3].

Tableau 2 – Utilisation de l'algorithme de consensus [3].

Consensus Algorithm	Count
Proof of Work (PoW)	8
Proof of Work (by pre-selected miner)	1
Practical Byzantine Fault Tolerance (PBFT)	6
Proof of Stake (PoS)	1
Proof of Interoperability	1
Proof of Conformance	1
Permissioned Voting-based	2
Ledger-based Byzantine	1
Fault ToleranceHybrid (Delegated PoS+PBFT)	1
Quorum Chain consensus	1
Non défini	16

2.2.5 Utilisation de contrats intelligents

Dans plusieurs des concepts proposés, les contrats intelligents étaient une caractéristique : 38% des études incluses utilisaient des contrats intelligents pour certaines fonctionnalités. Les autres études n'ont pas défini si les contrats intelligents étaient une caractéristique ou non (tableau 3) [3].

Tableau 3 – Utilisation des contrats intelligents [3].

Utilisation des smart contrat	Count
Oui	15
Non défini	24

2.3 Le potentiel de la blockchain dans le domaine de la santé

Après avoir dans la section précédente donné un résumé des publications scientifiques en matière de blockchain et de santé, nous allons dans celle qui suit décrirele potentiel de la blockchain dans ce domaine d'une manière un peu plus détaillée.

Les activités dans le domaine de la santé nécessitent un échange efficace de consentements des patients. Elles nécessitent également un processus de remboursement efficace. Tout ceci signifie échanger des données au-delà des frontières institutionnelles de plusieurs établissements. En même temps, les établissements de santé ont pour mandat de protéger les données hautement sensibles, que les patients choisissent de partager avec eux. Pour préserver à la fois la confidentialité des données du patient et échanger des données avec d'autres institutions de l'écosystème de santé, **le contrôle d'accès, la provenance, l'intégrité et l'interopérabilité des données sont essentiels.** La méthode traditionnelle de contrôle d'accès suppose généralement la confiance entre le propriétaire des données et les entités qui les stockent. Ces entités sont souvent des serveurs entièrement chargés de définir et d'appliquer les politiques de contrôle d'accès [3].

L'interopérabilité est la capacité de différents systèmes d'information, appareils ou applications à connecter, de manière coordonnée, à l'intérieur et au-delà des limites de l'organisation pour accéder, échanger et utiliser en coopération les données entre les parties prenantes, dans le but d'optimiser la santé des individus et des populations. La provenance des données fait référence à l'historique des données et à leurs origines. Dans les données du domaine de la santé, la provenance peut, par exemple, être d'assurer l'auditabilité et la transparence du DSE (dossier médical électronique), afin de garantir la confiance des patients dans le système logiciel du DSE. L'intégrité des données en tant que définition générale est la définition de la qualité des données qui traite de la qualité attendue des données. Cela signifie que le degré auquel la qualité attendue des données estatteinte ou dépassée détermine l'intégrité des données.

Les établissements de santé connaissent actuellement une demande accrue dedonnées du monde réel de la part de l'industrie et des organismes de recherche. Dans le même temps, le partage non autorisé, les piratages et le vol de données sensibles très médiatisés érodent constamment la confiance du public dans les établissements de santé. Un troisième problème concerne les mauvaises pratiques au sein de l'écosystème de la santé, qui exploitent la même confiance (par exemple, les problèmes avec les médicaments contrefaits, les procédures, les compétences et les patients). Pris ensemble, c'est une situation qui oblige à repenser et à envisager des approches alternatives. Avec certains de ses attributs clés tels que la décentralisation, distribution et intégrité des données, et sans aucun tiers nécessaire, la technologie blockchain possède de nombreuses propriétés attrayantes qui pourraient être utilisées pour améliorer et obtenir un niveau d'interopérabilité plus élevé, partager des informations, contrôler l'accès, garantir provenance et intégrité des données parmi les parties prenantes mentionnées, évoluant ainsi vers une nouvelle infrastructure pour bâtir et maintenir la confiance.

2.4 Blockchain dans la e-santé

2.4.1 E-Santé (santé électronique) définition

La santé électronique « E-Santé » fait référence à l'application des technologies de l'information et de la communication dans les services médicaux et à ce qui est lié à la télémédecine, à la prévention des soins à domicile et aux dossiers médicaux électroniques tels que définis par l'Organisation mondiale de la santé en 1945.

La santé électronique est devenue une solution adaptée pour répondre aux besoins du système de santé, mais même si certains pays disposent de systèmes de prescription électronique et de portails et de dossiers de santé nationaux en ligne (Le patient est numérisé depuis 2000 dans certains pays), la santé électronique est encore sous-utilisée malgré son importance. Cependant, avec la crise sanitaire mondiale que nous avonsconnue en 2020 à cause du covid 19, les pratiques de e-santé (télémédecine, dossier médical électronique etc .) ont prouvé leur importance pour les patients dans les contextes de confinement et dans ceux de

difficultés de déplacement.

Aujourd'hui, la sécurité des données est devenue un enjeu majeur dans le secteurde la santé. Les informations des patients et les données médicales sont des informations personnelles et nécessitent une réelle sécurité pour garantir leur confidentialité et leur intégrité. La gestion décentralisée, la flexibilité et la confidentialité sont des défis que la blockchain peut relever.

2.4.2 La technologie de la blockchain pour l'E-santé

Les services fournis par la blockchain, en particulier l'automatisation des transactions de contrats intelligents, ouvrent de larges perspectives pour l'amélioration etla croissance de certains acteurs dans des domaines tels que l'IoT ainsi que la e-santé. Ils donnent également accès à un nouveau paradigme pour l'échange d'informations médicales plus efficaces, et plus sûr en matière de protection des données personnelles.

La technologie blockchain permet d'établir la confiance entre des acteurs aux intérêts différents. Initialement destinée à répertorier les transactions interpersonnelles, elle a largement évolué en fonction des progrès technologiques et de l'intérêt croissant desentreprises internationales. Dans le secteur de la santé, la blockchain peut être utile parplusieurs de ses fonctionnalités : son immutabilité qui en fait un excellent support pour authentifier des données sensibles comme des consentements d'essais cliniques, la possibilité d'éditer des smart contracts qui automatisent et facilitent de nombreux processus ou encore la constitution d'un réseau qui se met d'accord sur l'état de l'information. Beaucoup plébiscitée, la blockchain doit néanmoins faire ses preuves dans les conditions réelles d'utilisation et s'inscrire dans un contexte réglementaire et économique particulièrement complexe dans le secteur de la santé [9].

La technologie Blockchain peut être appliquée pour le partage et la sécurité des patients. Leurs données sont traitées quotidiennement, tout en respectant la confidentialité grâce au contrôle d'accès modifiable. Elle permet à toutes les données d'être partagées et hachées et sauvegardées et enfin d'être consultées après application d'un contrôle d'accès. Cette politique

sauvegardée dans la blockchain définit quel médecin peut accéder à quels types de données et pendant quelle période. Le patient peut ajouter des données et des consentements/autorisations. Le personnel de santé peut accéder aux données (lire) et ajouter/modifier les données (écrire) selon l'autorisation du patient. L'intégrité des données est garantie grâce à l'utilisation du hachage.

2.4.2.1 Applications de la Blockchain dans les soins de santé.

Avec son mécanisme de stabilisation et la protection des ensembles de données avec lesquels les utilisateurs peuvent interagir, le potentiel de la technologie blockchain peut être vu dans les domaines de la médecine, de la génomique, de la télémédecine, de la télésurveillance, de la médecine électronique, des neurosciences et des applications médicales personnalisées. Différentes interactions entre différents types de transactions (comme le montre le modèle de la figure 9 ci-dessous).

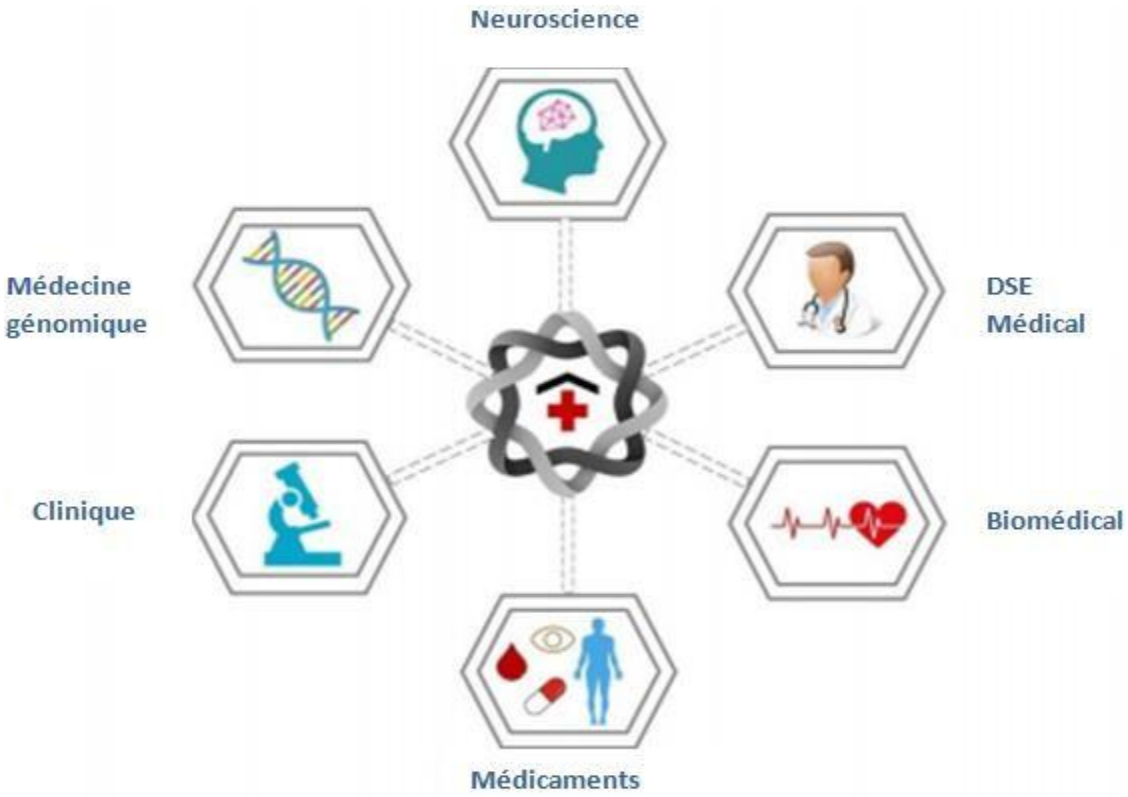

Figure 9 – Applications des blockchains en santé.

