REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre :RTIC05/M2/2021

Mémoire

Présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : **Réseaux et Technologies de l'Information et de la Communication (RTIC)**

Blockchain pour gestion des données médicales

Par :
ZOUAOUI RANIA

Soutenu le.../../…. devant le jury composé de :

Nom Prénom	grade	Président
Aloui Ahmed	MCB	Rapporteur
Nom Prénom	grade	Examinateur

Année universitaire 2020-2021

Résumé

Les dossiers de santé électroniques (DSE) sont des informations privées cri tiques et très sensibles dans le domaine des soins de santé et doivent être fréquemment partagés entre pairs.

La blockchain est une base de données partagée qui permet de créer la confiance entre individus sans tiers. Il fournit un historique partagé, immuable et transparent de toutes les transactions pour créer des applications fiables, responsables et transparentes. Cela offre une opportunité unique de développer un système de gestion et de partage des données (DSE) sécurisé et fiable en utilisant la blockchain. L'objectif de ce projet est de proposer un système simple basé sur la blockchain pour la gestion des données médicales.

Mots-clés : Blockchain, Santé, Dossier de santé électroniques DSE, Contrats intelligents

Abstract

Electronic health records (EHRs) are critical and highly sensitive private health care information and must be shared frequently among peers.

Blockchain is a shared database that creates trust between individuals without a third party. It provides a shared, immutable and transparent history of all transactions to create trusted, accountable and transparent applications. This provides a unique opportunity to develop a secure and reliable data management and sharing system (DSE) using blockchain. The objective of this project is to propose a simple blockchain-based system for medical data management.

Keywords : Blockchain, Healthcare, Electronic health record EHR, Smart contracts

Remerciements

Tout d'abord, je remercie **Dieu** Tout Puissant de m'avoir donné la force et la patience nécessaire pour achever ce travail de mémoire.

J'ai tenon d'abord à remercier mon encadreur **"Aloui Ahmed"** de sa disponibilité, son soutien continu, sa motivation qui a fortement contribué à mener à bien ce travail.

Je remercie également les membres de jury, qui vont accepter de lire et d'évaluer ce travail.

Mon remerciement s'étend également à tous nos enseignants pendant les années des études, aussi à l'équipe de département d'informatique.

Enfin, je tiens à remercier tous ceux qui m'ont aidé en particulier ma famille et ma copine **L. Douaa**.

Dédicaces

Je dédie ce travail

A ma maman, celle qui s'est toujours sacrifiée pour me voir réussir, qui m'a soutenu et encouragé durant toutes ces années d'études.

À mon papa qui ne m'a jamais laissé manquer de quoi que ce soit, qui m'a toujours poussé et motivé dans mes études et ma vie quotidienne.

À ma sœur et mes frères Douaa, Yahia et Youcef.

À mes toutes mes amies Rania, Imene et Ibtessam.

Et en fin Je le dédie à tous ce qui m'a donné leur moindre coup de pouce pour réussir ce travail

Table des matières

Liste des tableaux

Table des figures

Introduction générale

L'application de technologie de blockchain a apparu en novembre 2008 avec la publication de la première monnaie électronique Bitcoin. Cette technologie de registre distribué aide à rendre plus sûres et plus transparents les données et permet aux internautes de réaliser des transactions sécurisées de pair à pair pour garantir l'intégrité de ces transactions.

Le secteur de la santé est un secteur particulièrement prometteur de la technologie Blockchain, car il est vraiment très sensible puisqu'il s'agit de partager les informations des patients et leurs données de santé. Ces dossiers de santé sont généralement stockés dans des bases de données traditionnelles gérées par des fournisseurs. Cela présente plusieurs problèmes de sécurité. Parmi les solutions actuelles trouvées pour sécuriser les informations d'un patient et assurer la confidentialité et l'interopérabilité des données de santé, on trouve la blockchain. Grâce à sa nature décentralisée et son inaltérabilité, elle pourrait assurer l'intégrité des données de santé à travers l'ensemble des systèmes d'information.

Dans notre projet de fin d'étude, nous cherchons à explorer la technologie de blockchain en réalisant un état de l'art sur le thème et en présentant un exemple réel son utilisation. Dans ce contexte, nous avons développé une application de santé qui est un exemple classique d'utilisation des blockchains en dehors de monnaies électroniques.

Le mémoire est organisé de la façon suivant :

- Le premier chapitre présent en détaille les concepts fondamentaux de la technologie blockchain.
- Le deuxième chapitre présent les applications de Blockchain dans les soins de santé et les principaux travaux de recherche des systèmes qui utilise la blockchain dans le domaine médical et une synthèse des points essentiels cités dans chaque travail traité.
- Le troisième chapitre offre la conception du système proposé.
- Le quatrième chapitre présente la réalisation et l'implémentation de notre système.

On termine notre mémoire par une conclusion générale.

Chapitre 1

Technologie Blockchain

1.1 Introduction

La Blockchain est une technologie permettant le stockage et l'échange d'information valeur de pair-à-pair (P2P). Elle est structurellement accessible, partagée et sécurisée grâce aux algorithmes de consensus. Elle s'utilise ainsi de façon décentralisée et permet la désintermédiation ou le remplacement des (tiers de confiance).

1.2 Définition de Blockchain

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. (Définition de Blockchain France)

Une blockchain est une technologie des registres et un protocole technologique qui permet d'échanger des données directement entre les différentes parties contractantes au sein d'un réseau et sans passer par des intermédiaires. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie entre les membres ou participants (nœuds)[1].

1.2.1 Une comparaison entre la base des données et blockchain

Une blockchain, est définie comme une base de données distribuées qui conserve un enregistrement permanent des données transactionnelles liées entre elles par une chaîne [2].

	Base de données	Blockchain
Opération	Peut effectuer des opérations CRUD.	Seulement des opérations d'insertion.
Accès	Seuls les utilisateurs autorisés peuvent les consulter ou y avoir accès.	Tout le monde peut valider les transactions sur le réseau.
Réplication	Seul le parti central a une copie.	Réplication complète du bloc sur chaque pair.
Consensus	Validation en 2 phases.	La majorité des pairs s'accordent sur le résultat des transactions.
Vol didentité	Les comptes sont souvent piratés.	cryptage et pseudo-anonymat cela rend très difficile le piratage de la blockchain.

Table 1.1 – Comparaison entre Base de données et Blockchain.

Les caractéristiques principales de la technologie blockchain sont :

- l'immuabilité : les données ne peuvent pas être modifiées ou supprimées après avoir été créées.
- la transparence : tout le monde peut consulter les différentes transactions et les informations sous-jacentes.
- l'autonomie : la Blockchain ne dépend de personne.
- La traçabilité : Les transactions précédentes peuvent être suivies.
- La désintermédiation : La technologie blockchain permet d'échanger sans le contrôle d'un tiers [3].

1.3 Historique de Blockchain

- En 1991, Stuart Haber et W. Scott Stornita ont introduit le concept de blockchain et ont travaillé sur une chaîne sécurisée de crypto-monnaie où personne ne pouvait altérer les horodatages des documents [4].
- En 2008, une personne ou un groupe de personnes connu sous le nom de Satoshi Nakamoto a publié un article décrivant le bitcoin et comment il pourrait être utilisé pour la numérisation. Envoyer des paiements entre deux entités consentantes sans avoir besoin d'une institution financière tierce. Chaque transaction a été enregistrée sur le registre blockchain, le bloc le plus récent lié à ceux précédant l'utilisation d'une si-

gnature numérique. Pour assurer la confiance dans le grand livre, les participants du réseau ont exécuté des algorithmes compliqués pour vérifier ces signatures numériques et ajouter des transactions à la chaîne de blocs [5].

- En 2013, Vitalik Buterin, programmeur et co-fondateur de Bitcoin Magazine, a déclaré que Bitcoin avait besoin d'un langage de script pour développer des applications décentralisées. Puisque Vitalik n'a pas pu parvenir à un accord dans la communauté, il a commencé à développer une nouvelle plate-forme informatique distribuée basée sur la blockchain, Ehereum, qui avait une fonctionnalité de script appelée contrats intelligents [1].
- En 2018, la blockchain a trouvé ses premières applications dans la téléphonie mobile. Par exemple, la startup Sirin Labs, basée en Suisse, lançait en novembre 2018 le premier smartphone à utiliser la technologie de la blockchain. Le téléphone, baptisé "Finney" était vendu à près de 1000 dollars et basait sa communication sur l'ultra-sécurité. L'entreprise proposait également un périphérique conçu exprès pour les transactions de crypto-monnaies [6].

1.4 Fonctionnalités

Une blockchain sert à organiser des transactions sous formes de blocs qui sont vérifiées par un grand nombre de participants, [7] ces participants stockent une copie identique du grand livre puis travaillent ensemble dans le processus de valider et certifier les transactions numériques, en ajoutant de nouvelles transactions au grand livre et partagé sur un réseau [8].

Le fonctionnement d'une transaction peut schématiquement être décrit en 5 étapes :

1. A effectue une transaction vers B.
2. Plusieurs transactions sont regroupées dans un bloc.
3. Le bloc est validé par les nœuds du réseau au moyen de techniques cryptographiques.
4. Quand le bloc est validé, il est daté et ajouté à la chaîne de blocs à laquelle tous les utilisateurs ont accès.
5. B reçoit la transaction de A[5].

Voici un schéma récapitulatif expliquant le fonctionnement d'une blockchain publique lors d'une transaction.

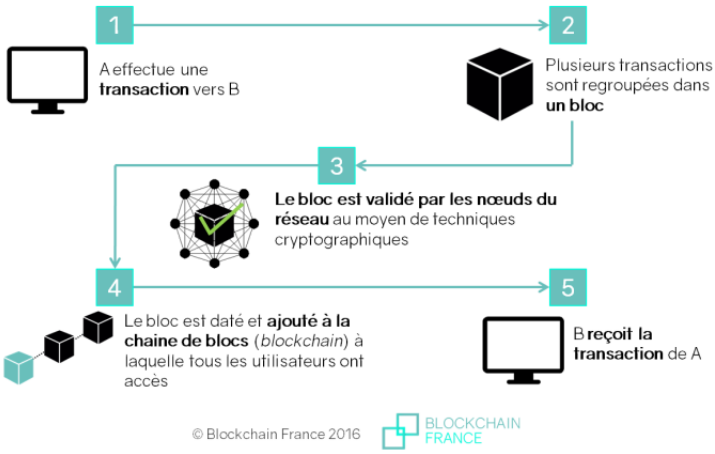


Figure 1.1 – Fonctionnement de la Blockchain

1.5 Structure dune Blockchain

La Blockchain a une architecture réseau distribué est Peer to Peer (P2P), fait référence à un groupe d'ordinateurs agissant en tant que nœuds pour partager des fichiers entre eux-mêmes. La Blockchain fonctionne donc sur un réseau distribué de serveurs, également appelé nœuds. Ces nœuds du réseau ont pour objectif de fournir un consensus sur l'état de la blockchain à tout moment et contiennent une copie de la blockchain. L'application fondamentale de la Blockchain est un grand livre de transactions, un peu comme un grand livre public sécurisé, qui stocke toutes les transactions qui ont lieu dans le réseau [2].

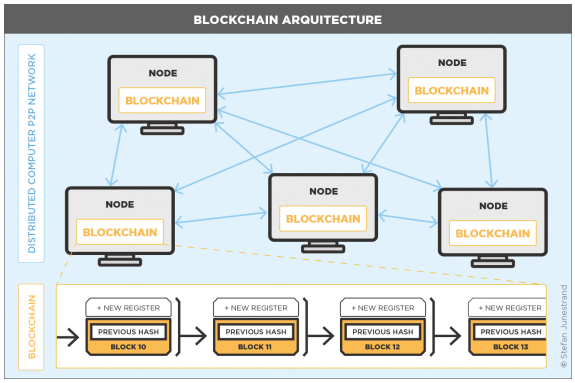


Figure 1.2 – Larchitecture dun blockchain.

La structure de la technologie Blockchain est représentée par une liste de blocs avec des transactions dans un ordre particulier. Les données de transaction sont stockées en blocs, qui sont reliés entre eux pour former une chaîne. À mesure que le nombre de transactions augmente, la taille de la Blockchain augmente également. Il existe des composants majeurs

pour tout écosystème de blockchain comme suit :

1.5.1 Transaction

Dans la blockchain, une transaction est une valeur de transfert qui est diffusée sur le réseau et transmise à tous les participants du réseau, également appelée nœuds et regroupée en blocs. Les transactions contiennent une ou plusieurs entrées et une ou plusieurs sorties (une entrée est une référence à une sortie d'une transaction précédente). Toutes les transactions seront dans un statut non confirmé jusqu'à ce que les mineurs valident les nouvelles transactions et les enregistrent dans le grand livre mondial de Blockchain [4][9]. Les transactions consistent généralement en une adresse de destinataire, une adresse d'expéditeur et une valeur.
Input :
Txx : transaction s (on peut avoir plusieurs transactions dans 1 seul bloc).
Pb : la clé publique
Sig : signature du l'émetteur
Output :
Data : les informations envoyées.
Hash(P) : le haché de clé publique du destinataire.

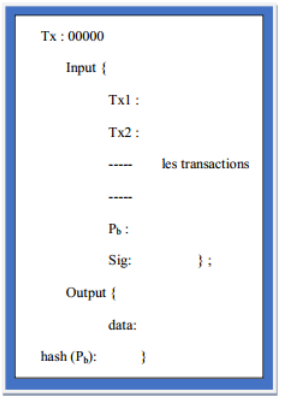


Figure 1.3 – Transaction blockchain.