2.4.2.2 Gestion des données médicales

De nos jours, il est difficile de visualiser de manière claire toutes les données liées à un patient et accumulées au cours de son parcours de soins. Ces informations proviennent habituellement de sources très variées, comme les médecins de ville, l'hôpital, les assurances, les pharmaciens ou les laboratoires d'analyses médicales. Les logiciels utilisés par ces parties prenantes pour collecter et gérer les dossiers médicaux sont différents et ne sont pas interopérables. Ainsi, il est parfois difficile de partager les informations. Par ailleurs, même si ces informations peuvent toutes être récupérées et assemblées, il n'est pas toujours évident de savoir dans quel ordre elles ont été produiteset si elles sont exhaustives. Ce problème est fréquemment rencontré lors de l'admission d'un patient à l'hôpital. Les professionnels de santé n'ont en effet pas toujours accès à sonhistorique et n'ont pas une visibilité complète sur les traitements qu'il prend, sur l'historique de sa maladie ou sur ses antécédents familiaux.

L'idéal serait donc d'avoir une liste qui répertorie tous les lieux où se trouvent les données médicales d'un même patient afin de pouvoir rapidement les récupérer. Cette liste serait accessible, avec l'accord du patient, à tout professionnel de santé qui en feraitla demande. Ainsi, plutôt que de n'avoir accès qu'à la base de données de l'établissement où l'on se trouve, on pourrait avoir accès à toutes les sources d'informations dispersées dans toutes les bases de données du réseau. La technologie *blockchain* apporte justement cette solution sous la forme d'un registre distribué et sécurisé qui permet au patient non seulement d'avoir une visibilité sur ses données, mais aussi d'en contrôler les accès et d'en être le propriétaire.

2.4.2.3 Respect de la vie privée des patients et le contrôle d'accès sur les données

Dans le monde de l'E-santé aujourd'hui, deux grands axes sont abordés : la sécurité et la propriété des données. Les dossiers médicaux sensibles manquent actuellement de structure sécurisée, ce qui entraîne des violations de données aux conséquences graves. Selon une étude récente menée par le Ponemon Institute pour le compte d'IBM Security, le coût total moyen des violations de données aux États-Unis était de 7,91 millions de dollars, le secteur de la santé

ayant le coût par habitant le plus élevé.

La technologie Blockchain peut être appliquée aux dossiers patients pour lespartager et les sécuriser lors de leur traitement quotidien, tout en respectant la vie privée grâce à un contrôle d'accès modifiable. Quelques systèmes basés sur la blockchain ont été proposés pour l'organisation et l'accès aux dossiers médicaux des patients. MedBlock[10], un système de gestion des informations basé sur la blockchain, permet un accès et une récupération efficaces du DME (dossier médical électronique) grâce aux principes de la blockchain distribuée.

Les systèmes de contrôle d'accès sont utilisés en informatique pour réguler l'accès aux ressources critiques ou précieuses telles que les données, les services, les systèmes informatiques, l'espace de stockage, etc.

L'accès du sujet aux ressources se fait généralement par le biais de politiques de contrôle d'accès, évaluées au moment de la demande d'accès par rapport au contexte d'accès actuel. Dans le contrôle d'accès basé sur les attributs (ABAC) (Attribute-based access control), les politiques consistent en un ensemble de conditions sur lesquelles les caractéristiques des objets, des ressources, etc., sont liées à la demande d'accès.

Parmi les attributs du sujet, il pourrait y avoir, par exemple, son identifiant,l'identifiant de l'entreprise pour laquelle il travaille, son rôle dans cette société, le nom des projets qui lui sont assignés, sa position physique, le nombre de ressources qu'elle utilise actuellement. Enfin, certains scénarios exigent que les droits d'accès puissent être transférés d'un sujet à un autre pour certaines raisons. Par exemple, un utilisateur pourrait vendre son droit d'accès à un autre utilisateur. Un autre exemple est celui où un employé d'une entreprise censé effectuer un calcul donné sur une machine virtuelle délègue l'exécution de cette tâche à un autre employé, qui doit accéder à cette même machine virtuelle [11].

Le partage sécurisé des données de santé fait également l'intégration des soins de santé. Les auteurs de [12] ont organisé un plan de partage d'informations sur les patients, appelé

système de partage des informations sur la santé des patients, basé sur la blockchain, sécurisée et préservant la confidentialité, qui pourrait améliorer le diagnostic des patients dans les systèmes de santé virtuels. Leur schéma comprend l'usage de chaînes de blocs privés de consortium et des mécanismes de consensus pour une sécurité maximale. Les informations privées sur la santé des patients sont stockées dans la blockchain privée tandis que les enregistrements de l'activité, les informations sur la santé des patients, sont stockés dans la blockchain du consortium, et toutes les données sont cryptées [12].

2.4.2.4 Détection de fraude médicale

Une importante application des blockchains dans l'industrie médicale comprend la gestion de la chaîne d'approvisionnement en médicaments. La gestion de l'offre est une question cruciale à préserver dans tous les secteurs, mais elle revêt une importance accrue dans le secteur de la santé en raison de sa complexité croissante. En effet, tout compromis dans la chaîne d'approvisionnement en soins de santé affecte le bien-être du patient. Les chaînes d'approvisionnement sont vulnérables et consistent en des trous pour les attaques frauduleuses car elles impliquent un certain nombre de pièces et de personnes en mouvement. Les Blockchains constituent une plate-forme sûre et sécurisée permettant d'éliminer ce problème et, dans certains cas, d'empêcher la fraude, en introduisant une transparence accrue des données et une traçabilité améliorée des produits.

2.4.2.5 Dossier de Santé Électronique (DSE)

Au cours de la dernière décennie, la numérisation des dossiers médicaux a été rendue nécessaire par les médecins, les hôpitaux et les dispositifs médicaux, car la numérisation de ces données permet un accès et un partage aisés, ainsi qu'une base pour une prise de décision rapide et plus efficace. Comme nous l'avons vu lors des sections précédentes, les applications les plus courantes des technologies de blockchain en matière de soins de santé se situent actuellement dans le domaine des dossiers médicaux électroniques.

Toutefois, les dossiers de santé électroniques (DSE) ne sont pas créés pour gérer les enregistrements de plusieurs institutions. Devant le besoin critique de trouver un moyen

innovant de gérer les DES, de manière à encourager les patients à consulter leurs données de santé actuelles et historiques, de nombreux chercheurs ont évoqué la technologie blockchain pour la maintenance des DSE. Un prototype appelé « MedRec » utilise des avantages distincts pour la gestion de l'authentification, la confidentialité, l'intégrité et le partage aisé des données. Il fonctionne sur un système de gestion des dossiers décentralisé et prétend fournir aux patients un historique immuable et détaillé, et permet un accès facile à leurs informations de soins de santé respectives auprès de divers prestataires et établissements de traitement. « MedRec » ne stocke pas de dossiers médicaux et n'exige pas de temps d'ajustement. Il enregistre une empreinte du dossier sur une blockchain et en informe le patient, qui est responsable de l'emplacement du dossier.

L'empreinte garantit qu'un duplicata inchangé du disque a été acquis. De même,il déplace le pouvoir de contrôle de l'organisation au patient, ce qui pèse sur le patient et lui permet d'assumer la responsabilité de propriétaire. Pour les patients qui préféreraientne pas traiter leurs informations, les associations d'administrateurs sont supposées remplir le rôle d'agent du patient pour cette tâche. Le cadre MedRec comprend également une interface utilisateur, destinée à améliorer la connexion persistante avec les enregistrements de soins de santé, qui se déplacent dans plusieurs organisations.

Exemples d'utilisation de la blockchain :

Dans le domaine de la santé, un certain nombre d'entreprises ont commencé à utiliser la blockchain dans divers domaines d'applications par exemple, l'entreprise Gem (en collaboration avec Philips Healthcare Blockchain Lab), PokitDok, Healthcoin, HashedHealth.

Ou encore, le groupe de travail Hyper ledger Healthcare qui est un consortium qui fournit une collaboration open source des entreprises membres du secteur de la santé, dansle but d'accélérer le développement de l'adoption commerciale de la blockchain. Cependant ceci relève encore de la recherche scientifique, et nous n'avons pas pu au coursde notre travail, trouver un exemple concret d'utilisation.

2.5 Conclusion

La recherche sur l'utilisation de la blockchain dans les soins de santé est désormais établie en tant que domaine académique, et le nombre et la qualité des publications augmentent rapidement. Cette tendance est également perceptible dans les soins de santé, le secteur industriel, où le marché de la technologie blockchain devrait selon certains spécialistes dépasser les 500 millions de dollars d'ici 2022. En raison de l'importance primordiale de maintenir la confiance tout en satisfaisant une demande toujours croissante d'échange de données au sein de l'écosystème de la santé, les établissements de santé sont en manque de solutions nouvelles qui pourraient améliorer ou préserver la confiance. L'état de la recherche, comme nous venons de le décrire dans ce chapitre, montre que des solutions basées sur la blockchain sont actuellement explorées dans quelques DSE. Plusieurs autres domaines de la e-santé sont encore sous-explorés, car il existe peu ou pas de publications sur ces thèmes, à savoir, les systèmes d'archivage d'images et de communication, les services de diagnostic automatisé pour les patients, les systèmes administratifs, les systèmes de gestion de la santé de la population ainsi que les chaînes d'approvisionnement pharmaceutique. Le programme de recherche doit être élargi pour aborder ces domaines concrètement, ainsi que pour répondre à la recherche de solutions basées sur la blockchain qui préservent la confiance en atténuant les menaces tant à l'intérieur qu'à l'extérieur du secteur de la santé. Nous avons au cours de ce chapitre fait une analyse des champs de recherche actuel concernant la blockchain dans le domaine de la santé. Nous avons également présenté quelques applications possibles. Lors du prochain chapitre, nous allons définir la problématique que nous avons traité dans notre projet de fin d’études, nous donnerons également les étapes de la conception de l’application que nous avons développé afin d’apporter une solution à cette problématique.

Chapitre 3

Dapps et Blockchain dans la E-Santé : Contrôle d'accès aux données médicales

3.1 Introduction

Après avoir lors du chapitre précédent donné un descriptif des applicationspossible de la blockchain dans le domaine de la santé, nous allons dans celui qui suit présenter la problématique que nous avons traité à savoir la proposition d'un système de contrôle d'accès pour l'amélioration de la sécurisation du partage de l'information entre acteurs, dans un système de santé. Nous allons par la suite donner les étapes de conception de notre solution. Mais dans un premier temps, nous allons d'abord définir la notion de Dapp (application décentralisée) ainsi que ces caractéristiques.

3.2 Dapps

Qu'est-ce qui ressort de la capacité de manipuler les chiffres et les données de façon fiable grâce à des contrats intelligents et qu'est-ce que nous pourrions appeler une telle application ? Nous pouvons maintenant dissocier l'application d'une entreprise individuelle ou d'un propriétaire et créer une « application décentralisée » également connue sous le nom de contraction Dapp.

Un prototype d'application logicielle moderne comprend au moins une interface utilisateur (UI). Il peut s'agir d'une application mobile téléchargée à partir d'un magasin d'application, d'un site web (accessible à partir d'un ordinateur ou d'un appareil mobile) ou d'une application de bureau installée sur un ordinateur. Il s'agit généralement de données. Ces données peuvent être fournies par un seul groupe ou une seule entreprise, par exemple à

l’aide de l’application météo de l’organisation météorologique nationale oucomme dans une application de réseautage social, elles peuvent être fournies par l’utilisateur final lui-même. Enfin, c’est une sorte de manipulation ou de calcul de données.

Une Dapp utilise la blockchain au cœur de son stockage et de son traitement des données. Cela est mis en œuvre à l’aide d’un contrat intelligent. Actuellement l’interface utilisateur d’une Dapp est généralement créée en utilisant un modèle de site Web traditionnel. Nous pouvons donc penser à une Dapp comme la somme d’un site Web et d’un ou plusieurs contrats intelligents. Une Dapp possède les mêmes propriétés générales qu’une application traditionnelle. La principale différence, par conséquent, est que les données et le calcul sont fournis par la blockchain [13]. La figure 10 ci-dessous illustre la différence entre une Dapp et une application client-serveur.

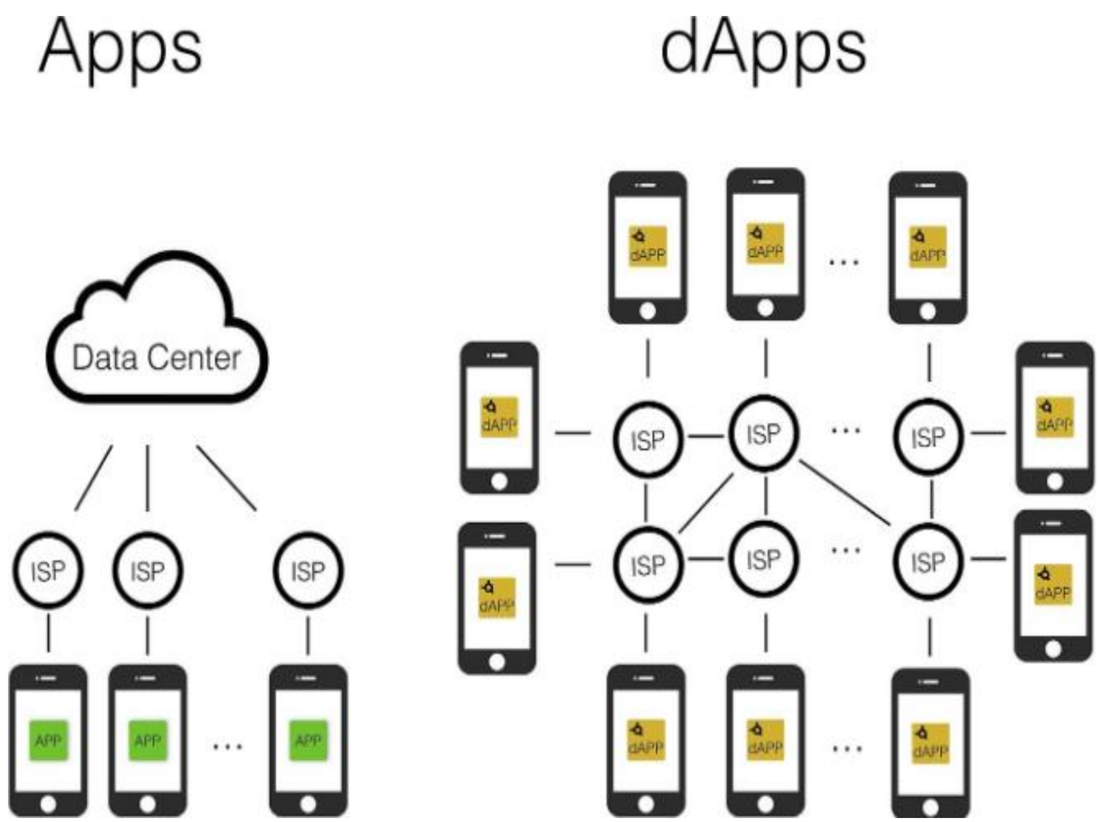

Figure 10 – La différence entre les Apps et Dapps.

Caractéristiques des Dapps

Les Dapps sont caractérisées par quatre propriétés :

- **Open Source :** En raison de la nature fiable de la blockchain, les Dapps doivent rendre leurs codes source ouverts, de sorte que les audits de tiers soient possibles.
- **Support interne de crypto-monnaie :** La monnaie interne est le véhicule qui gère l'écosystème pour une Dapp particulière. Avec des jetons, il est possible pour une Dapp de quantifier tous les crédits et transactions entre les participants du système,y compris les fournisseurs de contenu et les consommateurs.
- **Consensus décentralisé :** le consensus entre les nœuds décentralisés est le fondement de la transparence.
- **Aucun point central de défaillance :** Un système entièrement décentralisé ne devrait pas avoir de point central de défaillance puisque tous les composants des applications seront hébergés et exécutés dans la blockchain [14].

3.3 Problématique traitée dans notre travail

Comme nous l'avons vu au cours du chapitre précédent, les défis associés au déploiement de la blockchain avec tout système de soins de santé complexe incluent non seulement l'interopérabilité, mais aussi des problèmes liés à l'accès aux données et à la confidentialité. La confidentialité des données et la possibilité d'accéder à desinformations sensibles spécifiques aux patients sont l'un des principaux défis de la conception d'une application blockchain de soins de santé. La majorité des publications scientifiques tendent à explorer ce sujet. Les systèmes actuels d'administration des prestations souffrent de plusieurs limitations clés qui résultent directement de la nature centralisée des technologies de l'information sur la santé aujourd'hui. Par ailleurs, l'infrastructure informatique de santé à grande échelle existante est rigide et coûteuse à entretenir et à mettre à jour pour faire face aux changements technologiques programmatiques [15]. Nous avons par conséquent choisi de développer un systèmeblockchain permettant de contrôler les accès aux données sensibles des patients.

3.4 Description générale de notre application de contrôle d'accès aux données des patients

Dans notre système blockchain, l'application définit quel personnel de santé peut accéder à quels types de données. Le patient peut ajouter des données et donne l'autorisation pour voir et modifier ses données. Le personnel de santé peut accéder aux données (lire) et modifier les données (lire / écrire) selon l'autorisation du patient, notre but consiste à gérer le contrôle d'accès des utilisateurs.

Donc notre application web contient une interface Connexion Admin à partir de laquelle l'administrateur peut consulter son profile, ajouter un personnel de santé ou un patient et définir des rôles. L'administrateur gère également le contrôle d'accès des utilisateurs.

Notre application contient également une interface « Connexion Personnel de santé » qui contient son numéroEpmloyé (son identifiant) et son mot de passe. Le personnel de santé peut consulter son profil et ajouter les patients. Il pourra également mettre à jours les données du patient si le patient lui donne son autorisation sinon il ne peut rien écrire juste lire.

En dernier lieu, notre application contient une interface Connexion patient, à partirde laquelle, le patient consulte son profile et donne l'autorisation au personnel de santé.

Scénario d'utilisation de notre application

Dans cette sous-section, nous effectuons une visite guidée de notre application à travers un scénario d'utilisation. Pour rendre ce scénario possible, les patients, les personnels de santé et l'administrateur sont tous supposés utiliser de E-santé (c'est-à-dire qu'ils utilisent des DES). John est un patient. Lorsqu'il rend visite à son médecin Bob, il est libre de décider (donner son autorisation), en fonction de sa volonté d'accorder à Bob l'accès à ses données. Dans le cas positif, l'administrateur donne l'autorisation à Bob la permission voulue par John (Lecture-Écriture/Lecture)

- Si Bob a obtenu la permission de la lecture seule, il peut seulement voir la liste des

patients. Et consulter leurs données médicales.

- Si le personnel a la permission de la lecture/écriture, il peut voir la liste des patients comme il peut aussi ajouter des patients. Et modifier leurs données médicales.

3.5 Conception

Dans cette partie nous exposons quelques modèles de conception de notre application, représentés par les diagrammes UML : diagramme de cas d'utilisation,diagramme de séquence.

3.5.1 Diagramme de cas d'utilisation

La figure 11 suivante représente le diagramme de cas d'utilisation :

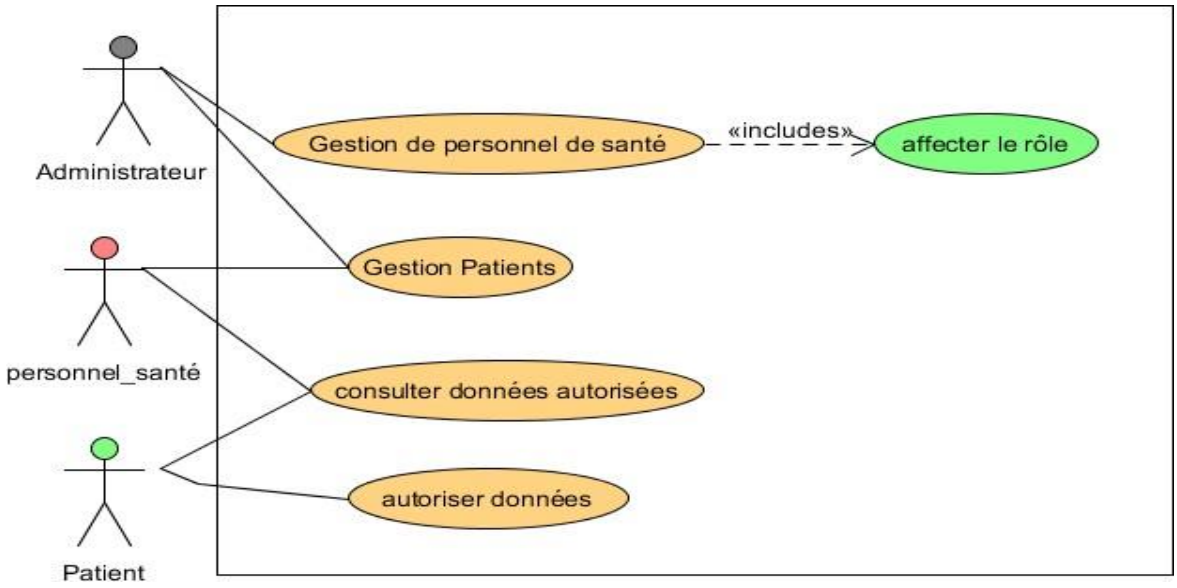

Figure 11 – Diagramme de cas d'utilisation.