1.5.2 Blocs

La blockchain est une chaine de blocs et chaque bloc contenant chacun plusieurs transactions, et qui vont être inscrits au fur et à mesure dans la blockchain par des nœuds du réseau. Chaque bloc est composé de deux éléments principaux sont l'en-tête et le corps de bloc.

1. En-tête de bloc

   L'en-tête de bloc est une partie importante, car il contient tous les éléments essentiels qui contiennent des métadonnées pour ce bloc. Ces données sont les suivantes :

   - La version de bloc «block version» : c'est le numéro de bloc, chaque bloc ayant son propre numéro, les numéros sont croissants (bloc 78, bloc 79, bloc 80, etc…), sa taille 4 octets.
   - L'empreinte «hash» de bloc précédent : est le hachage du bloc précédent qui sert à le lier au bloc suivant, sa taille est de 32 octets.
   - Le temps «timestamp» : c'est la date exacte de la création du bloc. Sa taille 4 octets.
   - Un nombre aléatoire «nonce» : est un nombre aléatoire nécessaire pour le processus de consensus, sa taille 4 octets.
   - Hash de bloc actuel : est le hachage du bloc réel et sa taille est de 32 octets.
   - Racine de Merkle : se compose de tous les hachages de transaction hachés dans la transaction [10].

2. Le corps de bloc

   Est composé d'une Liste des transactions et un compteur des transactions.

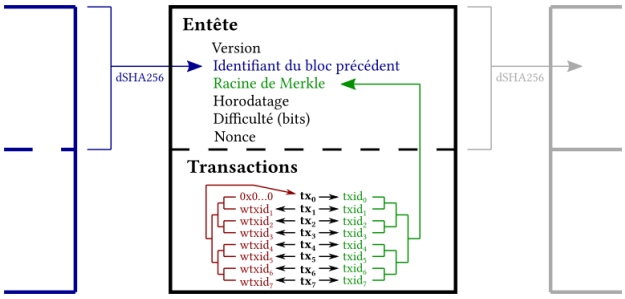


Figure 1.4 – Composante de bloc.

3. Processus de consensus

   La Blockchain étant basée sur une architecture décentralisée, il n'existe pas de nœud central ayant vocation à servir d'organe de contrôle pour vérifier et valider les informations stockées au sein du réseau. Le protocole de Consensus c'est la technique par lequel le réseau d'une Blockchain assuré le consensus sur le contenu de la blockchain et sur la manière de la création et la validation des nouveaux blocs. Pour cela la recherche et le développement des nouveaux Protocoles de consensus sont des sources de l'innovation dans l'industrie des Blockchains, l'innovation est portée sur la réduction de

temps de transaction, l'augmentation de la capacité de transaction et réduire les coûts de fonctionnement de la Blockchain qu'est essentiel due au haute consommation de l'électricité (cas PoW). Donc le consensus est une technique de coordination de travail dans la Blockchain [11].

(a) Proof of Work (PoW)

La PoW représente la méthode de validation de bloc la plus adoptée par les systèmes blockchain. Dans ce mécanisme, un mineur doit effectuer une quantité de travail, qui est souvent un puzzle ou un défi mathématique, difficile à calculer, mais facile à vérifier. La preuve de travaille a l'avantage de protéger l'intégrité des transactions et des blocs [2].

(b) Proof of Stake (PoS)

Afin de résoudre les lacunes de la PoW (Preuve de Travail), la PoS (Preuve d'Enjeu) a été proposée. Les mineurs sont appelés forgeurs. Un forgeur peut valider des blocs en fonction de la quantité d'argent qu'il possède. Ce qui signifie que plus il possède de monnaies, plus il augmente sa chance de validation. Chaque forgeur parie sur un bloc. On peut dire qu'une fois que les blocs honnêtes sont ajoutés à la chaîne, chaque forgeur touche une récompense relative à son pari. Dans la PoS un forgeur dont le bloc s'avère malhonnête est pénalisé et le montant du pari qu'il a mis est débité de son solde [2].

(c) Comparaison entre PoW et PoS

Figure 1.5 – Proof of Work Vs Proof of Stake

1.6 Hachage

Le hachage génère une ou plusieurs valeurs à partir d'une chaîne de texte à l'aide d'une fonction mathématique. Le hachage est un moyen d'activer la sécurité pendant le processus de transmission du message lorsque le message est destiné à un destinataire particulier uniquement. Une formule génère le hachage, ce qui contribue à protéger la sécurité de la transmission contre la falsification. En termes simples, le hachage signifie prendre une chaîne de caractère de n'importe quelle longueur et donner une sortie d'une longueur fixe (le hash) [12].

Fonctions de hachage

Une fonction de hachage cryptographique doit posséder certaines propriétés pour être considérée comme sécurisée.

- Déterministe : Cela signifie que peu importe le nombre de fois que vous analysez une entrée particulière via une fonction de hachage, vous obtiendrez toujours le même résultat.
- Calcul rapide : La valeur de hachage d'un message se calcule très rapidement.
- Résistance pré-image : Pour une valeur de hachage donnée H (A), il est impossible de déterminer un message A ayant cette valeur de hachage.
- De petits changements dans l'entrée modifient le hachage : Même si vous apportez un petit changement dans votre entrée, les changements qui seront reflétés dans le hachage seront énormes.
- Résistant aux collisions : Étant donné deux entrées différentes A et B où H (A) et H (B) sont leurs hachages respectifs, il est impossible que H (A) soit égal à H (B). Cela signifie que pour la plupart, chaque entrée aura son propre hachage unique.

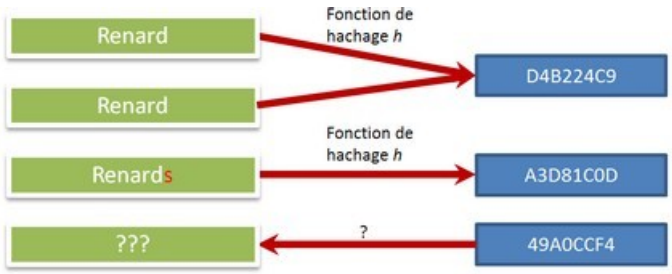


Figure 1.6 – Fonctions de hachage.

1.6.1 Hachage SHA-256

SHA 256 est la technique qui permettre la création de ces empreintes cette technique permettre de traduire n'importe qu'elle type des données (inputs) à des outputs standards de 64 chiffre. Le hash produit par cette technique dans le cas Blockchain Bitcoin est la preuve de travail [11]. Cette méthode de cryptage présente de nombreux avantages :

- La compression des données est effectuée rapidement.
- Il est impossible d'annuler le processus de conversion sans clés.
- Il est impossible de décrypter les données converties.
- Un algorithme de cryptage unidirectionnel traite une quantité illimitée d'informations [13].

1.7 Mineurs et les nuds

1.7.1 Mineurs

Les "mineurs" sont des particuliers qui permettent de vérifier la validité des transactions bloc par bloc. Ils sont rémunérés pour mettre à disposition la puissance de calcul de leurs processeurs [5].
Les mineurs doivent déterminer pour «trouver» un bloc et cela se fait comme suit [56] :

1. Un nombre aléatoire est deviné «Nonce».
2. Le Nonce est ajouté à la fin de toutes les données du bloc.
3. Tout cela est haché selon la méthode SHA256.
4. Si ce hachage commence par un nombre prédéterminé de zéro, un nouveau bloc est trouvé. Sinon, le mineur doit recommencer à l'étape 1 en devinant un autre Nonce [4].

1.7.2 Les nuds

Les nœuds sont des ordinateurs reliés au réseau. Chaque nœud comporte une copie de la base de données qui trace l'historique de l'ensemble des transactions effectuées. Ainsi se forme une chaine de blocs reliés entre eux, ce qui rend la blockchain infalsifiable. Ainsi, si un tiers souhaite hacker le réseau, il est nécessaire pour cet hackeur de corrompre plus de la moitié (plus de 51%) des nœuds simultanément. Le nombre de nœuds étant très important, en cas de tentative de fraude, cela serait détecté très rapidement [14].

1.8 Chaîne générique de blocs

La blockchain est structurée comme une liste liée en arrière de blocs où chaque bloc renvoie au bloc précédent. Elle est souvent visualisée comme une chaîne horizontale, comme sur l'image ci-dessous, où chaque bloc contient plusieurs transactions. Le premier bloc sert de bloc de genèse (Genesis block), qui est le premier bloc de transactions jamais confirmé dans cette blockchain spécifique. Lorsque le bloc suivant est vérifié, ce sera le bloc parent du bloc précédent. Pour « lier » les blocs entre eux, chaque bloc contient une référence à son bloc parent. En concevant les blocs de cette manière, une «chaîne» est créée où, si vous modifiez les données d'un bloc, la chaîne entière devra changer. Enfin, le dernier bloc sera appelé le bloc le plus récemment ajouté [15].

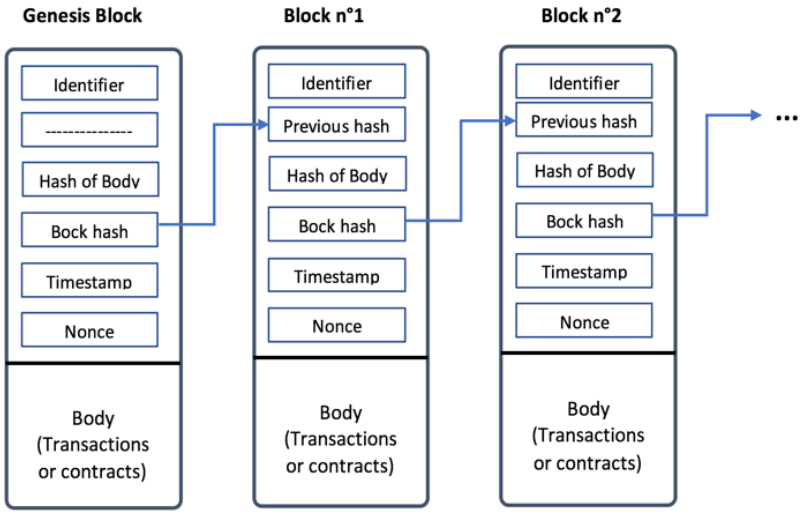


Figure 1.7 – Chaîne générique de blocs.

1.9 Contrats intelligents

En 1994, Nick Szabo, juriste et cryptographe a réalisé que le grand livre décentralisé pouvait être utilisé pour des contrats intelligents (contrats blockchain). Dans ce format, les contrats pourraient être convertis en code informatique, stockés et répliqués sur le système et supervisés par le réseau d'ordinateurs qui exécutent la blockchain. Cela entraînerait également une rétroaction du grand livre, comme le transfert d'argent et la réception du produit ou du service [16].

1.9.1 Définition

Les contrats intelligents ou (smart contracts), sont des programmes informatiques exécutant un ensemble d'instructions prédéfinies (si telle condition est remplie, telle transaction est faite), garantissant la force obligatoire des contrats non plus par le droit, mais par le code Ces smart contacts sont souvent partie intégrante du fonctionnement de blockchains récentes[17].

1.9.2 Caractéristiques

Les contrats intelligents sont capables de suivre la performance en temps réel et peuvent apporter des économies considérables. Pour obtenir des informations externes, un contrat intelligent nécessite des informations oracles, qui alimentent le contrat intelligent avec des informations externes.

Les contrats intelligents sont :

- Auto-vérification.
- Auto-exécutable.
- Inviolable.

1.9.3 Fonctionnement

Les contrats intelligents fonctionnent en suivant des déclarations simples "si/quand ... alors" qui sont écrites en code sur la blockchain. Un réseau d'ordinateurs exécute les actions (déblocage des fonds aux parties concernées ; envoi de notifications ...) lorsque des conditions prédéterminées ont été remplies et vérifiées. La blockchain est ensuite mise à jour lorsque la transaction est terminée [18].

Ces programmes sont capables de surmonter les problèmes d'aléa moral, et de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude. L'avantage de mettre en place des smarts-contracts dans une blockchain réside dans la garantie que les termes du contrat ne pourront pas être modifiés. Un smart-contract qui ne serait pas dans la blockchain serait un programme dont les termes pourraient être changés en cours d'exécution [5].

1.9.4 Avantages de contrats intelligents

Voici ce que vous offrent les contrats intelligents :

- Autonomie : il n'est pas nécessaire de compter sur un courtier, un avocat ou d'autres intermédiaires pour confirmer. Incidemment, cela élimine également le risque de manipulation par un tiers, puisque l'exécution est gérée automatiquement par le réseau.
- Confiance : les documents sont chiffrés sur un registre partagé. Personne ne peut dire qu'il l'a perdu.
- Sauvegarde : Sur la blockchain, les documents sont dupliqués plusieurs fois sur chacun des blocs.
- Sécurité : la cryptographie, le cryptage des sites Web, protège vos documents.
- Vitesse : les contrats intelligents utilisent le code logiciel pour automatiser les tâches, réduisant ainsi les heures de travail sur une gamme de processus métier.
- Économies : les contrats intelligents vous font économiser de l'argent, car ils suppriment la présence d'un intermédiaire.
- Précision : évitez les erreurs liées au remplissage manuel de tas de formulaires [16].

1.9.5 Inconvénients de contrats intelligents

- Le principal inconvénient des contrats intelligents est une conséquence de leur principal avantage, à savoir que le code est immuable. Si une erreur est faite lors de la transcription du contrat en code informatique, il est impossible de revenir en arrière.
- Il est aussi compliqué de connecter le monde physique aux réseaux blockchains. En effet, même si les oracles de blockchain offrent des solutions pour rapatrier des données du monde physique, cela reste coûteux et compliqué [4][5].