- **Administrateur dans le cas d'utilisation : Gestion de Personnel de Santé**

La première phase est la création d'un contrat pour tout le personnel médical, cecontrat ne peut pas être modifié ou supprimé.

- **Administrateur dans le cas d'utilisation : Affecter les Rôles**

L'administrateur peut gérer aussi les contrôles d'accès en créant différents rôles (médecin,

infirmier, pharmacien…), et en affectant des permissions à chaque rôle (lire, écrire, lire et écrire).

●Administrateur dans le cas d'utilisation : Gestion Patients

L'administrateur peut créer un contrat pour chaque patient. Les informations des patients seront saisies en remplissant un formulaire avec des données.

●Personnel Santé dans le cas d'utilisation : Gestion patients

Tout le staff médical a l'accès aux données médicales des patientsselon des permissions et des rôles.

●Personnel Santé dans le cas d'utilisation : Consultation des donnéesautorisées

Le Personnel de santé peut consulter les contacts des patients qu'il suit, si cesmalades lui ont fourni l'autorisation d'y accéder.

●Patient dans le cas d'utilisation : Consultation des données

Le patient peut consulter ces propres donnés médicales.

●Patient dans le cas d'utilisation : Autoriser données

Le patient donne l'autorisation et l'accès à un médecin particulier pour laconsultation de ces données.

3.5.2 Diagramme de séquence

3.5.2.1 Diagramme de séquence Administrateur pour gestion de personnels de santé

L'administrateur s'authentifie et ajoute un nouveau personnel de santé par emplir un formulaire avec ses données et lui affecte un rôle donc le contrat de personnel de santé est créé et ajouter au système enfin il s'affiche dans la liste de personnel de santé.

La figure 12 ci-dessous illustre le diagramme de séquence administrateur pour la gestion de personnel de santé.

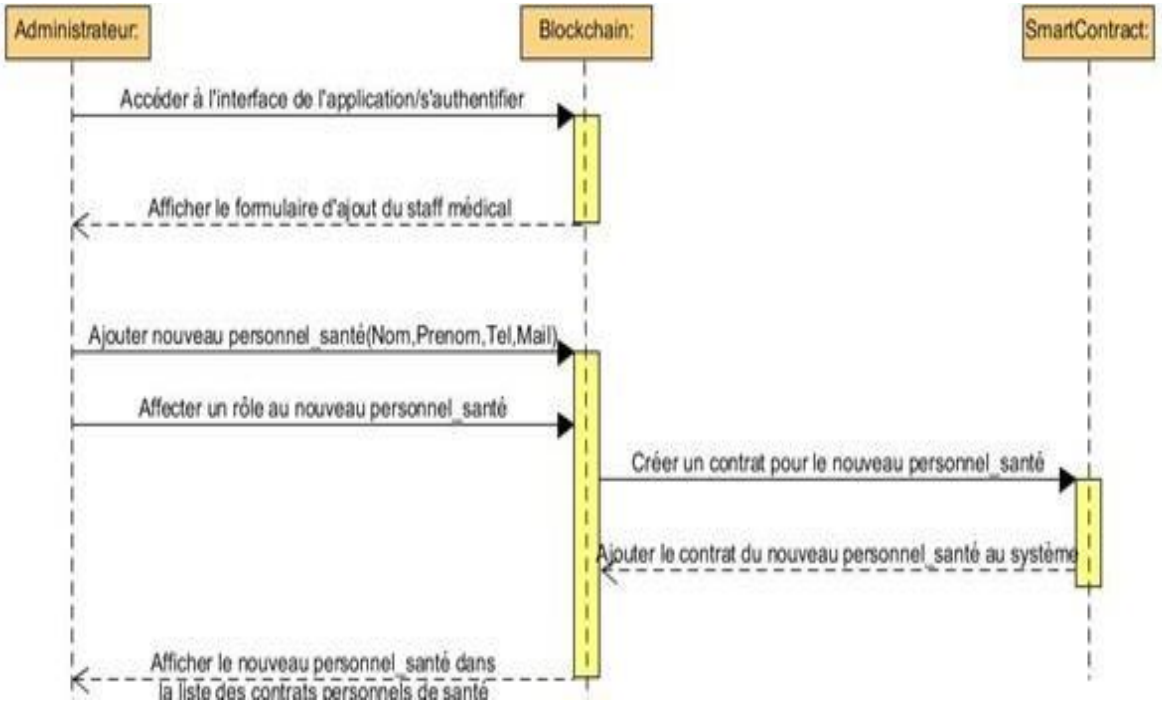

Figure 12 – Diagramme de séquence administrateur pour gestion de personnel de santé.

3.5.2.2 Diagramme de séquence Administrateur et personnel de santé pour lagestion de patient

Le personnel de santé peut ajouter un nouveau patient par remplir un formulaire par les données de ce dernier. L'administrateur affiche la liste des patient et aussi ajoute un nouveau patient dans le système et il donne la permission au personnel de santé (lecture /écriture ou lecture) par rapport à des patients donc le contrat est créé et la liste de nouveaux patients s'affiche dans le système.

La figure 13 ci-dessous illustre diagramme de séquence, administrateur pour la gestion depatient et personnel de santé pour gestion de patient.

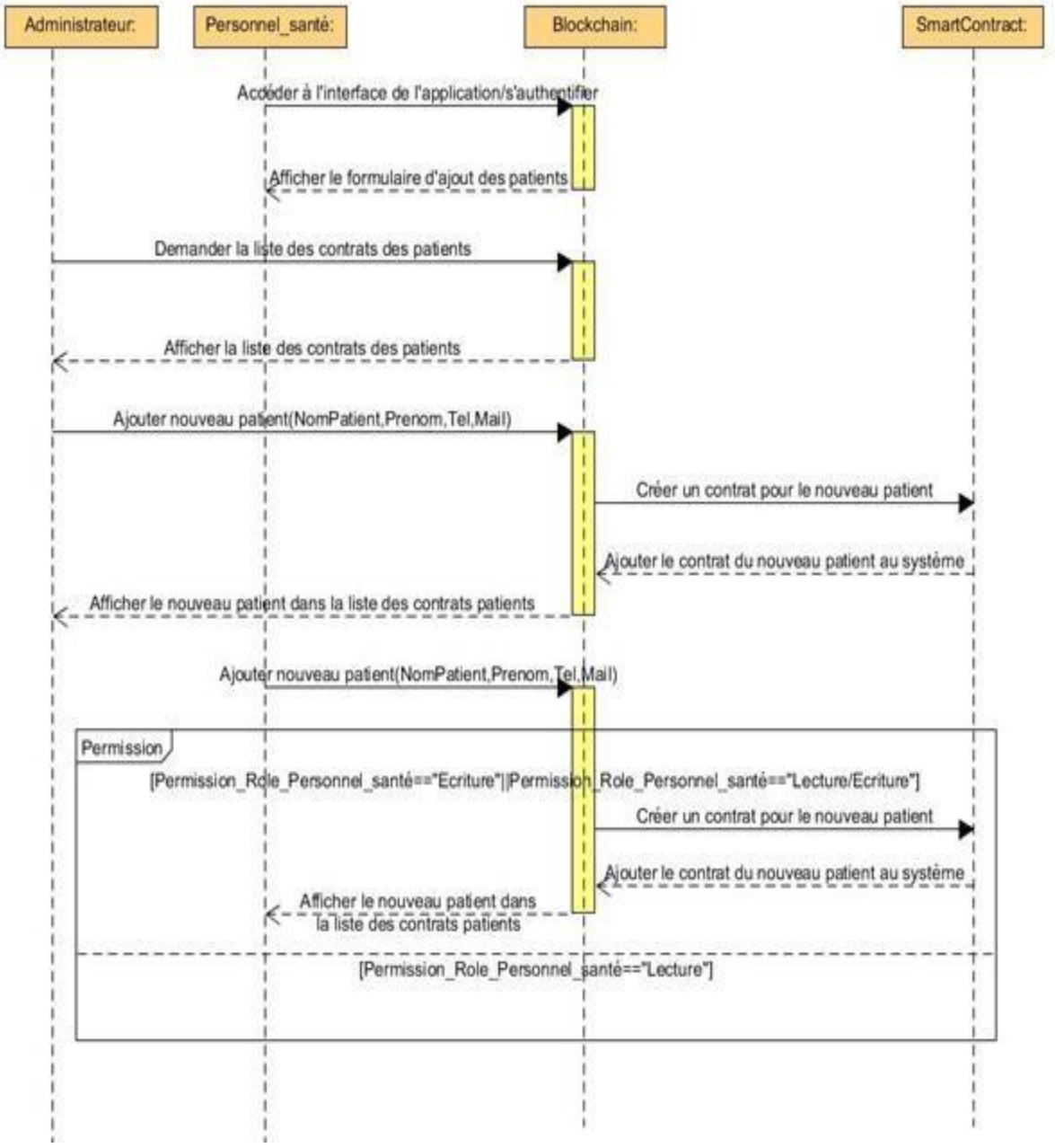

Figure 13 – Diagramme de séquence administrateur et personnel de santé pour la gestion de patient.

3.5.2.3 Diagramme de séquence Administrateur pour affecter les rôles

L'administrateur s'authentifie, il aura un formulaire d'ajout de rôle, il affecte un nouveau rôle et s'affiche dans la liste de personnel de santé dans la case rôle.

La figure 14 ci-dessous illustre le diagramme de séquence, administrateur affecte les rôles.

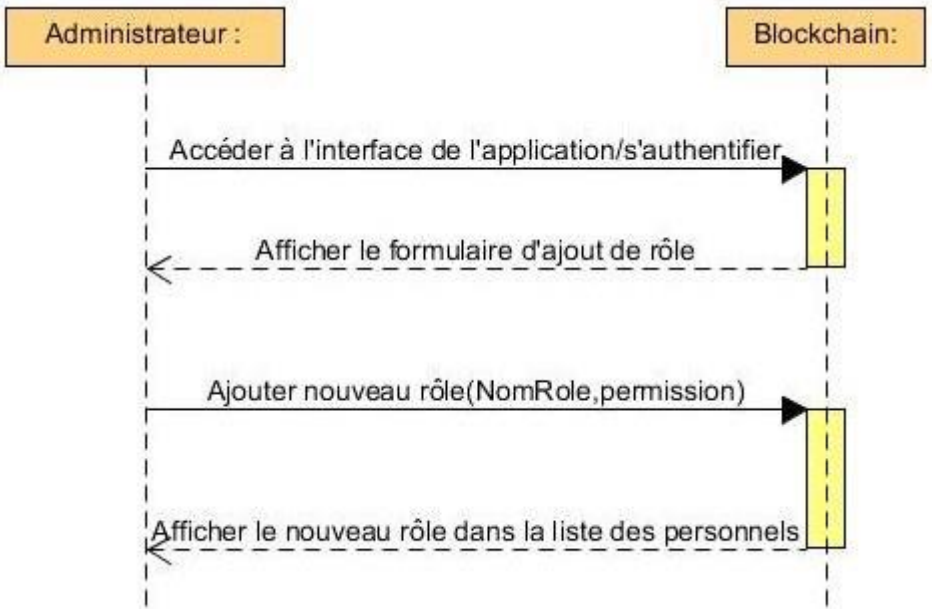

Figure 14 – Diagramme de séquence administrateur pour affecte les rôles.

3.5.2.4 Diagramme de séquence Demande l'autorisation d'accès et Consultation des données

Le personnel de santé s'authentifie puis s'affiche la liste des patients et il sélectionne un patient donc le personnel de santé demande l'autorisation du patient si le patient lui donne l'autorisation alors ses informations s'affichent et le personnel de santé peut les consultés.

La figure 15 ci-dessous illustre le diagramme de séquence, demande l'autorisationet consultation des données.

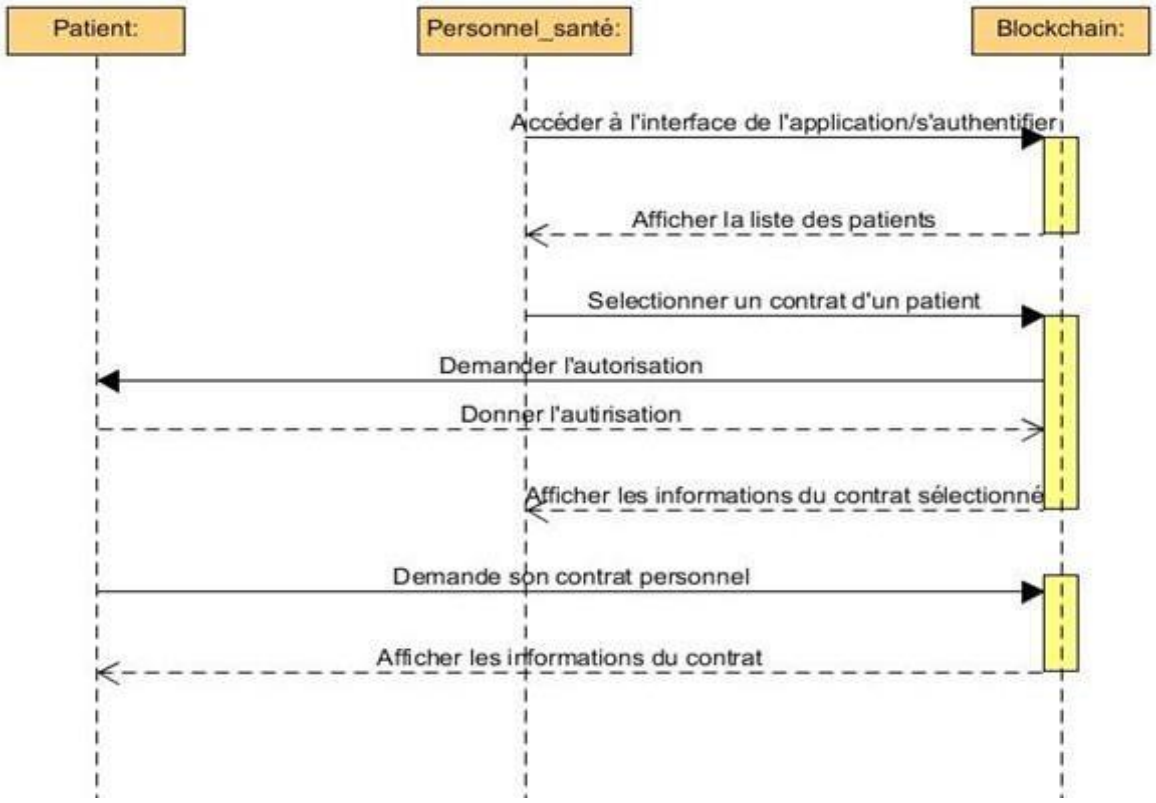

Figure 15 – Diagramme de séquence demande de l'autorisation et consultation desdonnées.

3.6 Conclusion

Le service de santé est différent des autres services et doit respecter des règles de confidentialité particulièrement strictes. Afin de jouer un rôle dans le secteur de la santé,la blockchain doit d'abord assurer la protection et l'anonymat des données des patients. Lors de ce chapitre, nous avons présenté notre proposition de solution au problème de contrôle d'accès aux données médicales des patients, dans un système de e-santé. Lors du prochain chapitre, nous allons aborder la partie implémentation et discuter de notre proposition.

Chapitre 4

Implémentation

4.1 Introduction

Après avoir lors du chapitre précédent présenté la conception de notre application décentralisée de gestion de contrôle d'accès aux données médicales, basée sur la technologie Blockchain. Nous allons dans celui qui suit donner une brève description des outils que nous avons utilisés lors de l'implémentation de notre solution, ainsi que les différentes fonctionnalités de celle-ci.

4.2 Généralités sur Ethereum

Ethereum est une plate-forme blockchain mondiale et open-source pour les applications décentralisées (Dapps). Elle est alimentée par des contrats intelligents et intègre une cryptomonnaie native, l'ether (ETH). Sur Ethereum, du code peut être écrit pour contrôler la transmission de la valeur numérique basée sur des conditions programmables.

Ethereum a été conceptualisé à travers un livre blanc publié en Novembre 2013 par VitalikButerin, et avec des contributions supplémentaires de ses sept co-fondateurs et d'autres développeurs, le réseau a été lancé en Juin 2015. Le développement initial a été dirigé par Ethereum Switzer land, cependant, depuis la dissolution de celle-ci il estactuellement supervisé par la fondation ethereum; une organisation à but non lucratif basée en Suisse[16].

4.3 Solidity

Solidity est un langage de haut niveau orienté objet pour la mise en œuvre de contrats intelligents. Il a été influencé par C++, Python et Javascript et est conçu pour s'exécuter dans une machine virtuelle Ethereum (EVM).

Solidity est statiquement typé, supporte l'héritage, les bibliothèques et les types complexes définis par l'utilisateur entre autres fonctionnalités. Avec Solidity, nous pouvons créer des contrats pour des utilisations telles que le vote, le financement participatif, les enchères aveugles et les portefeuilles à plusieurs fournisseurs[16].

4.4 Angular

Angular est un Framework de conception d'applications et une plate-forme de développement pour créer des applications simples efficaces et sophistiquées. La figure 16 ci-dessous illustre la version de Angular CLI.

Figure 16 – Version de Angular CLI.

4.5 Web 3 (Ethereum JavaScript API)

Web 3.0 est un concept qui propose essentiellement un Web sémantique et intelligent comme une évolution de la technologie Web 2.0 existante. Telle est la vision d'un écosystème dans lequel les personnes, les applications, les données et le Web sont tous connectés et

peuvent interagir de manière intelligente. Avec l'avènement de la technologie Blockchain, une idée du Web décentralisé a également émergé, ce qui était en fait la vision originale d'Internet. L'idée centrale est que tous les principaux services, tels que le DNS, les moteurs de recherche et l'identitésur Internet, seront décentralisés dans le Web 3.0. C'est là qu'Ethereum est envisagé comme une plate-forme pouvant aider à concrétiser cette vision[17].

4.6 Installation des outils de développement et configurationde l'environnement

Tout d'abord, nous allons installer et configurer une blockchain privée pour développer un smart contract localement.

4.6.1 Ganache

Ganache est une blockchain personnelle pour le développement rapide d'applications distribuées. Cela nous permettra de déployer un smart contract. Ganache peut fournir 10 comptes Ethereum avec une balance de 100 ether (du faux ether) pour chaque compte et c'est la raison pour laquelle nous avons choisi de l'utiliser. La figure 17 ci-dessous illustre Ganache.

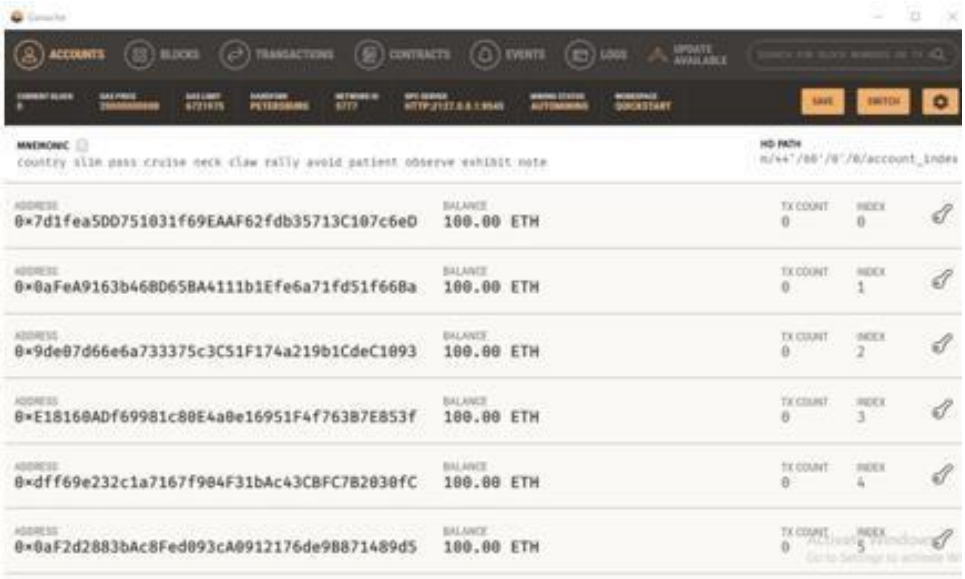

Figure 17 – Ganache.