1.10 Types de cryptographie dans Blockchain

La cryptographie est la méthode de déguisement et de révélation, aussi connue sous le nom de cryptage et de décryptage, de l'information par le biais de mathématiques complexes. Cela signifie que l'information ne peut être consultée que par les destinataires prévus et personne d'autre [19].

1.10.1 Cryptographie symétrique

Technique de chiffrement basée sur un algorithme combiné à une clé secrète partagée par les deux entités communicantes. La même clé sert donc à chiffrer et déchiffrer, l'algorithme

de décryptage assurant une fonction inverse à celui de chiffrement [20].

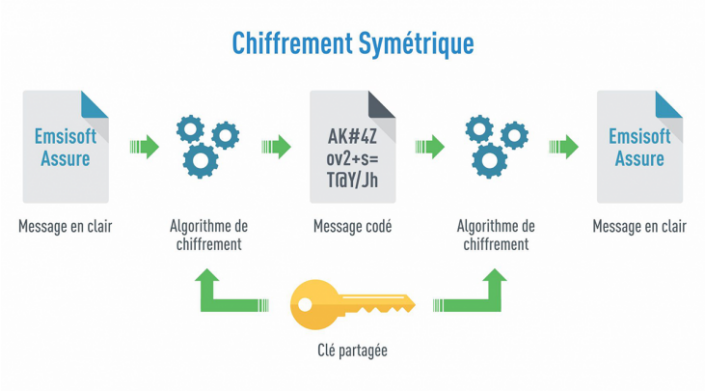


Figure 1.8 – Cryptographie symétrique.

1.10.2 Cryptographie Asymétrique

Est la branche de la cryptographie la plus utilisée dans le monde des blockchains. Elle s'appuie sur deux clés que possède chaque participant : une clé privée gardée secrète par son propriétaire et une clé publique qui peut être distribuée à tous[21].

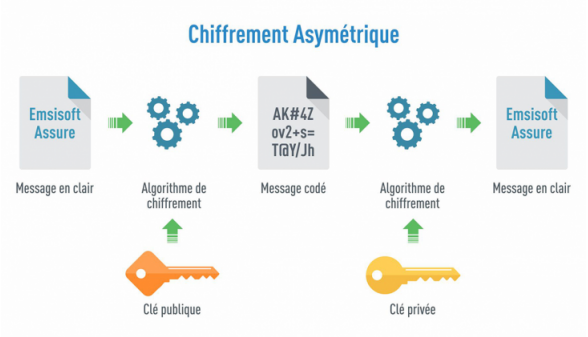


Figure 1.9 – Cryptographie asymétrique.

1.10.3 La signature numérique

La signature numérique permet d'ajouter à tout document ou message une preuve que le document provient réellement de l'expéditeur et n'a pas été altéré entre-temps. Cela peut être vérifié en utilisant la clé publique de l'expéditeur et si la vérification est bonne, alors il ne fait aucun doute que la signature a été créée en utilisant la clé privée appartenant uniquement à l'expéditeur [22].

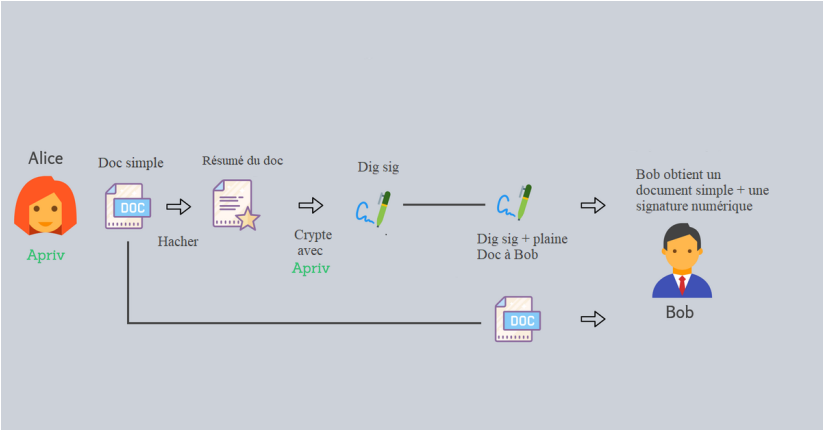


Figure 1.10 – la signature numérique.

Ainsi, la signature numérique peut

- Intégrité : prouver que le message n'a pas été modifié.
- Authentification : prouver la source du message.
- Non-répudiation : s'assurer que la signature numérique n'est pas fausse e que le signataire ne peut pas la répudier.

1.10.4 Fonction de Hachage

A fonction de hachage cryptographique fait partie d'un groupe de fonctions de hachage adaptées aux applications cryptographiques. Comme les autres fonctions de hachage, les fonctions de hachage cryptographiques sont des algorithmes mathématiques à sens unique utilisés pour mapper des données de toute taille à une chaîne de bits de taille fixe. Les fonctions de hachage cryptographique sont largement utilisées dans les pratiques de sécurité de l'information, telles que les signatures numériques, les codes d'authentification de message et d'autres formes d'authentification [23].

1.11 Types de blockchains

Il existe trois catégories des Blockchains, chaque catégorie a ses propres caractéristiques est orienté pour une utilisation spécifique.

1.11.1 Blockchains publiques

En principe la Blockchain est publique, c'est-à-dire accessible par n'importe qu'il personne, chaque personne peut devenir utilisateur, crée son propre nœud et participer à la validation des transactions et la création des blocs, etc. il est suffisant de télécharger le logiciel de la Blockchain concerné sur un ordinateur pour devenir un participant dans le réseau comme dans les Blockchains Bitcoin et Ethereum [11].

1.11.2 Blockchains privées

Les blockchains privées sont souvent appelées "blockchain permissionnaire". Contrairement aux blockchains publiques, elles constituent un réseau fermé et ne permettent la participation que de certaines entités autorisées. Les blockchains privées ont généralement un administrateur réseau accorde des droits et des restrictions spécifiques aux participants du réseau. Cela signifie essentiellement que les blockchain privées sont plus centralisées [24].

1.11.3 Blockchains consortiums (hybride)

La blockchain à consortium se situe sur la limite entre chaînes publiques et privées, combinant des éléments des deux côtés. Au lieu d'un système ouvert où n'importe qui peut valider des blocs ou d'un système fermé où seule une seule entité nomme les producteurs de blocs, une chaîne à consortium comporte une poignée de parties équitablement puissantes qui fonctionnent simultanément en tant que validateurs [25].

1.12 Avantages et les inconvénients de la Blockchain

1.12.1 Les avantages de la Blockchain

- Distribué : Étant donné que les données de la blockchain sont souvent stockées dans des milliers de périphériques sur un réseau de nœuds distribué. Le système et les données sont extrêmement résistants aux défaillances techniques et aux attaques malveillantes. Chaque nœud du réseau est capable de répliquer et de stocker une copie de la base de données.
- Stabilité : Les informations contenues dans la chaîne de blocs ne peuvent être effacées ni modifiées. Une fois qu'une opération a été réalisée, elle restera gravée à jamais dans

la chaîne de blocs : ce qui permet de savoir exactement le chemin parcouru par les informations.

- La sécurité : L'aspect décentralisé assure la sécurité des informations et des échanges inscrits dans l'historique de la blockchain. En effet, comme tous les utilisateurs disposent d'une copie de chaque transaction, le risque de cyberattaque bien plus faible.

1.12.2 les inconvénients de la Blockchain

- Évolutivité : Les registres de Blockchain peuvent devenir très volumineux avec le temps.
- Clés privées : Les utilisateurs ont besoin de leur clé privée pour accéder à leur fonds, ce qui signifie qu'ils agissent comme leur propre banque. Si l'utilisateur perd sa clé privée, alors l'argent est déjà perdu et ne peut pas être récupéré.
- Modification de données : une fois que des données ont été ajoutées à la blockchain, il est très difficile de les modifier. Si la stabilité est l'un des avantages de la blockchain, cela n'est pas toujours un point positif. Modifier les données ou le code d'une chaîne de blocs est généralement très exigeant.
- L'attaque à 51% désigne une attaque d'une blockchain (fonctionnant avec des mineurs) conduite par un ensemble de nœuds du réseau qui contrôle plus de la moitié de la puissance de calcul du réseau. Elle résulte dans la possibilité pour cet ensemble de nœuds de choisir les transactions inscrites dans la blockchain et de rendre possible une double dépense. C'est une attaque classiquement redoutée, car susceptible de rendre inutilisable la blockchain. Ce terme est souvent utilisé en référence à la blockchain Bitcoin [19].

1.13 Usage de la blockchain

Dans la pratique, la blockchain est souvent exploitée pour répondre à des problématiques plus complexes, Nous allons présenter quelques exemples.

- La santé : Chaque année, les systèmes de gestion des soins de santé incompatibles coûtent des milliards de dollars et des milliers de patients meurent de soins inadaptés. La technologie Blockchain pourrait apporter une contribution importante à la simplification de la gestion des données de santé. Philips a développé un concept de stockage

des données patient dans une chaîne de blocs en coopération avec la société Tierion [26].

- La banque : Les banques se sont empressées d'utiliser la blockchain à leur avantage en essayant de créer un système de paiement plus sécurisé avec moins de délais, de coûts et d'efforts manuels, où tous les acteurs du commerce international (importateur, exportateur, banques, transporteurs) peuvent partager des informations [27].
- L'énergie : Dans le milieu de l'énergie, le projet Brooklyn Microgrid a pour but est de permettre à un ensemble de personnes produisant de l'énergie solaire de pouvoir gérer le flux d'électricité produite à une échelle communautaire de façon totalement décentralisée grâce à des smart contract basés sur Ethereum. Ce cas d'usage démontre très simplement comment une communauté d'utilisateurs peut décider de se passer des intermédiaires [28].
- L'immobilier : La blockchain pourrait offrir de nombreux avantages au secteur immobilier. Les caractéristiques de cette technologie permettront la transparence de l'information par rapport à l'historique des propriétaires. De ce fait, le risque de fraude et les travaux de vérification et d'expertise diminueraient.
- Vote : Les moyens d'expression des votants ont beaucoup évolué au fil du temps et parmi ces derniers, le vote électronique séduit par sa simplicité autour de la gestion de votes grâce aux automatismes de l'informatique. Utiliser la Blockchain dans un système de vote permettrait, avec ses attributs de distributivité et de non-altération des données, de supprimer les questions subsistantes sur les potentielles fraudes et de gagner en rapidité. La Blockchain rend disponible l'information sur le vote effectif dans un délai court sans pour autant divulguer le choix du votant [29].

1.14 Blockchain aujourdhui

1.14.1 Bitcoin

Le bitcoin est une monnaie virtuelle créée en 2009. Contrairement aux monnaies classiques, le bitcoin n'est pas émis et administré par une autorité bancaire. Il est émis sur le protocole blockchain du même nom. Cette technologie permet de stocker et transmettre des informations de manière transparente, sécurisée et sans organe central de contrôle. Le bitcoin, comme beaucoup d'autres crypto-monnaies, est mis en circulation via le minage. Les

”mineurs”, des personnes réparties partout dans le monde, effectuent des calculs mathématiques avec leur matériel informatique pour le réseau bitcoin afin de confirmer les transactions et augmenter leur sécurité. En échange, ils reçoivent des bitcoins. Ils peuvent ensuite être convertis en monnaie fiat ou être échangés contre d'autres crypto-monnaies sur des plateformes d'échange [30].

1.14.2 Crypto-monnaies

On désigne par crypto monnaie à la fois une monnaie cryptographique et un système de paiement de pair à pair. Ces monnaies numériques sont donc des monnaies virtuelles dans le sens où ces dernières sont caractérisées par une absence de support physique : ni pièces, ni billets, et les paiements par chèque ou carte bancaire ne sont pas possibles non plus.

Ce sont des monnaies alternatives qui n'ont de cours légal dans aucun pays du globe. Elles ne sont pas non plus régulées par un organe central ou des institutions financières. Il n'y a pas de banques centrales à leurs têtes. Et pourtant, sécurité et transparence sont leurs principaux atouts ! En effet la cryptographie sécurise les transactions qui sont toutes vérifiées et enregistrées dans un domaine public, assurant tout à la fois confidentialité et authenticité grâce à la technologie Blockchain [31].

1.14.3 Ethereum

Ethereum est une plate-forme blockchain open source qui permet à quiconque de développer et de déployer des applications décentralisées Blockchain, quel que soit le type d'applications, y compris la crypto-monnaie, les symboles, les applications sociales et plus encore. En d'autres termes, Ethereum a ouvert les possibilités de la technologie ”Blockchain” et ”Ledger distribué” à d'autres domaines d'application [4].

1.14.4 Hyperledger Fabric

Les réseaux blockchain traditionnels ne peuvent pas prendre en charge les transactions privées et les contrats confidentiels qui sont de la plus haute importance pour les entreprises. Hyperledger Fabric a été conçu en réponse à cela comme une fondation modulaire, évolutive et sécurisée pour offrir des solutions blockchain industrielles. Est un cadre blockchain modulaire qui sert de base au développement de produits, de solutions et d'applications basés sur la

blockchain à l'aide de composants plug-and-play destinés à être utilisés au sein d'entreprises privées [32].

1.15 Conclusion

L'utilisation de la Blockchain commence à dépasser le cadre des crypto-monnaies. Nombreux sont ceux qui commencent à s'y intéresser et à penser son développement. Comme nous avons pu le constater, les inconvénients existants sont surtout le fait de la nouveauté de cette technologie, qui doit continuer son développement afin de gagner en efficience. Dans le chapitre suivant, on met l'accent sur la Blockchain dans les soins de santé.

Chapitre 2

Applications de Blockchain dans les soins de santé

I. Applications de Blockchain dans les soins de santé

2.1 Introduction

La blockchain souvent décrite comme un outil permettant d'instaurer la confiance entre des acteurs. Ses applications ont largement évolué au gré des avancées technologies et à l'intérêt grandissant des entreprises internationales. La technologie de la Blockchain se révèle être un allié important dans le domaine des soins de santé par plusieurs 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 contrats qui automatisent et facilitent de nombreux processus.

2.2 Applications des blockchains en santé

Les soins de santé, dans tous les contextes, génèrent d'abondantes données complexes et riches, ces données proviennent habituellement de sources très variées, comme les médecins de ville, l'hôpital, les assurances, les pharmaciens ou les laboratoires d'analyses médicales [33]. Allant des données sensibles identifiables des patients aux analyses opérationnelles. La diffusion et les actions essentielles d'échange de ces données liées à la santé font qu'elles restent exposées au risque d'atteintes à la vie privée Les technologies

blockchain ont été proposées pour authentifier et vérifier les utilisateurs et utilisée pour contrôler l'accès aux données sensibles [34].

La plupart des données contenues dans les dossiers médicaux électroniques ne peuvent pas être partagées et échangées entre les utilisateurs de manière appropriée qu'une fois que le patient a consenti. Les technologies blockchain ont le potentiel de résoudre les problèmes de stockage, le potentiel d'augmenter l'interopérabilité entre les patients, les soignants, les professionnels de la santé et les chercheurs grâce à la mise en place de nouvelles méthodes de liaison de données de sources disparates [35]. Le consentement du patient permet également aux prestataires de soins de santé de faire confiance aux données auxquelles ils accèdent, ce qui leur permet de traiter leurs patients en conséquence [36].

En plus d'assurer la sécurité d'accès, l'évolutivité et la confidentialité des données, les blockchains ont également le potentiel d'améliorer la recherche médicale grâce à divers cas d'utilisation, les données provenant des dossiers médicaux et des applications de santé être stockées et rendues accessibles aux utilisateurs tout au long de leur vie, ce qui faciliterait la réalisation d'études longitudinales et d'applications de pharmacovigilance. Chaque fois qu'un patient obtient une nouvelle ordonnance ou des résultats de tests, il pourrait être informé que les nouvelles données ont été cryptées, envoyées pour être stockées et ajoutées à un système automatisé [35]. Une fois les données cryptées et stockées, les chercheurs peuvent être sûrs que les données ne seront pas modifiées [37]. Les patients et les participants peuvent donner leur consentement et révoquer l'accès, tout en gardant le contrôle de leurs informations [38].

2.2.1 Les blockchains en recherche Clinique

Alors que la recherche clinique évolue vers une saisie des données dans le monde réel avec un partage accru des données, il existe un besoin croissant de technologies centrées sur le patient qui garantissent l'authenticité des données et favorisent l'accès des chercheurs et des patients. La blockchain fait partie d'un ensemble émergent de technologies de registres distribués ayant le potentiel d'offrir à la fois la transparence et la confiance dans les données de recherche. Les systèmes basés sur la blockchain étant développés pour des applications de recherche clinique [39].

Les essais cliniques et la gestion du consentement des sujets des essais sont un domaine

où la blockchain a le potentiel d'accroître la transparence et la responsabilité des praticiens et des chercheurs médicaux. Ce sont une étape obligatoire dans le développement d'un médicament : ils correspondent le plus souvent à la première administration d'un médicament chez l'homme. La participation des patients est donc la condition sine qua non pour que des essais cliniques puissent être réalisés. Le consentement éclairé du patient doit obligatoirement être recueilli avant le début de l'essai [40]. En conservant un journal immuable du consentement des patients, les organismes de réglementation peuvent facilement surveiller les normes des essais cliniques. Cet aspect est particulièrement important, car les formulaires de consentement éclairé falsifiés figurent parmi les types de fraude clinique les plus courants. Ce qui inclut la modification des dossiers et la falsification du consentement du patient, ce qui indique qu'un niveau d'authentification du sujet de l'essai serait nécessaire pour empêcher cela [41].

2.2.2 Blockchains dans la détection de fraude médicale

La fraude et les abus constituent un défi financier, juridique et politique majeur qui concerne tous les secteurs de l'industrie des soins de santé, y compris les fabricants de médicaments et de dispositifs médicaux, les hôpitaux, les pharmacies et les payeurs. Le groupe le plus touché est sans doute celui des payeurs, qui sont victimes de fraudes dans les demandes de remboursement de soins de santé chaque année. La fraude en matière de soins de santé se présente sous différentes formes, notamment les pots-de-vin, les fausses demandes et les autoréférences illégales. Elle a un impact négatif direct sur l'utilisation des soins de santé, car elle entraîne un gaspillage de ressources limitées et met potentiellement en danger les patients en leur fournissant des soins inutiles ou en les empêchant d'accéder aux services médicalement nécessaires, ce qui peut entraîner un risque plus élevé de mortalité toutes causes confondues et d'hospitalisation d'urgence.

Bien que des efforts aient été faits pour automatiser la détection de la fraude, la plupart des poursuites pour fraude et abus continuent d'être le fait de dénonciateurs.

La blockchain est une technologie susceptible de relever ces défis. Les cas d'utilisation de la blockchain dans le domaine de la santé commencent à mûrir, principalement pour améliorer la gouvernance des données et des processus de santé. L'une des principales utilisations consiste à améliorer la gestion, à permettre le partage et à améliorer l'échange des données sur la santé des patients et des consommateurs. Cela s'étend

également à l'utilisation de la blockchain pour la recherche clinique afin d'améliorer la gestion des données des essais et le consentement électronique. Nombre de ces utilisations se concentrent sur des approches centrées sur le patient pour gérer et préserver la confidentialité des données de santé avec la blockchain [42].

2.2.3 Blockchains dans lindustrie pharmaceutique et la recherche

La contrefaçon de médicaments est un problème mondial qui présente des risques importants pour les consommateurs et le grand public. Selon l'Organisation mondiale de la santé, dix pour cent des médicaments sont contrefaits dans le monde, et dans les pays en développement, ce chiffre atteint 30 pour cent [43]. Ils sont également très répandus lors des épidémies, lorsque des pénuries de médicaments essentiels ont tendance à se produire et que la contrefaçon est la plus susceptible d'augmenter. Les médicaments de qualité inférieure sont dangereux. Les médicaments falsifiés et de qualité inférieure, qui peuvent contenir des ingrédients inactifs, des ingrédients actifs, mais dans un mauvais dosage ou des contaminants potentiels, peuvent être mortels [4]. Les médicaments se déplacent dans une chaîne de distribution qui implique plusieurs participants. Ceux-ci comprennent généralement un fabricant, un grossiste et un détaillant. Un organisme de réglementation, tel que la FDA, peut tester la qualité d'un lot de produits

pharmaceutiques avant ou pendant leur distribution le long de la chaîne d'approvisionnement. Ces participants établissent entre eux des relations directes fondées sur des contrats.

La technologie Blockchain permet de confirmer l'authenticité des recettes et des médicaments à l'aide de dispositifs numériques spéciaux. Et facilite la détection de la fraude en interdisant toute duplication ou modification dans la transaction, et en permettant finalement une transaction transparente et sécurisé ayant la particularité d'être immuable. Industrie et recherche pharmaceutiques Blockchains, grâce à son pouvoir de traçage détaillé, contrôle chaque étape de la chaîne d'approvisionnement pharmaceutique [2]. Il en résulte une réduction du nombre de médicaments contrefaits sur le marché, ainsi qu'une amélioration de la qualité des soins médicaux pour la population.

2.2.4 Blockchain et le Dossier de Santé Électronique

Les systèmes de DSE ont été mis en œuvre dans un certain nombre d'hôpitaux à travers le monde en raison des avantages qu'ils procurent, notamment l'amélioration de la sécurité et leur rentabilité. Ils sont considérés comme un élément essentiel du secteur des soins de santé, car ils permettent le stockage électronique des dossiers médicaux, la gestion des rendez-vous des patients, la facturation et la comptabilité, ainsi que les tests de laboratoire. Ils sont disponibles dans de nombreux systèmes de DSE utilisés dans le secteur de la santé. L'objectif principal est de fournir des dossiers médicaux sécurisés, résistants et partageables sur différentes plateformes. Bien que l'idée derrière l'utilisation des systèmes de DSE dans les hôpitaux ou les soins de santé soit d'améliorer la qualité des soins, ces systèmes ont rencontré certains problèmes et n'ont pas répondu aux attentes qui leur étaient associées. Il a été conclu que les systèmes de DSE étaient confrontés à des problèmes liés à leur manque de fiabilité et à leur faible convivialité. Une blockchain présente certains avantages tels que la sécurité, l'anonymat et l'intégrité des données sans l'intervention d'un tiers. Ces avantages en font un choix raisonnable pour y stocker les dossiers médicaux des patients, car l'innovation technologique dans le secteur des soins de santé a fait de la sécurité des données médicales des patients une priorité absolue. Un certain nombre de chercheurs ont également identifié que l'utilisation de la technologie blockchain dans les soins de santé serait une solution réalisable[44].

2.3 Management et partage de données de santé

La manipulation des dossiers de santé électroniques de manière sécurisée est devenue un véritable défi, car les données sont réparties entre plusieurs établissements médicaux. La plupart des systèmes de soins de santé existants sont centralisés et vulnérables aux défaillances et aux fuites

d'informations. La fuite d'informations personnelles et critiques d'un patient peut avoir de graves conséquences. De plus, les systèmes médicaux actuels ne parviennent pas à assurer la transparence, la traçabilité fiable, l'immuabilité, l'audit, la confidentialité et la sécurité, tout en gérant les dossiers de santé électroniques. Compte tenu de ces défis dans les systèmes de santé actuels, la technologie blockchain a le potentiel de les

résoudre. On estime que l'adoption de la blockchain peut permettre d'économiser des milliards par an en coûts liés aux violations de données et par une réduction des fraudes et des produits contrefaits.

La blockchain est une technologie prometteuse qui peut contribuer à rationaliser les opérations de gestion des données de santé en assurant une efficacité sans précédent des données et en renforçant la confiance. Elle offre un large éventail de caractéristiques importantes et intégrées, telles que le stockage décentralisé, la transparence, l'immuabilité, l'authentification, la flexibilité de l'accès aux données, l'interconnexion et la sécurité, permettant ainsi une utilisation généralisée de la technologie blockchain pour la gestion des données de santé. Blockchain utilise le concept de contrats intelligents qui présentent des conditions sur lesquelles tous les partenaires de soins de santé impliqués dans le réseau sont d'accord. Elle permet de réduire les coûts administratifs inutiles [45].

2.4 Communication de données de santé entre les divers acteurs du parcours de soin du patient

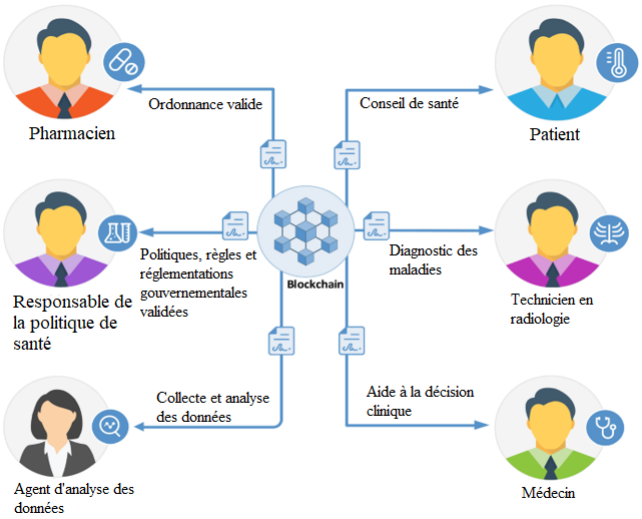


Figure 2.1 – Communication de données de santé entre les divers acteurs

2.5 Comparaison entre la solution classique et la solution blockchain

Nous possédons tous un carnet de santé. Puis nous le perdons, ou cessons de l'utiliser, ou ne savons plus trop comment le remplir –faute d'être fait correctement par le personnel médical. C'est regrettable, car notre suivi en tant que patient devient beaucoup plus approximatif : vaccins, allergies et autres antécédents médicaux… Autant d'informations pourtant cruciales pour établir un diagnostic ou gérer une urgence et qui peuvent être facilement perdues.

L'idée d'utiliser le numérique pour aider au stockage et à la gestion des données médicales a germé dans la fin des années 60. Cela resta à l'état de concept jusqu'en 2004 quand eurent lieu des expérimentations pour mettre en place un Dossier Médical Partagé (DMP). Le DMP n'a pas rencontré le succès escompté, car les médecins généralistes n'avaient pas d'incitation à faire l'effort de le remplir et le service n'était pas intuitif.

En parallèle, plusieurs compagnies et articles de recherche proposent des solutions basées sur la blockchain. Bien que cela ouvre la voie à de nombreuses améliorations du suivi des patients [46].

	Dossier Médical Partagé	Solution Blockchain
Données disponibles	— Historique des soins des 24 derniers mois — Historique des remboursements des 12 derniers mois. — Résultats dexamens (radios, analyses biologiques). — Antécédents médicaux (pathologies, allergies). — Comptes rendus dhospitalisation. — Directives anticipées de fin de vie.	Toutes données issues de : — Divers centres de soins, tels que les hôpitaux, les laboratoires biologiques etc — Données dappareils connectés (privés et dispositifs médicaux). — Résultats déclarés et autres renseignements autodéclarés sur la santé. — Données génomiques et les données propres à la maladie (biomarqueurs etc).
Données dessais cliniques	Non	Oui
Données de vie réelle	Non	Oui
Contrôle et traçabilité daccès aux données	Oui	Oui
Prix	Gratuit	Gratuit (+fonctions participatives + premium)
Statut	Etat	Privé
Sécurité	Hébergeur de donnée de santé	Blockchain
Vente des données	Non	Oui

Table 2.1 – Tableau comparatif de la solution DMP classique par rapport à la solution blockchain .