4.6.2 Node.js

Node.js est un système logiciel côté serveur, conçu pour écrire des applications Internet évolutives, notamment les serveurs Web. Nous aurons besoin de Node Package Manager (NPM) fourni par Node.js

4.6.3 Truffle

C'est un environnement de développement de classe mondiale, cadre de test et pipeline d'actifs pour les chaînes de blocs en utilisant la machine virtuelle Ethereum (EVM), visant à rendre la vie en tant que développeur plus facile.

Truffle offre de nombreuses fonctionnalités :

- Compilation, liaison, déploiement et gestion binaire de contrats intelligents intégrés ;
- Tests de contrats automatisés pour un développement rapide ;
- Scriptable, extensible déploiement & migrations Framework ;
- Gestion de réseau pour le déploiement sur de nombreux réseaux publics et privés ;
- Gestion de paquets avec Ethpm et NPM, en utilisant la norme ERC19 ;
- Console interactive pour la communication contractuelle directe ;
- Pipeline de construction configurable avec support pour une intégration serrée ;
- Gestionnaire de scripts externes qui exécutent des scripts dans un environnement Truffle.

Pour installer le Framework Truffle :

```
npm install -g truffle
```

4.6.4 Metamask

Metamask est un navigateur Ethereum et portefeuille Ether. Il interagit avec EthereumDapps via le biais du navigateur sans exécuter un nœud Ethereum complet.

La plupart des dApps doivent installer le client Ethereum ou utiliser MetaMask. La figure 18 ci-dessous montre une capture de l'interface de MetaMask.

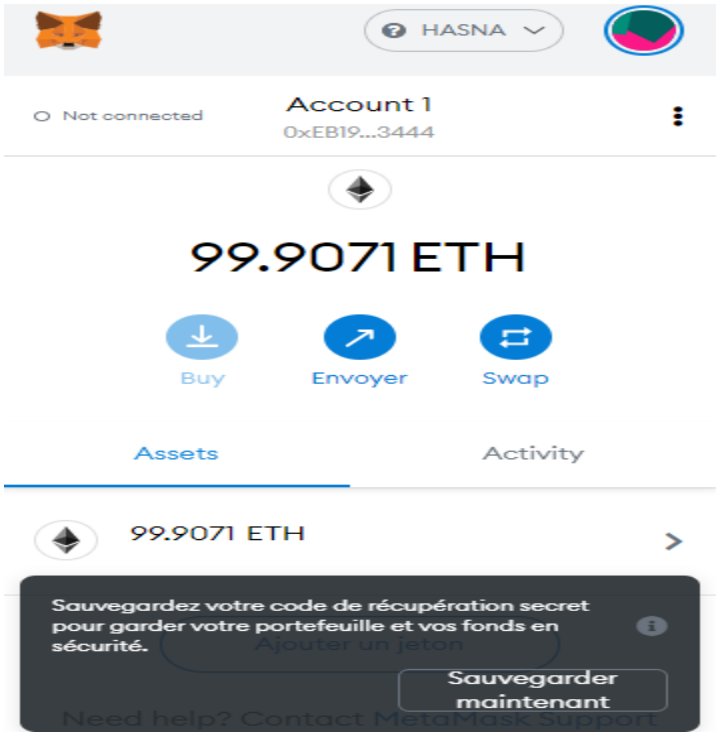

Figure 18 – Metamask.

4.6.5 Visual Studio Code

C'est un éditeur de code multiplateforme édité par Microsoft. Cet outil destiné aux développeurs supporte plusieurs dizaines de langages de programmation comme le HTML, C++, PHP, Javascript, Markdown, CSS, etc. Il intègre plusieurs outils facilitant lasaisie de code par les développeurs comme la coloration syntaxique ou encore le système d'auto-complétion IntelliSense. En outre, l'outil permet aux développeurs de corriger leur code et de gérer les différentes versions de leurs fichiers de travail puisqu'un module de débogage est aussi de la partie. La figure 19 ci-dessous représente son interface.

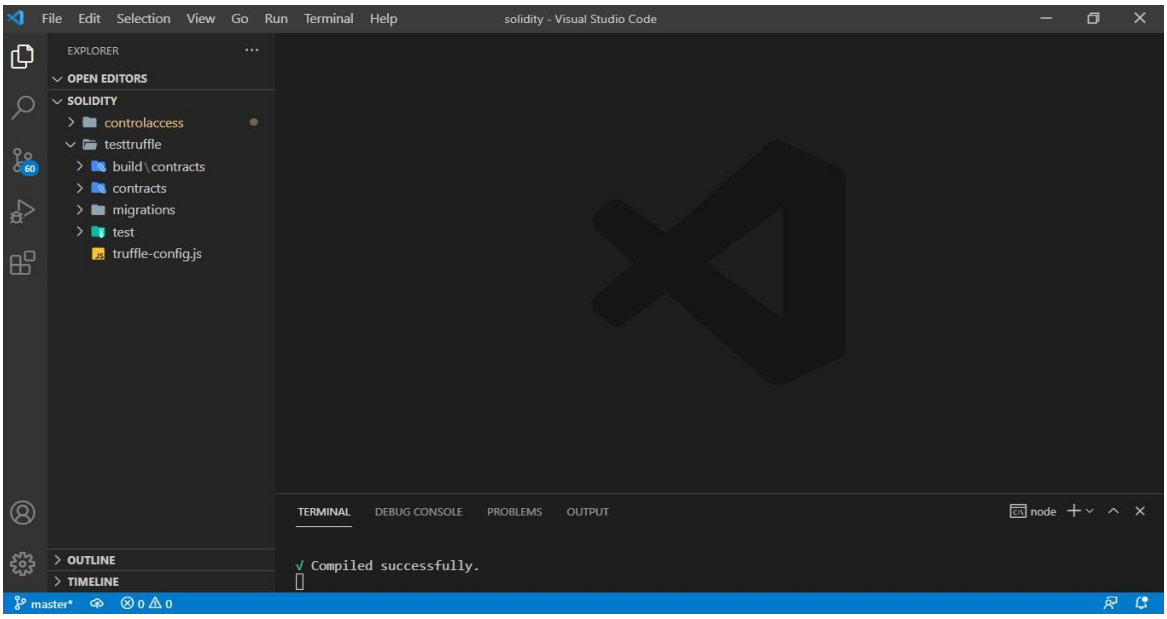

Figure 19 – Outil Visual Studio Code.

4.7 Back-end

Dans cette section nous allons créer nos smart contracts et les déployer

4.7.1 Les smarts contracts

Nous avons créé trois smart contracts

4.7.1.1 Smart contract administrateur

La figure 20 ci-dessous illustre une partie du code du smart contract pour l'administrateur.

```
pragma solidity >=0.4.22 <0.9.0;
/*d'encoder et de décoder arbitrairement des tableaux et des
structures imbriqués.Il produit un code moins optimal*/
pragma experimental ABIEncoderV2;
//notre contrat pour l'administrateur//
contract Administrateur{
        string idAdmin;
        uint256 telAdmin;
        string nomAdmin;
        string prenomAdmin;
        string mailAdmin;
        string motpassAdmin;
//declaration de structure pour les roles
struct Role_Struct {
        string typeRole;
        string permission;
    }
mapping(string => Role_Struct)Role;
string[] public listRole;
```

Figure 20 – Code de smart contract administrateur.

La figure 21 ci-dessous illustre la fonction infoAdministrateur pour ajouter les informations principales de l'administrateur.

```
function infoAdministrateur(
  string memory _idAdmin,
  uint256  _telAdmin,
  string memory _nomAdmin,
  string memory _prenomAdmin,
  string memory _mailAdmin,
  string memory _motpassAdmin
) public {
idAdmin = _idAdmin;
telAdmin = _telAdmin;
nomAdmin = _nomAdmin;
prenomAdmin = _prenomAdmin;
mailAdmin = _mailAdmin;
motpassAdmin = _motpassAdmin;
}
```

Figure 21 – Code fonction infoAdministrateur.

4.7.1.2 Smart contract personnels de santé

La figure 22 ci-dessous illustre smart contract pour le personnel de santé

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;
/*d'encoder et de décoder arbitrairement des tableaux et des
structures imbriqués.Il produit un code moins optimal*/
pragma experimental ABIEncoderV2;
/*notre contrat pour le Personnels du sante*/
contract Personnelssante{
struct Personnelsante {
        uint256 idPersonnelsante;
        uint256 telPersonnelsante;
        string rolePersonnelsante;
        string nomPersonnelsante;
        string prenomPersonnelsante;
        string addressPersonnelsante;
        string mailPersonnelsante;
        string motpassPersonnelsante;
        address createurPersonnelsante;
    }
    struct liste_Numero_Personnelsante{
    uint256 NumeroPersonnelsante;
    uint256 idPersonnelsante;
```

Figure 22 – Code smart contract personnel de santé.

La figure 23 ci-dessous illustre la fonction setNewPersonnelsante pour ajouter les informations principales de chaque Personnel médical.

```
function setNewPersonnelsante(
    uint256  _idPersonnelsante,
    string memory _rolePersonnelsante,
    string memory _nomPersonnelsante,
    string memory _prenomPersonnelsante,
    string memory _addressPersonnelsante,
    string memory _mailPersonnelsante,
    string memory _motpassPersonnelsante,
    uint256 _telPersonnelsante,
    address _createurPersonnelsante

) public {   nombrePersonnelsante = listPersonnelsante.length + 1;

    Personnelsante_Struct[_idPersonnelsante].idPersonnelsante = _idPersonnelsante;
    Personnelsante_Struct[_idPersonnelsante].rolePersonnelsante = _rolePersonnelsante;
    Personnelsante_Struct[_idPersonnelsante].nomPersonnelsante = _nomPersonnelsante;
    Personnelsante_Struct[_idPersonnelsante].prenomPersonnelsante = _prenomPersonnelsan
    Personnelsante_Struct[_idPersonnelsante].addressPersonnelsante = _addressPersonnels
    Personnelsante_Struct[_idPersonnelsante].telPersonnelsante = _telPersonnelsante;
    Personnelsante_Struct[_idPersonnelsante].mailPersonnelsante = _mailPersonnelsante;
    Personnelsante_Struct[_idPersonnelsante].motpassPersonnelsante = _motpassPersonnels
    Personnelsante_Struct[_idPersonnelsante].createurPersonnelsante = _createurPersonne
```

Figure 23 – Code fonction SetNewPersonnelsanté.

4.7.1.3 Smart contract patient

La figure 24 ci-dessous illustre le smart contract pour le patient.

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;
/*d'encoder et de décoder arbitrairement des tableaux et des
structures imbriqués.Il produit un code moins optimal*/
pragma experimental ABIEncoderV2;
/*notre contrat pour le patient*/
contract Patients{
/*Structure pour le patient pour identifier propre infos &
dans la structure melange des attributs (string,unit) que vs voulez*/
    struct bloc_Patient {
        uint256 idPatient;
        uint256 telPatient;
        string nomPatient;
        string prenomPatient;
        string sexePatient;
        string adressePatient;
        string maladiePatient;
        string mailPatient;
        string motpassPatient;
        address createurPatient;
    }
```

Figure 24 – Code smart contract patient.