2.6 Travaux connexes

2.6.1 L'article 1 : Blockchain Applications for Healthcare Data Management

2.6.1.1 Objectifs

[47] Dans une blockchain, les données sont distribuées sur le réseau et il n'y a pas de

point de défaillance unique, ce qui entraîne un mécanisme de sauvegarde inhérent. En outre, une version unique des données est copiée sur chaque nœud de la blockchain. Cela réduit le volume des transactions entre les systèmes d'information, réduisant ainsi la charge sur l'écosystème des soins de santé. Avec les progrès réalisés dans la collecte des données électroniques liées à la santé, le stockage des données de santé dans le nuage et les réglementations sur la protection de la vie privée des patients, de nouvelles possibilités s'ouvrent pour la gestion quotidienne des données de santé, ainsi que pour la commodité pour les patients d'accéder à leurs propres données de santé et de les partager. Le potentiel de l'utilisation de la technologie blockchain dans les hôpitaux a commencé à être testé dans plusieurs projets pilotes à l'échelle mondiale [47].

2.6.1.2 Méthodes

Nous avons réalisé une enquête préliminaire pour combler le fossé qui existe entre les manuscrits purement techniques sur les blockchains, d'une part et la littérature qui s'intéresse principalement aux discussions marketing sur leur impact économique attendu, d'autre part.

2.6.1.3 Description du cas

(a) Blockchain pour la gestion des données des dossiers médicaux électroniques (DME)

Aux États-Unis, Booz Allen Hamilton Consulting a développé et mis en œuvre une plate-forme pilote basée sur la blockchain conçue pour aider le Bureau des sciences translationnelles de la Food and Drug Administration à explorer comment utiliser la technologie pour les données du dossier médical électronique (DME) que le projet pilote est actuellement en cours. Mis en œuvre dans quatre grands hôpitaux utilisant Ethereum.

(b) Blockchain et protection des données de santé

La relation entre les blockchains et le règlement général sur la protection des données (RGPD) est quelque peu controversée. D'une part, les blockchains semblent représenter un bon alignement avec le RGPD (en ce qui concerne la portabilité des données, par exemple, ou la gestion des consentements, la traçabilité des données et l'audibilité des accès légaux). En revanche, différents problèmes peuvent être

identifiés (lorsqu'il s'agit du droit à l'oubli, mais aussi lorsque la mise en œuvre technique via des contrats intelligents risque d'affaiblir le contrôle réel des données, via une exécution automatique). Une option pour résoudre ce problème est la «gestion dynamique du consentement», qui est pleinement conforme à la disposition du RGPD concernant le consentement. En outre, il est considéré que "les blockchains privées", par exemple, Entreprise Blockchain peuvent facilement se conformer aux directives du RGPD puisque les transactions des enregistrements numériques des informations stockées peuvent être modifiées et effacées par des entités ou des autorités privées qui peuvent posséder et contrôler cette plate-forme. En utilisant une classe particulière d'algorithme de consensus. Le potentiel des blockchains est également abordé par le projet pilote IMI (Innovative Medicine Initiative) du programme de recherche et d'innovation de la Commission européenne nommé «Blockchain Enabled Healthcare» dirigé par Novartis, qui vise à tirer parti des normes existantes, telles qu' Ethereum, et à développer des normes complémentaires si obligatoires. L'accent est mis sur la mise en place de services qui bénéficient directement aux patients.

(c) Blockchain pour la gestion des données du dossier de santé personnel (PHR)

Les données personnelles du journal de vie ont récemment commencé à être capturées via des capteurs portables ou des appareils IoT médicaux. Les applications distribuées ou décentralisées (Dapps) développées sur la blockchain permettent aux médecins et aux patients de participer facilement à la télémédecine sans frais d'intermédiaire mis à part les frais minimes du réseau Ethereum, améliorant ainsi l'autonomisation des patients.

(d) Blockchain pour la génomique au point de service

La plupart des entreprises de mHealth développant des services de blockchain ciblent le potentiel des patients à posséder et à vendre leurs données de santé en mettant l'accent sur les dossiers de santé électroniques (DSE) personnels et les profils de routine de bien-être collectés par des capteurs portables, ainsi que sur le génome personnel (à domicile). Selon Timi Inc., qui est une société de plateforme blockchain, les données d'un patient individuel sont estimées à 7 000 USD par an. Genomes.io est une autre société de blockchain de génomique qui permet aux consommateurs de stocker en toute sécurité leur génome à partir du moment où il

est séquencé, puis d'accorder l'accès de manière sélective. L'idée est d'éviter que les informations génétiques ne tombent entre de mauvaises mains, tout en donnant aux consommateurs la possibilité de vendre petit à petit leurs données génétiques s'ils le souhaitent.

(e) Blockchain pour la gestion des données de DSE

L'idée est de permettre aux individus de contrôler leurs données de santé aussi facilement que leurs comptes bancaires en ligne pour permettre une meilleure communication entre les organisations de santé et les soignants pour ouvrir la voie à un niveau de soins plus élevé, pourrait permettre aux patients d'être rémunérés avec des jetons pour leurs partages des données sur la santé avec les prestataires et leurs partenaires de recherche. Health Wizz pilote une application mobile d'agrégation de DSE compatible blockchain et FHIR, qui utilise des blockchains pour tokénize les données, permettant aux patients d'agréger, d'organiser, de partager, de faire un don et / ou d'échanger en toute sécurité leurs dossiers médicaux personnels.

2.6.1.4 Avantage

Les blockchains présentent cinq avantages potentiels par rapport aux systèmes de gestion de bases de données de soins de santé traditionnels.

(a) Les blockchains permettent une gestion décentralisée, ils conviennent aux applications où les acteurs de la santé souhaitent collaborer entre eux sans le contrôle d'un intermédiaire central de gestion.

(b) Les blockchains fournissent des pistes d'audit immuables, ils conviennent aux bases de données immuables pour enregistrer des informations critiques.

(c) Les blockchains permettent la provenance des données, ils sont adaptés à une utilisation dans la gestion des actifs numériques. La propriété ne peut être modifiée que par le propriétaire, suivant des protocoles cryptographiques. En outre, les origines des actifs sont traçables, ce qui augmente la réutilisabilité des données vérifiées.

(d) Les blockchains garantissent la robustesse et la disponibilité des données, ils conviennent à la conservation et à la disponibilité continue des documents.

(e) Ils augmentent la sécurité et la confidentialité des données, les données sont cryptées dans des blockchains et ne peuvent être décryptées qu'avec la clé privée du

patient.

2.6.1.5 Résultats

Les résultats montrent que de nouvelles plates-formes numériques basées sur des chaînes de blocs émergent pour permettre une interaction rapide, simple et transparente entre les fournisseurs de données, y compris les patients eux-mêmes.

2.6.2 L'article 2 : MedRec : Using Blockchain for Medical Data Access and Permission Management

2.6.2.1 Objectifs

Les dossiers médicaux ont besoin d'innovation, car la personnalisation et la science des données incitent les patients à s'impliquer dans les détails de leurs soins de santé et à reprendre le contrôle de leurs données médicales. Les patients et les prestataires de soins peuvent être confrontés à des obstacles importants lorsqu'il s'agit de récupérer et de partager des données, en raison d'incitations économiques qui encouragent le "blocage des informations de santé". Lors de la conception de nouveaux systèmes pour surmonter ces obstacles, nous devons donner la priorité à l'agence du patient [48].

2.6.2.2 Méthodes

Dans cet article, nous proposons MedRec : un nouveau système décentralisé de gestion des dossiers pour traiter les DME, en utilisant la technologie blockchain. Nous nous appuyons sur ce protocole de registre distribué associé à l'origine à Bitcoin. La blockchain utilise la cryptographie à clé publique pour créer une chaîne de contenu à appendice unique, immuable et horodatée. Des copies de la blockchain sont distribuées sur chaque "nœud" participant du réseau. Nous incitons les acteurs médicaux (chercheurs, autorités de santé publique, etc.) à participer au réseau en tant que "mineurs" de la blockchain. Cela leur permet d'accéder à des données agrégées et anonymes en tant que récompenses pour le minage, en échange du maintien et de la sécurisation du réseau via la preuve de travail.

2.6.2.3 Avantage

Notre mise en œuvre de la blockchain MedRec aborde les quatre problèmes majeurs soulignés ci-dessus :

- L'accès fragmenté et lent aux données médicales.
- L'interopérabilité des systèmes.
- L'agence des patients.
- L'amélioration de la qualité et de la quantité des données pour la recherche médicale.

Nous rassemblons des références à des données médicales disparates et les encodons sur un grand livre de la blockchain. Nous organisons ces références afin d'habiliter les individus à l'authenticité des dossiers, à l'audibilité et au partage des données.

2.6.2.4 Résultats

En s'appuyant sur la technologie blockchain, MedRec a montré comment les principes de décentralisation peuvent être appliqués à la gestion des données à grande échelle dans un système de DME. Notre mise en œuvre de la blockchain nous donne plusieurs propriétés clés de la décentralisation. MedRec bénéficie d'un solide modèle de basculement, s'appuyant sur les nombreuses entités participantes du système pour éviter un point de défaillance unique.

2.7 Conclusion

Face aux nombreux défis posés par le-santé, et face aux besoins suscités en termes de décentralisation, de traçabilité et de confiance, la blockchain offre des réponses. Sans avoir la prétention de résoudre tous les problèmes, elle ouvre également la porte vers de nouveaux horizons. De ce fait, elle présente des champs d'investigation inédits aux acteurs du domaine.

Chapitre 3

Conception

3.1 Introduction

Dans ce chapitre, nous avons cherché à concevoir un système basé sur la technologie blockchain pour la gestion des données médicales qui pourrait donner le contrôle final des données médicales aux patients et garantir la vie privée de ces derniers. Donc, on va présenter l'architecture générale de notre système, ainsi que les différents diagrammes, à savoir les diagrammes de cas d'utilisation et le digramme séquence. Ensuite, nous allons réaliser l'application et nous terminons par une conclusion.

3.2 Problématique et objectif

3.2.1 Problématique

Le plus grand défi des systèmes de soins de santé est de savoir comment partager des données médicales avec des parties (laboratoires, médecins, hôpitaux, assurances, patients) prenantes tout en garantissant l'intégrité des données et la protection de la vie privée des patients.

3.2.2 Objectif

Dans ce travail, on va proposer un nouveau système simple basé Blockchain pour assurer la gestion des données médicales.

3.3 Acteurs du système

L'architecture proposée de notre système se compose de :

- Administrateur : Fais l'organisation de système et donne l'autorisation d'accès.
- Le patient : Notre système se compose de plusieurs patients qui se soignent chez les médecins traitants de ce réseau, consulter ou récupérer des données de leurs dossiers et contacter les médecins.
- Professionnels de santé :
  1. Le médecin : Notre système se compose de plusieurs médecins traitants, chaque médecin peut ajouter des informations médicales.
  2. L'hôpital : Ajouter des informations médicales, consulter ou récupérer des données.
  3. Laboratoire : Rédige les analyses des patients sur la blockchain.
  4. L'assureur : Vérification du règlement des traitements et des paiements.
  5. La pharmacie : Délivrés des médicaments et enregistre également l'opération sur la blockchain

3.4 Architecture Globale

On a choisi la plateforme privée pour notre système, les nœuds du système sont connus et validés par l'administrateur, chaque nœud de ce réseau possède une copie de la blockchain. La figure 3.1 représente l'architecture de notre système :

3.5 Contrat intelligent

Un contrat intelligent est le code avec lequel les applications interagissent pour lire et mettre à jour les données du grand livre de la blockchain. Un contrat intelligent peut transformer une logique d'entreprise en un programme exécutable qui est accepté et vérifié par tous les membres d'un réseau blockchain.

Les smart contracts et les DApps pourraient résoudre les principaux problèmes des écosystèmes de santé, le patient s'identifie avec son adresse (clé publique) et utilise un smart contract pour définir les conditions d'accès à son DME en le signant avec sa clé privée.

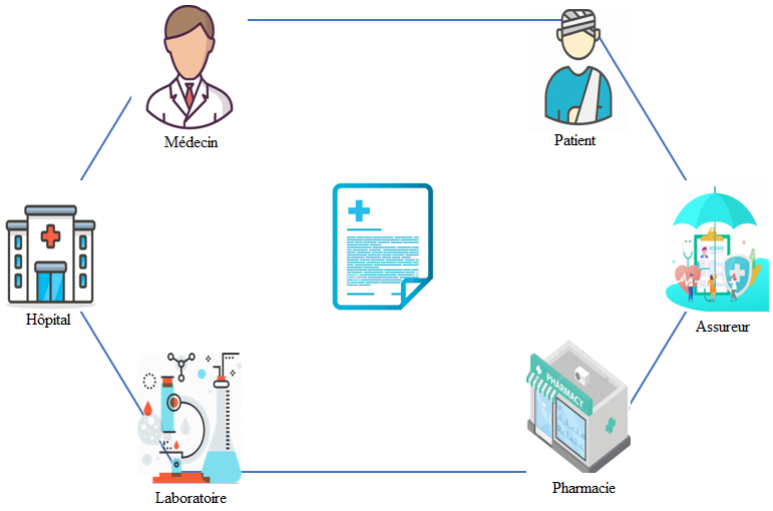


Figure 3.1 – Architecture Globale de système.

Le patient laisse son DME verrouillé par un verrou intelligent contrôlé par un contrat intelligent. Le DME a sa propre adresse blockchain (clé publique) stockée sur la blockchain.

Lorsque quelqu'un veut accéder au DME du patient ou être l'un des professionnels de la santé, il trouve le DME du patient répertorié sur internet. Il signe le contrat avec sa clé privée en le transférant de son adresse blockchain (clé publique) à l'adresse blockchain du patient.

Le contrat intelligent est accepté et vérifié par tous les membres d'un réseau blockchain.

Si le réseau reconnaît que toutes les conditions sont remplies, il obtient automatiquement le code d'accès au DME du patient. La blockchain l'enregistre comme nouvel acteur.

3.6 Fonctionnement global

3.6.1 Diagrammes de cas dutilisation

Dans cette partie du chapitre, on présente les diagrammes de cas pour définir les grandes fonctions d'un système

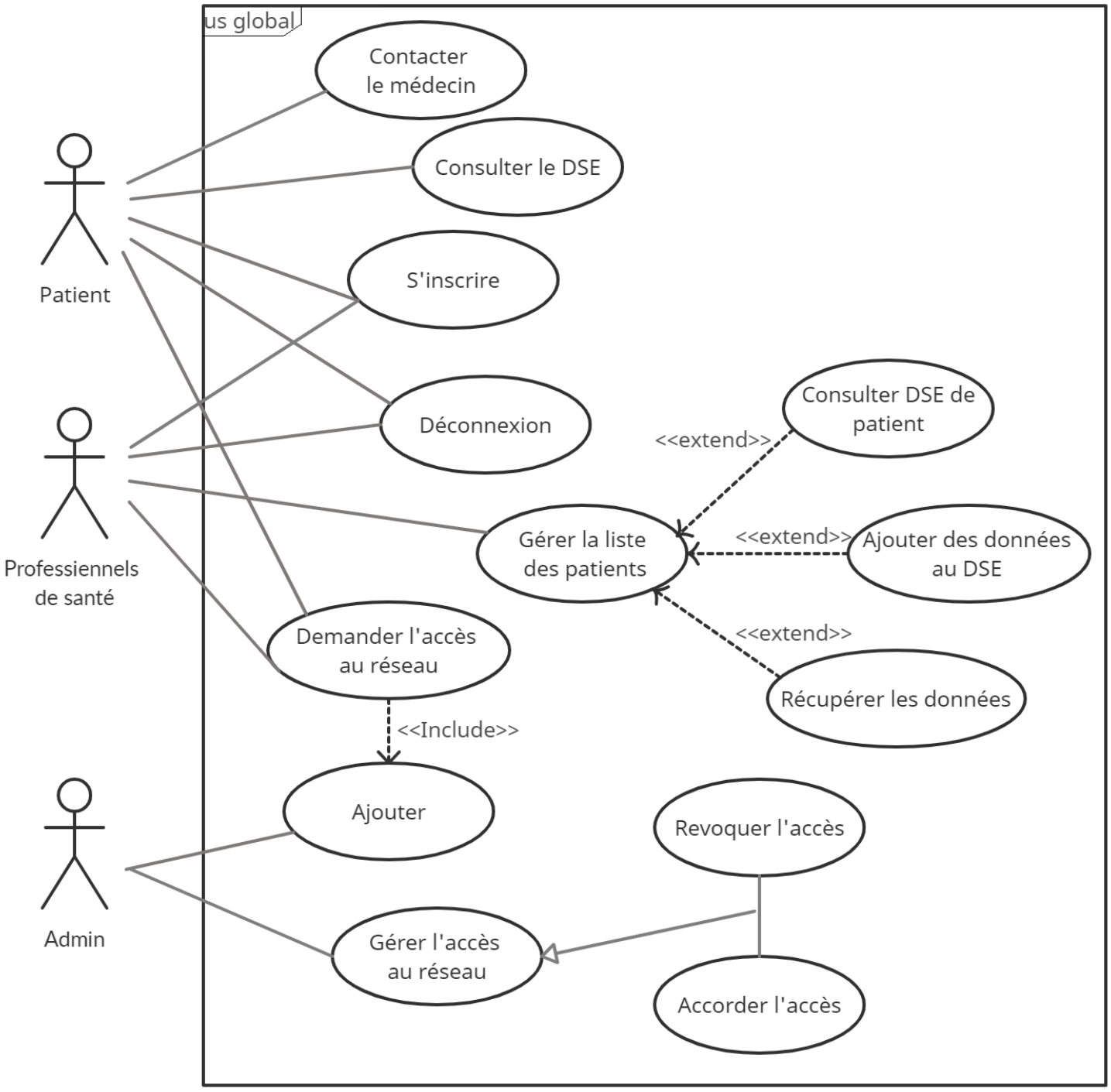


Figure 3.2 – Diagramme de cas d'utilisation de notre application.

3.6.2 Diagrammes de séquence

Dans ce qui suit, nous présenterons les diagrammes de séquences des cas d'utilisation les plus pertinents de notre système.

1. Diagramme de séquence de cas «Inscription».

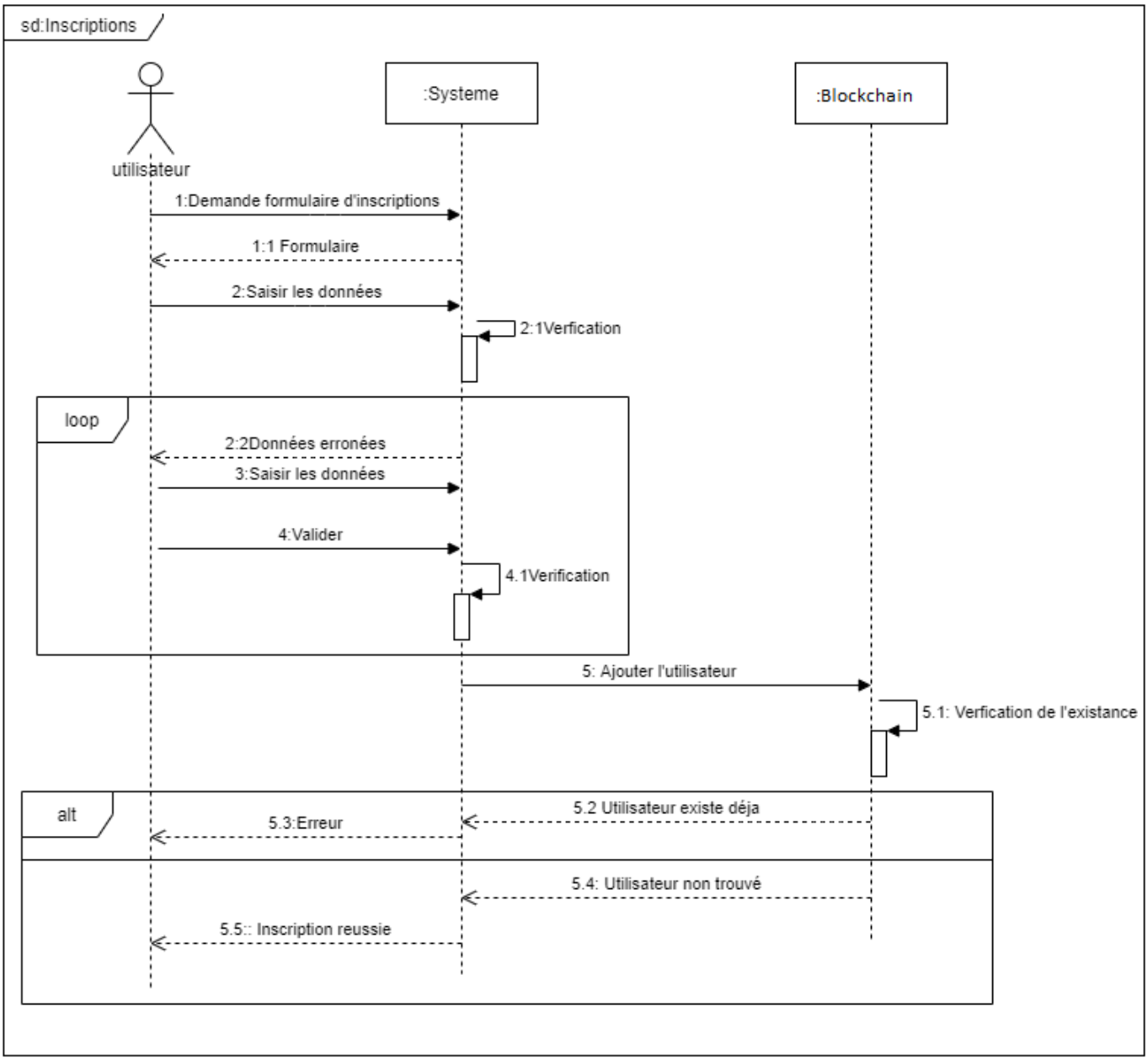


Figure 3.3 – Diagramme de séquence du cas «Inscription».

2. Diagramme de séquence du cas «Authentification»

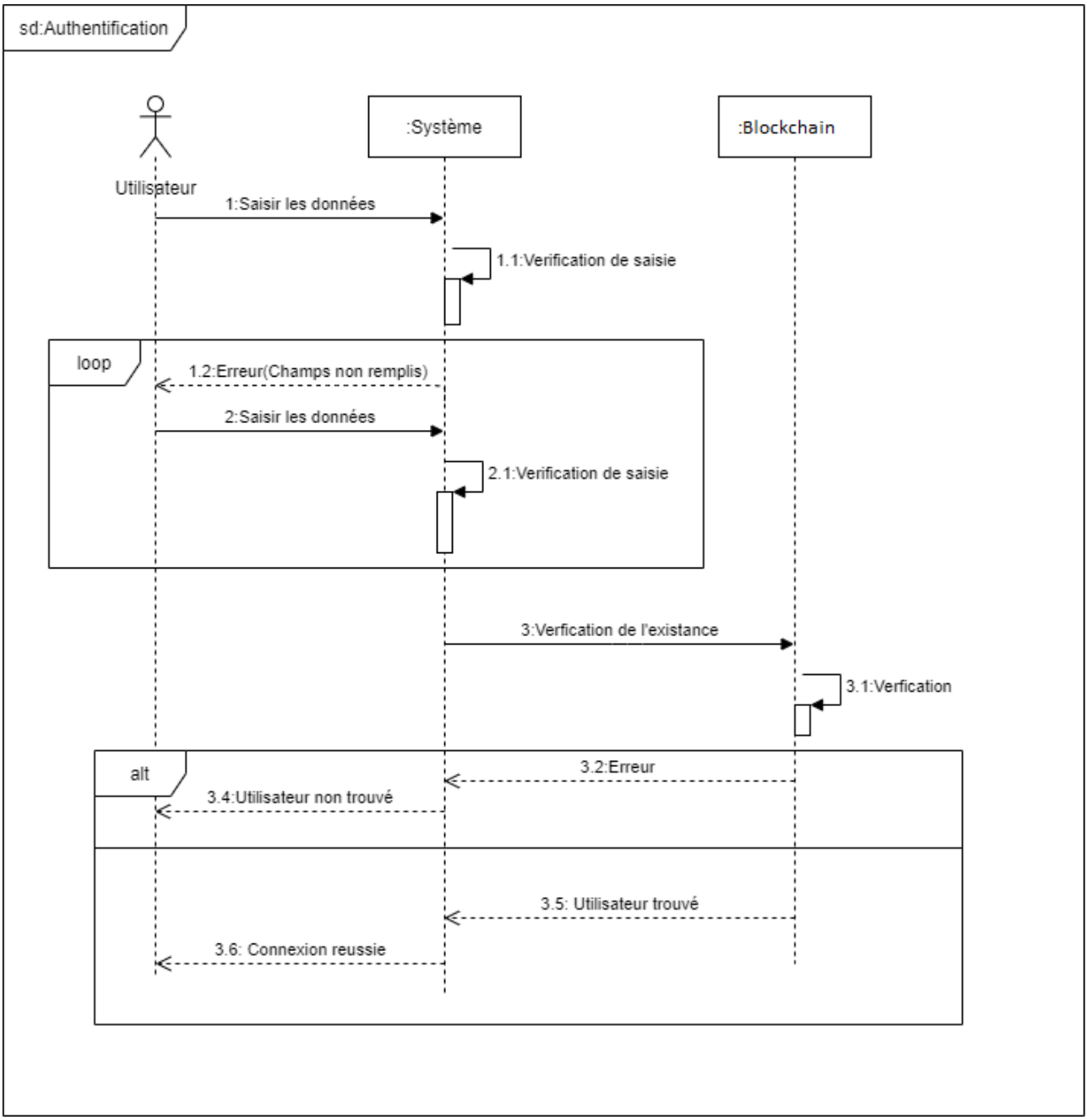


Figure 3.4 – Diagramme de séquence du cas «Authentification».