La figure 25 ci-dessous montre la fonction SetNewPatient pour ajouter les informations principales de chaque Patient.

```
/*On a crée la fonction pour ajouter les
informations principales de chaque Patient .*/
    function setNewPatient(
      string memory _nomPatient,
      string memory _prenomPatient,
      string memory _sexePatient,
      string memory _adressePatient,
      string memory _maladiePatient,
      uint256 _telPatient,
      string memory _mailPatient,
      string memory _motpassPatient,
      address _createurPatient
   ) public {
nombrePatient = listPatient.length + 1;

Patient_Struct[_mailPatient].idPatient = nombrePatient;
Patient_Struct[_mailPatient].nomPatient = _nomPatient;
Patient_Struct[_mailPatient].prenomPatient = _prenomPatient;
Patient_Struct[_mailPatient].sexePatient = _sexePatient;
Patient_Struct[_mailPatient].adressePatient = _adressePatient;
Patient_Struct[_mailPatient].maladiePatient = _maladiePatient;
Patient_Struct[_mailPatient].telPatient = _telPatient;
Patient_Struct[_mailPatient].mailPatient = _mailPatient;
```

Figure 25 – Code fonction SetNewPatient.

4.7.2 Déploiement des smart contract

La première étape consiste en la migration de nos trois smart contract vers la blockchainlocale en utilisant la commande :

- truffle migrate --compile-all --reset --network development

Voici le résultat :

La figure 26 ci-dessous illustre la migration de nos trois smart contract vers lablockchain locale.

```
C:\Users\HP\Desktop\solidity\testtruffle>truffle migrate --compile-all --reset --network development

Compiling your contracts...
===========================
> Compiling .\contracts\Administrateur.sol
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Patients.sol
> Compiling .\contracts\Personneslsante.sol
> Compilation warnings encountered:
```

Figure 26 – migration des smart contract.

4.7.2.1 Déploiement de Smart contract administrateur

La figure 27 ci-dessous illustre le déloiment du smart contract « Administrateur ».

```
2_Administrateur.js
===================

   Replacing 'Administrateur'
   --------------------------
   > transaction hash:    0x9f8cf834e3b285405c13d39329a37b1ced3b0134ab3dc1b69fd2fe987bf5c8ac
   > Blocks: 0            Seconds: 0
   > contract address:    0x4513Ed6b108EE36d938cad6818A9AEfd9bAa556C
   > block number:        3
   > block timestamp:     1622061751
   > account:             0xEB19AA9Ef230914B4E215Ea7c0307C9803Ad3444
   > balance:             99.97463938
   > gas used:            1033750 (0xfc616)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.020675 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.020675 ETH
```

Figure 27 – Déploiement smart contract administrateur.

4.7.2.2 Déploiement du Smart contract personnels santé

La figure 28 ci-dessous illustre le déploiement du smart contract de personnel de santé.

```
4_Personneslsante.js
====================

   Replacing 'Personnelssante'
   ---------------------------
   > transaction hash:    0x580f612a9ed6313090ac77b04677f09b3e06a93d030e3d6eafbed87053b1e222
   > Blocks: 0            Seconds: 0
   > contract address:    0xF371121Bbb0dd3e0f5Dbcd57DF543774d4b8cCA6
   > block number:        7
   > block timestamp:     1622061755
   > account:             0xEB19AA9Ef230914B4E215Ea7c0307C9803Ad3444
   > balance:             99.90768158
   > gas used:            1386176 (0x1526c0)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.02772352 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.02772352 ETH
```

Figure 28 – Déploiement smart contract personnel de santé.

4.7.2.3 Déploiement de Smart contract patient

La figure 29 ci-dessous illustre le déploiement de smart contract du patient.

```
3_Patients.js
=============

   Replacing 'Patients'
   --------------------
   > transaction hash:    0x14b06701767e510ab7757ad620bcf46c72c07fe81b9da996d9073bdaa366fc5f
   > Blocks: 0            Seconds: 0
   > contract address:    0xe83c12Db6052a98781982FF858F936198c6f0Bae
   > block number:        5
   > block timestamp:     1622061753
   > account:             0xEB19AA9Ef230914B4E215Ea7c0307C9803Ad3444
   > balance:             99.93595186
   > gas used:            1907038 (0x1d195e)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.03814076 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.03814076 ETH
```

Figure 29 – Déploiement smart contract patient.

4.7.2.4 Le coût total

La figure 30 ci-dessous illustre le déploiement total et le coût total en ether.

Figure 30 – Déploiement total et le coût total.

Comme le montre les résultats de la migration, le coût total de cette transactionest de 0.09037814 ether, ce qui est l'équivalent de 215.24 $ et 28704.4 DA. Cetteconversion est faite le 31/05/2021. Nous avons défini le prix de gas a 20Gwei ce qui équivaut à 0.000000002 ether. Après la migration des smart contract, nous allons lancer un serveur virtuel en local à l'aide du Framework truffle qui contient l'application côté client.

4.8 Front-end

La figure 31 ci-dessous illustre la Page d'accueil pour la connexion de l'administrateur, du personnel de santé ou du patient.

Figure 31 – Interface connexion pour l'administrateur. La figure 32 ci-dessous illustre la Page connexion de l'administrateur.

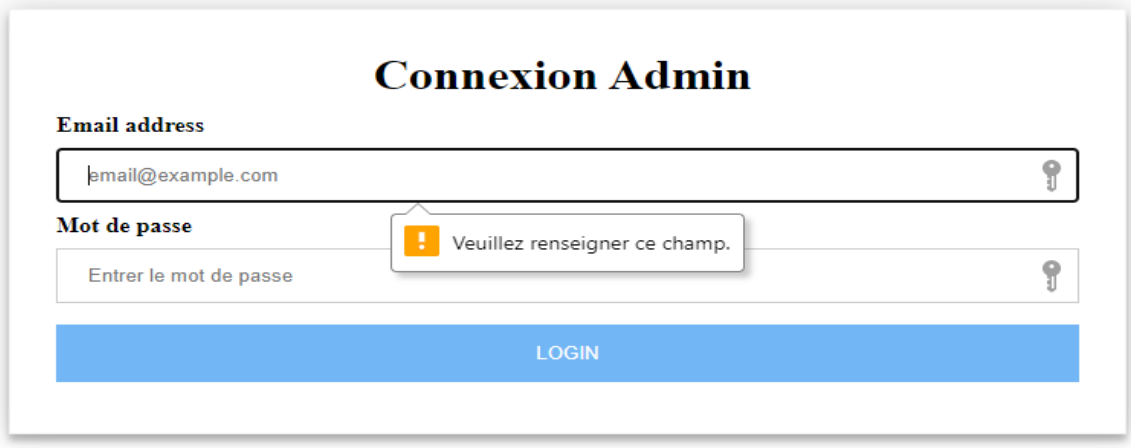

Figure 32 – Interface Connexion Admin.

A l'aide de l'interface connexion admin, l'administrateur peut consulter son profil et ajouter un personnel de santé, un patient ou un rôle, comme il peut gérer le contrôle d'accès de chaque utilisateur.

❖ **Ajouter Patient:**

La figure 33 ci-dessous illustre la Page ajouter patient par l'administrateur.

Figure 33 – Interface formulaire Ajouter patient.

❖ **Ajouter Personnel de santé**

La figure 34 ci-dessous illustre la Page ajouter personnels de santé par l'admin.

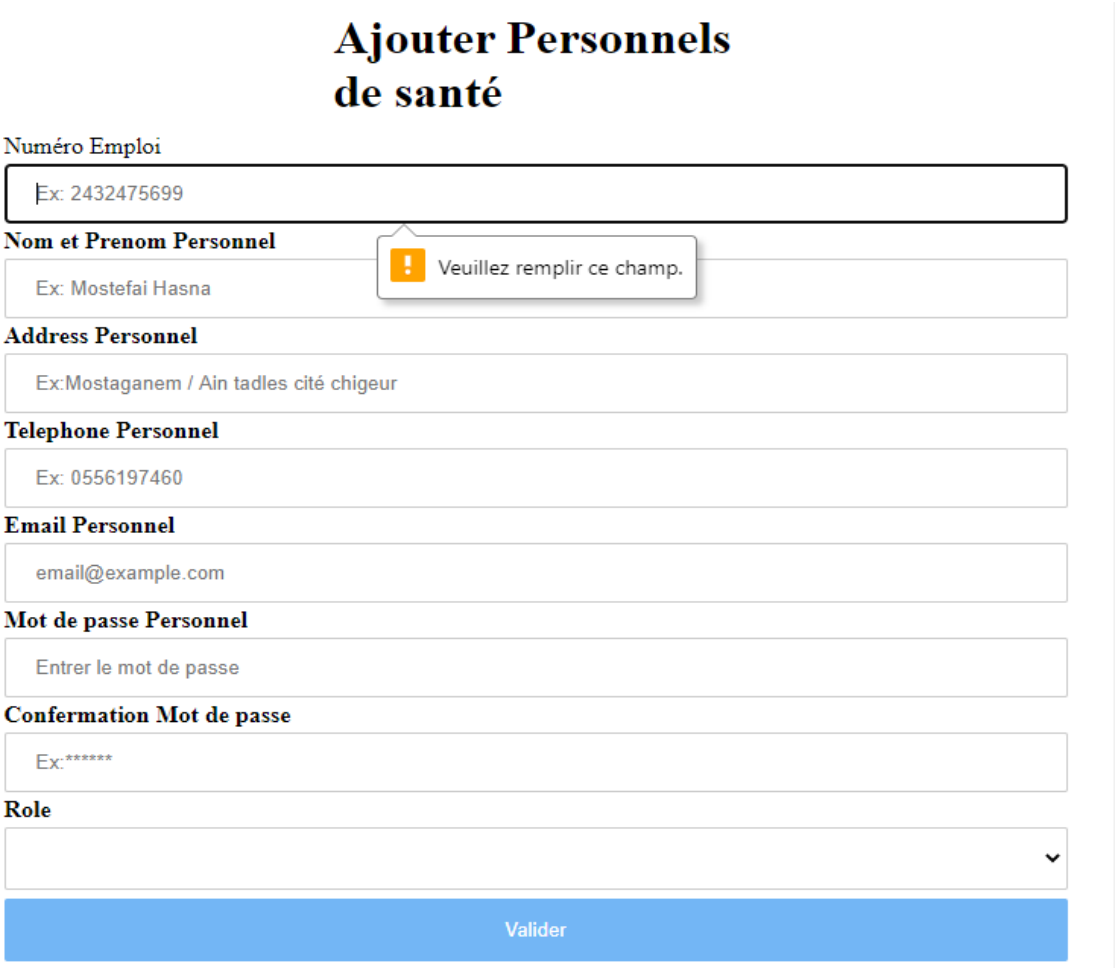

Figure 34 – Interface formulaire Ajouter personnels de santé.