3. Diagramme de séquence du cas «Gestion des utilisateurs»

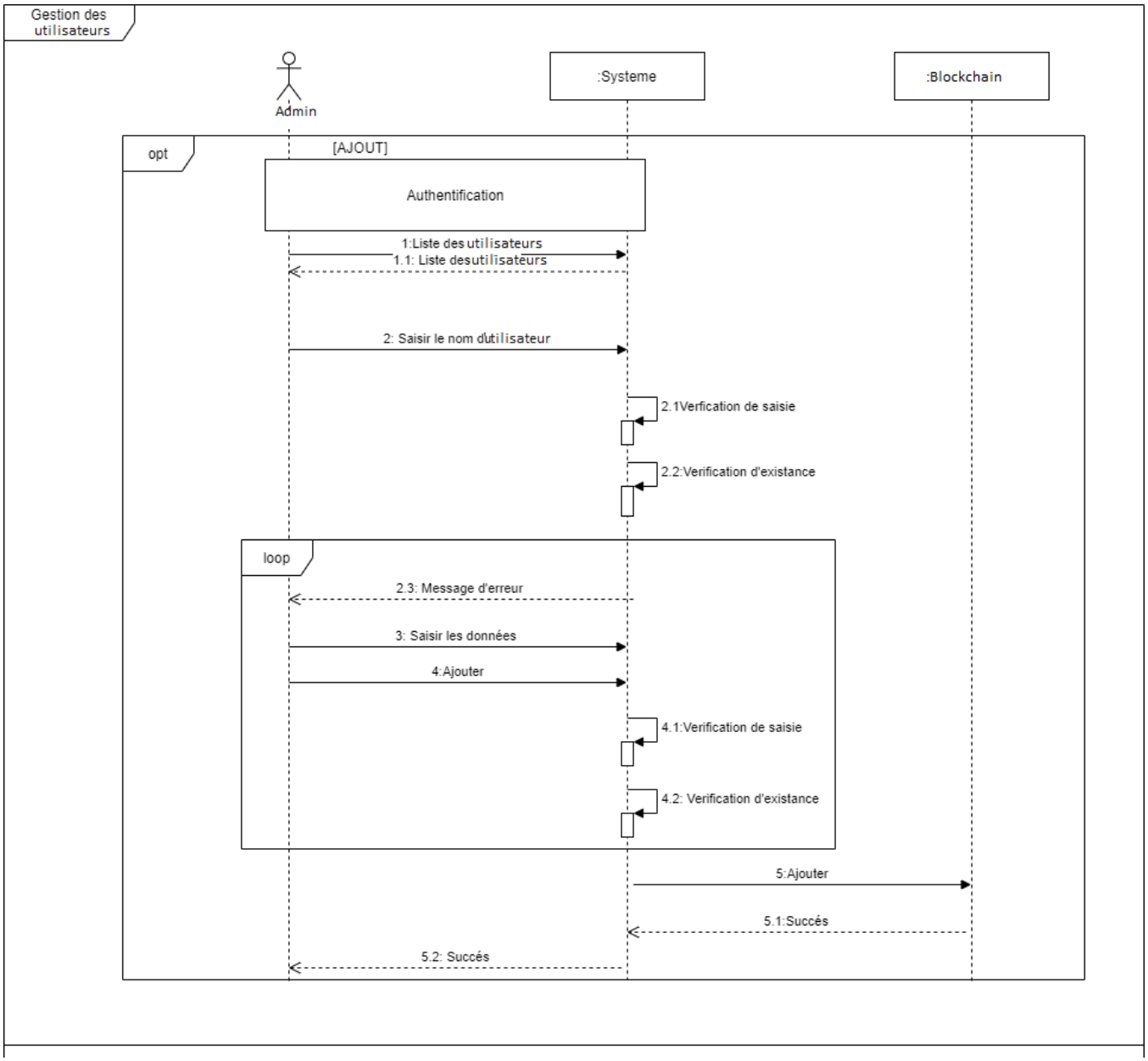


Figure 3.5 – Diagramme de séquence du cas «Gestion des utilisateurs».

4. Diagramme de séquence du cas « Écrire dans un DSE»

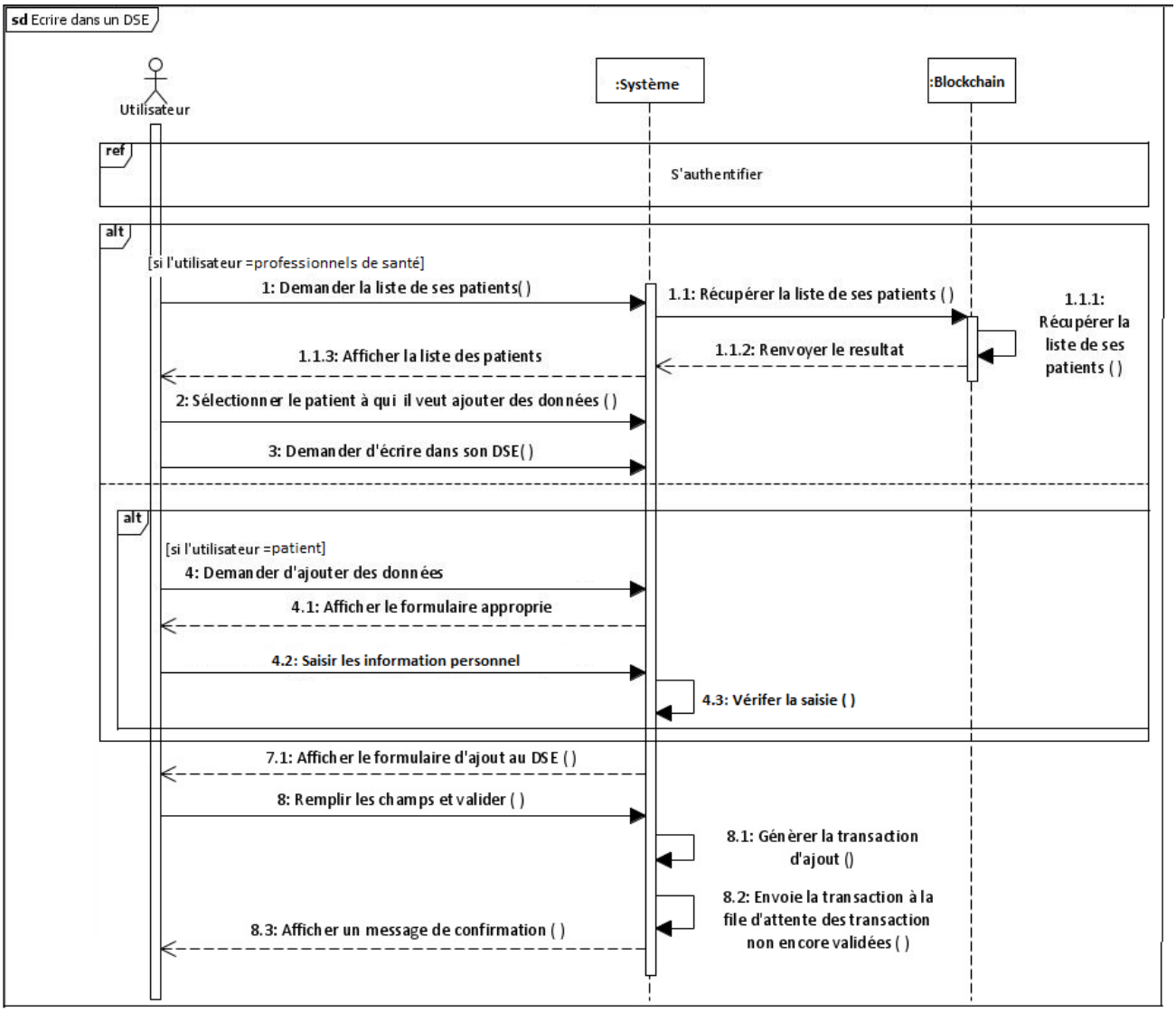


Figure 3.6 – Diagramme de séquence du cas «Écrire dans un DSE».

5. Diagramme de séquence du cas «Consulter un DSE »

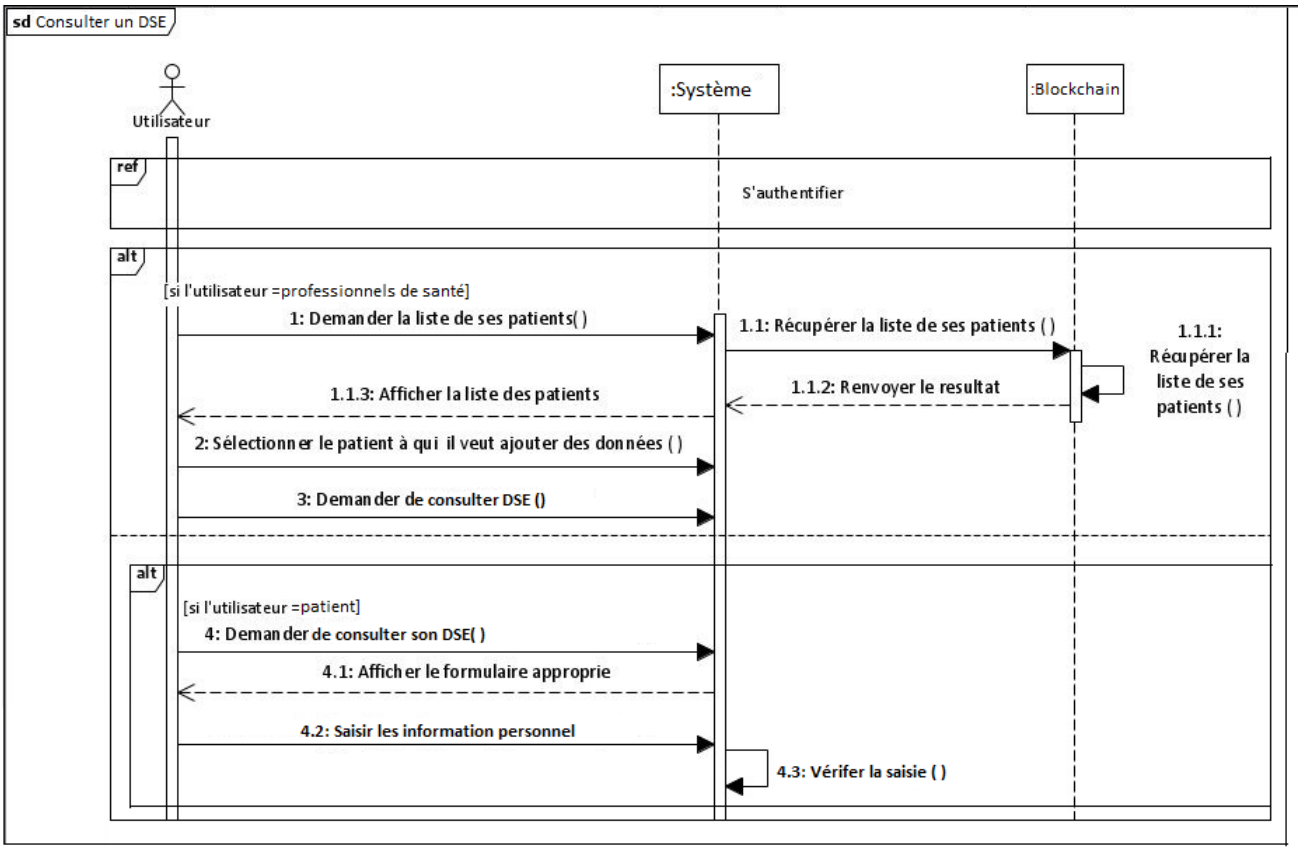


Figure 3.7 – Diagramme de séquence du cas «Consulter un DSE»

3.7 Architecture détaillée

3.7.1 Réseau Blockchain

Le dossier médical contient des informations médicales sensibles liées au patient qui sont stockées et partagées entre les participants tels que les patients, les médecins, les pharmacies ... la Blockchain donne un registre distribué entre toutes les entités impliquées dans le réseau.

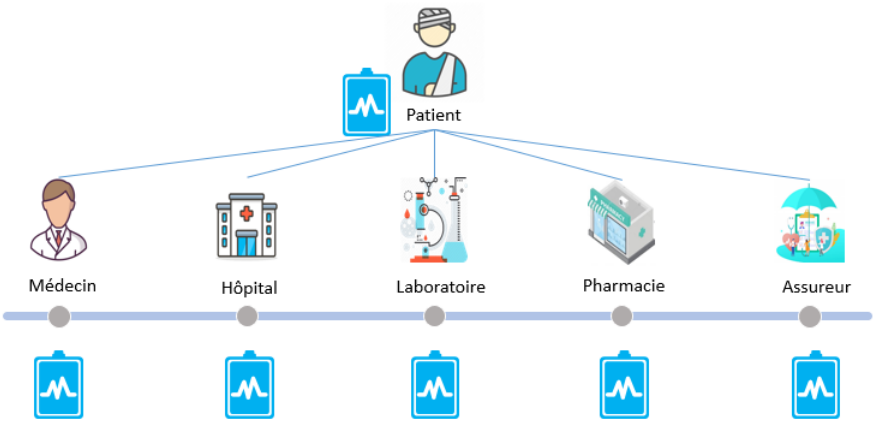


Figure 3.8 – Architecture «Réseau Blockchain».

3.7.2 Administrateur

À travers une interface web, il peut donne l'autorisation au différents participants pour accéder au DSE de patient.

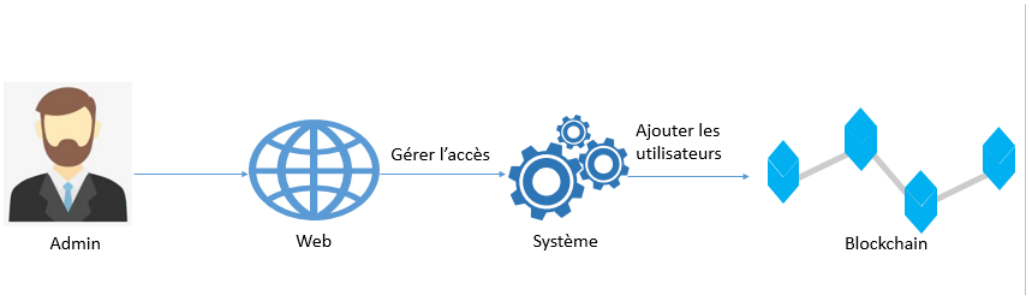


Figure 3.9 – Architecture noeud «Admin».