❖ **Ajouter rôles**

La figure 35 ci-dessous illustre la Page ajouter rôle par l'administrateur.

Figure 35 – Interface Ajouter les rôles par l'administrateur.

La figure 36 ci-dessous illustre la Page connexion personnels de santé.

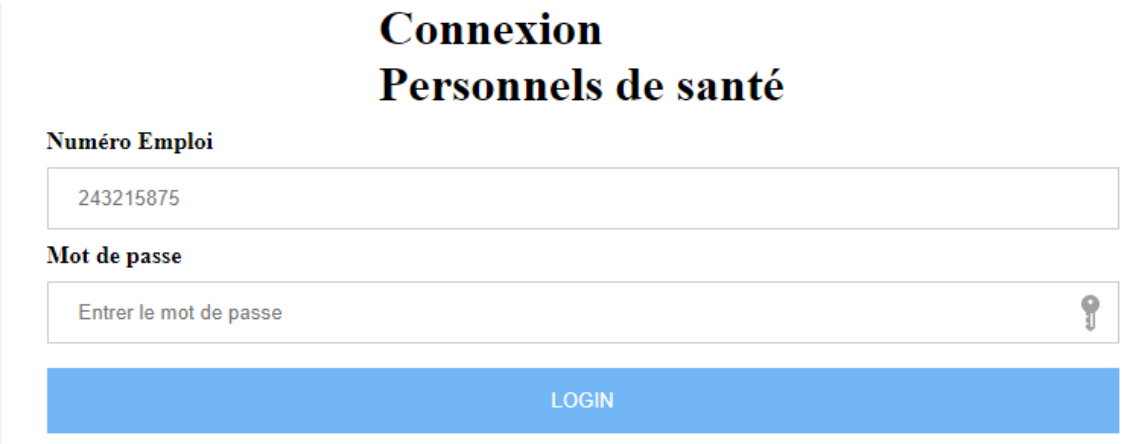

Figure 36 – Interface de Connexion personnels de santé.

4.9 Discussion de notre solution

Après avoir présenté notre application et ses différentes interfaces, la partie quiva suivre est consacrée à discuter de notre solution de contrôle d'accès au données médicales via Blockchain.

Question 1 : Comment enregistrer chaque nouvel utilisateur dans la blockchain via des smart contrat ?

Chaque acteur, géré par la Blockchain, doit créer ou établir un contrat intelligent pour s'enregistrer. Dans ce contrat intelligent, plusieurs informations seront spécifiées à savoir l'identité de l'acteur (par exemple administrateur, personnel santé, patient...), ses attributs et les règles d'accès dans le cas d'une ressource. Cette étape nécessite la création d'une transaction à chaque fois qu'un acteur doit rejoindre le réseau ou mettre à jour ses informations d'identité.

Question 2 : Comment se passe la demande d'accès aux données ?

L'entité se voit autorisé l'accès une fois vérifiés ses attributs et les règles d'accès.

Ce mécanisme bénéficie des avantages combinés de la technologie Blockchain suivants :

1. Les entités n'ont pas besoin de se connaître et leur confiance est établie au moyen de la blockchain.
2. La blockchain fournit une autorisation précise et offre une méthode très flexible pour fournir un accès basé sur l'évaluation des attributs.

Question 3 : Quelles sont les contraintes pour utiliser notre application dans un environnement réel ?

Pour utiliser notre application dans un environnement réel, il est nécessaire de se procurer des ethers afin de couvrir les frais de déploiement du contrat intelligent, ainsi que l'accès de control (frais de transaction) Comme nous l'avons illustré plus haut.

Question 5 : Quelle est la raison pour laquelle vous avez choisi l'outil Metamask et le framework Truffle ?

Nous avons choisi Metamask car il permet également la gestion des comptes blockchain, ainsi que les fonds Ether pour payer les transactions.

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 côté client de notre Smart contrat, etenfin de le déployer dans n'importe quel réseau Ethereum.

Question 6 : Quelles sont les limites de notre application ?

L'une des principales limites de notre application est le fait que la blockchain est en local.

De plus, nous avons besoin d'Ether pour déployer nos contrats intelligents, ce qui rends son utilisation onéreuse et rédhibitoire pour certains. Cependant les bénéfices de sonutilisation pourraient être supérieures.

Question 7 : Quelles sont les améliorations futures possibles pour notre application ?

- Relier notre application web avec des objets connectés dans des hôpitaux ou chez les particuliers d'une manière sécurisée et contrôlée. Pour faciliter l'assemblage des données médicales des patients.
- Ajouter un deuxième facteur d'authentification pour l'utilisateur (admin, personnel santé, patient). Ceci permettra d'ajouter plus de sécurité dans l'application.

4.10 Conclusion

Dans ce chapitre nous avons abordé la problématique de gestion du contrôle d'accès aux données médicales basée sur le système Blockchain , Nous avons proposé notre solution pour assurer la sécurité du partage des informations des patients entre les différents acteurs . Nous avons implémenté notre solution qui est un Smart contrat et une application côté client en local puis nous avons déployé notre smart contrat dans un réseaude test. Ensuite nous avons discuté de notre application et apporté des réponses à des interrogations possibles.

Conclusion Générale

La blockchain a apporté beaucoup de nouveaux concepts et d'idées dans le domaine de la recherche. Elle a aussi prouvé son efficacité en matière de sécurité et de décentralisation dans différents secteurs d'application dans le monde.

L'informatisation du secteur médical est une étape nécessaire et d'une importance primordiale pour rationaliser la gestion, valoriser et améliorer la qualité, la sécurité ainsi que la prise en charge des patients qui auront de plus en plus confiance dans le système desanté national.

Dans cette démarche, notre travail a consisté à étudier la technologie Blockchain etles smart contract ainsi que la plateforme Ethereum et à réaliser un système de contrôle d'accès pour l'amélioration de la sécurisation des soins et du partage de l'information entreacteurs de ce système.

L'application que nous avons conçue et développée au cours de ce travail est une application décentralisée en tous sens : le réseau est décentralisé présent en peer to peer et les données sont décentralisées.

Nous avons développé et déployé un smart contract dans la plateforme Ethereum qui assure la protection des données des patients et établit les règles d'accès aux données de celui-ci, selon certains Scritères et nous avons aussi développé une interface graphique.Nous avons effectué des tests en local à l'aide du Framework Truffle et mais également après le déploiement de notre Smart contract dans une Blockchain réel de test.

A titre d'amélioration de notre application décentralisée de E-Santé, deux point ontété marqués :

1. Relier notre application web basée sur la blockchain avec des objets connectés dans des hôpitaux ou bien chez des particuliers afin de collecter les données directement et les inscrire dans la base de données.

2. Augmenter la sécurité de notre application en termes de connexion enajoutant d'autre facteurs d'authentification en plus des mots de passes.

Pour conclure, Nous dirons que la recherche sur les applications de la blockchain n'en est encore qu'a ces prémisses, et nous estimons qu'elle pourrait apporter de grand bénéfices à la société dans les prochaines années.

Bibliographie

[1] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », p. 9.

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Illustrated edition. Princeton: Princeton University Press, 2016.

[3] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, « Blockchain in healthcare and health sciences—A scoping review », *Int. J. Med. Inf.*, vol.134, p. 104040, févr. 2020, doi: 10.1016/j.ijmedinf.2019.104040.

[4] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, « A blockchain-based approach to health information exchange networks », in *Proc. NIST Workshop BlockchainHealthcare*, 2016, vol. 1, nº 1, p. 1-10.

[5] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, « FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data », *Comput. Struct. Biotechnol. J.*, vol. 16, p. 267-278, janv. 2018, doi: 10.1016/j.csbj.2018.07.004.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, « Integrating blockchain for data sharing and collaboration in mobile healthcare applications », in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, oct. 2017, p. 1-5. doi: 10.1109/PIMRC.2017.8292361.

[7] « Hyperledger – Open Source Blockchain Technologies ». https://www.hyperledger.org/ (consulté le juin 12, 2021).

[8] « Exonum: Build trust into business with blockchain technology ». https://exonum.com/index (consulté le juin 12, 2021).

[9] I. O. Zolotovskii and D. I. Sementsov, « Dynamics of wave packets in fibres with amplification and inhomogeneous distribution of dispersion parameters », *Quantum Electron.*, vol. 34, nº 9, p. 852, sept. 2004, doi: 10.1070/QE2004v034n09ABEH002669.

[10] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, « MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain », *J. Med. Syst.*, vol. 42, nº 8, p. 136, juin 2018, doi: 10.1007/s10916-018-0993-7.

[11] « Distributed Applications and Interoperable Systems - 17th IFIP WG 6.1 International Conference, DAIS 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Techniques, DisCoTec 2017, Neuchâtel, Switzerland, June 19–22, 2017, Proceedings | Lydia Y. Chen | Springer ».

[12] A. Zhang and X. Lin, « Towards secure and privacy-preserving data sharing in e- health systems via consortium blockchain », *J. Med. Syst.*, vol. 42, nº 8, p. 1-18, 2018.

[13] W. Metcalfe, « Ethereum, Smart Contracts, DApps », in *Blockchain and Crypt Currency*, Springer, Singapore, 2020, p. 77-93.

[14] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, « Decentralized Applications: The Blockchain-Empowered Software System », *IEEE Access*, vol. 6, p. 53019-53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[15] « Blockchain research in healthcare: a bibliometric review and current research trends | SpringerLink ». https://link.springer.com/article/10.1007/s42488-021-00046-2 (consulté le juin 12, 2021).

[16] « Solidity — Solidity 0.8.5 documentation ». https://docs.soliditylang.org/en/v0.8.5/ (consulté le juin 12, 2021).

[17] I. Bashir, *Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks*. Packt Publishing, 2017.