3.7.3 Patient

Grâce à une interface Web, le patient peut s'inscrire au système pour, voire son DSE, modifier son information (poids, l'âge, taille, tension artérielle...).

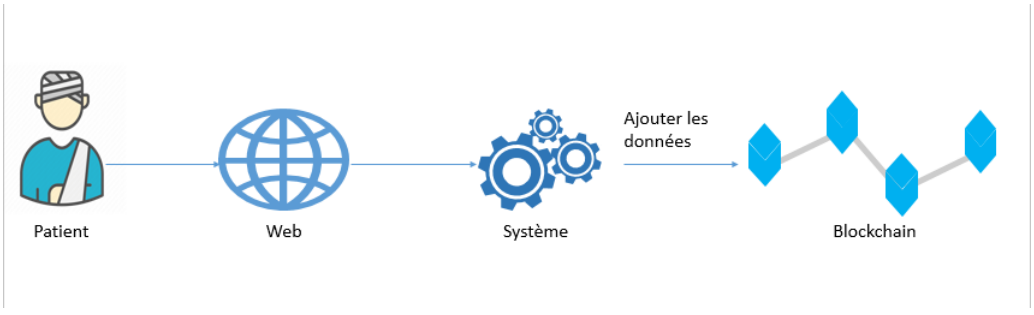


Figure 3.10 – Architecture noeud «Patient».

3.7.4 Professionnels de santé

Grâce à une interface Web, le professionnel de la santé peut simplement s'inscrire au système pour consulter ou ajouter au DSE.

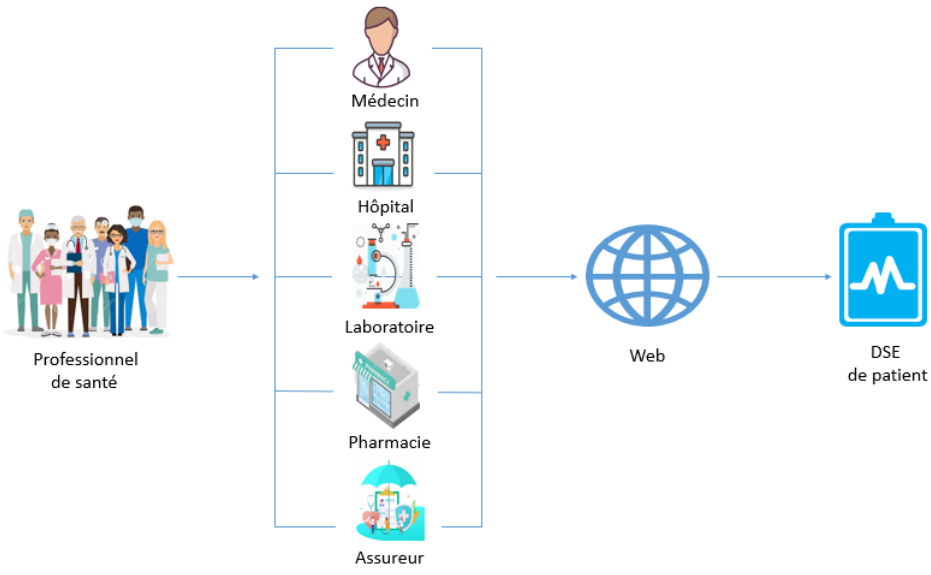


Figure 3.11 – Architecture noeud «Professionnels de santé».

3.8 Conclusion

Nous avons proposé une modélisation de notre système avec UML à travers les diagrammes de séquence, diagrammes de cas. On a présenté le développement de notre système. Le prochain chapitre fera l'implémentation et réalisation de notre système.

Chapitre 4

Implémentation

4.1 Introduction

Ce chapitre est consacré à la réalisation de l'application et va présenter l'implémentation du système, les outils de développement et quelques captures d'écran sur l'application réalisée.

4.2 Outils et Langages de programmation

Tout d'abord, Le projet est réalisé sur CPU 1.90 GHz 1.90 GHz Intel Core (TM) i3-4030U, avec 4 Go de mémoire. Nous implémentons le projet sous Windows 10. Les principaux outils et les langages que nous avons utilisés pour la réalisation de notre système sont les suivants :

4.2.1 Remix IDE

Est une application Web qui peut être utilisée pour écrire, déboguer et déployer des contrats intelligents Ethereum. (https ://remix.ethereum.org). Pour écrire du code dans **Solidity**, puis de le déployer sur une blockchain.

Figure 4.1 – Logo de Remix IDE et Solidity

4.2.2 Visual Studio Code

Est un éditeur de code source qui peut être utilisé avec une variété de langages de programmation, notamment Java, JavaScript, Node.js et C++. Elle est multi-plateforme, open source et gratuit.

Figure 4.2 – Logo de Visual Studio Code

4.2.3 Truffle

Est un pipeline d'actifs pour les blockchains utilisant la machine virtuelle Ethereum. Il permet aux développeurs de lancer un projet de contrat intelligent en un clic et vous fournit une structure de projet, des fichiers et des répertoires qui facilitent le déploiement et les tests.

Figure 4.3 – Logo de truffle

Pour installer truffle sous windows :

```
npm install -g truffle
```

4.2.4 Ganache

Est une blockchain personnelle pour le développement rapide d'applications distribuées Ethereum et Corda. Vous pouvez utiliser Ganache tout au long du cycle de développement ; vous permettant de développer, déployer et tester vos applications distribuées dans un environnement sûr et déterministe.

Ganache UI est une application de bureau prenant en charge les technologies Ethereum et Corda.

Figure 4.4 – Logo de Ganache

Après l'installation vous devriez voir la page d'accueil de Ganache !

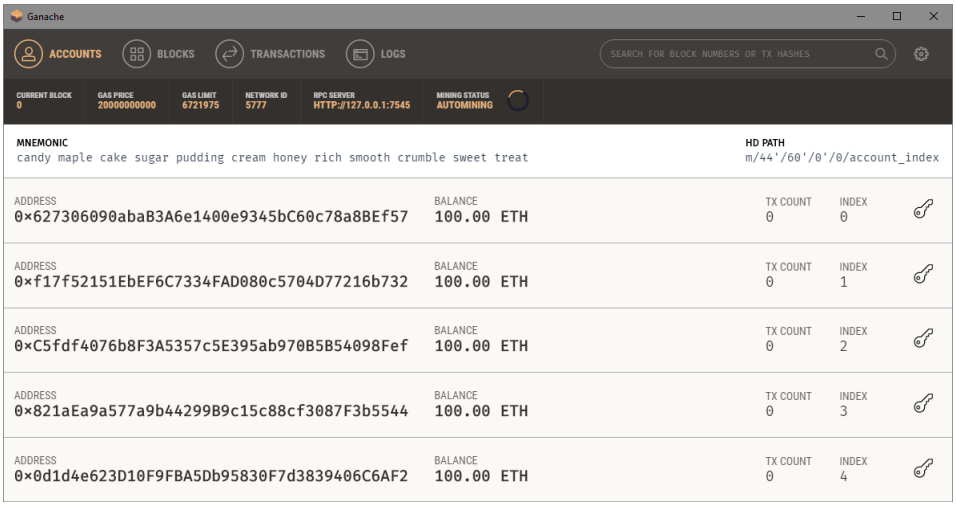


Figure 4.5 – La page d'accueil de Ganache

4.2.5 Node.js

Est une plate-forme basée sur le moteur d'exécution JavaScript de Chrome pour créer facilement des applications réseau rapides et évolutives. Nous devons configurer notre environnement pour développer des contrats intelligents. La première dépendance dont nous aurons besoin est Node Package Manager (NPM), fournie avec Node.js.

Figure 4.6 – Logo de Node js

La première dépendance dont nous aurons besoin est Node Package Manager (NPM) et système de fichier interplanétaire (IPFS), fournie avec Node.js.

NPM est le gestionnaire de packages pour la plate-forme Node JavaScript. Il met des modules en place pour que le nœud puisse les trouver et gère intelligemment les conflits de dépendances.

IPFS est un système distribué permettant de stocker et d'accéder à des fichiers, des sites Web, des applications et des données.

Après l'installation de nodejs, npm et ipfs on utilise invite de commade pour, voire les versions.

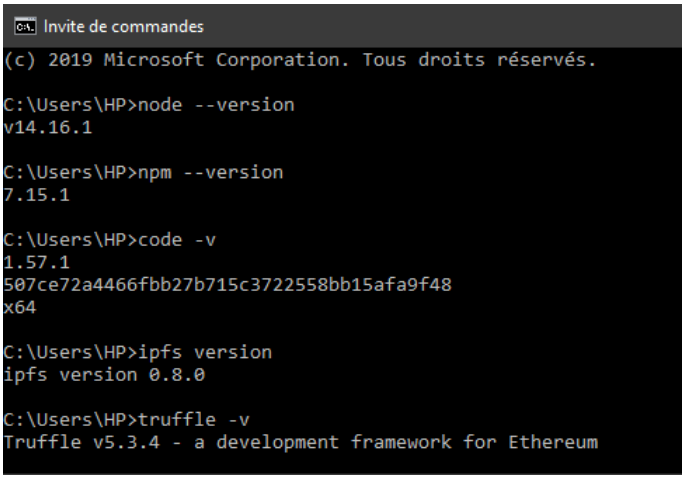


Figure 4.7 – Les version des outiles

4.2.6 React

Est une bibliothèque JavaScript permettant de créer des interfaces utilisateur interactives. Il aide les développeurs à définir des interfaces telles que des fonctions et des procédures.

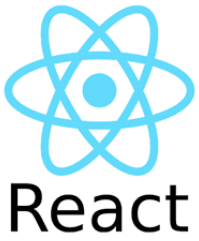


Figure 4.8 – Logo de React

4.2.7 MetaMask

Est une extension pour accéder aux applications distribuées activées par Ethereum, ou ”DApps” dans votre navigateur.

Figure 4.9 – Logo de MetaMask

Après avoir créé un compte, vous devriez vous retrouver sur la page principale de MetaMask.

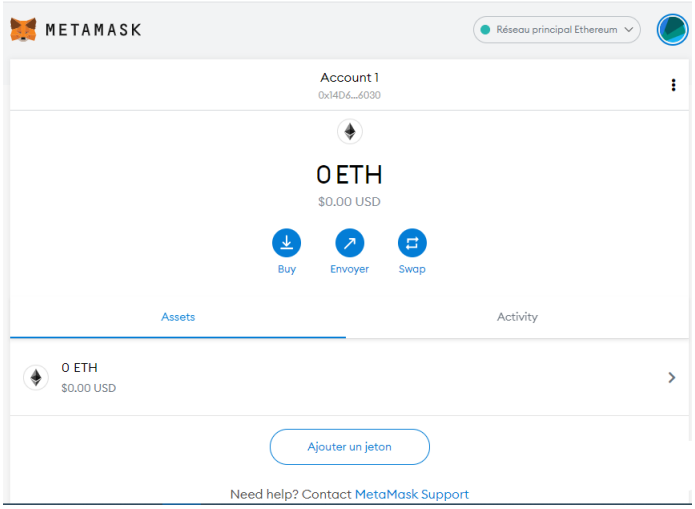


Figure 4.10 – Interface de MetaMask

4.3 Description du système

Notre but, dans ce système est de concevoir une application avec blockchain pour le contrôle, stockant et partageant des dossiers médicaux électroniques des patients facilement entre les professionnels de santé. Et Il permet également de fournir des informations médicales (antécédents médicaux, résultats d'analyses de laboratoire, imagerie, traitement en cours etc...).

4.4 Configuration de l'environnement

Dans cette partie nous allons présenter à l'aide des interfaces et les étapes nécessaires, un aperçu de notre système.

4.4.1 Créer le projet DSEsanté

Tout d'abord, créez un dossier nommé DSEsante et démarrez un projet npm dans le dossier DSEsante en tapant les commandes suivantes ci-dessous dans le terminal :

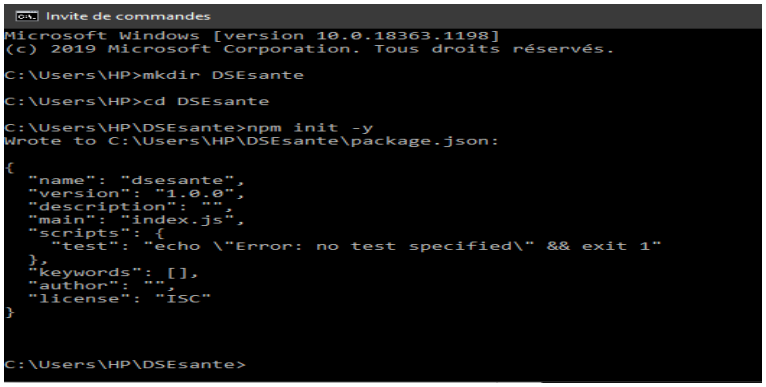


Figure 4.11 – Créer mon projet DSEsanté

Npm-install cette commande installe un package et tous les packages dont il dépend.

```
npm install
```

Express est un framework d'applications Web Node.js qui aide à développer des applications Web. C'est un serveur HTTP minimaliste.

```
npm install express --save
```

Web3.js nous aide à développer des sites Web ou des clients qui interagissent avec la blockchain - en écrivant du code qui lit et écrit des données à partir de la blockchain avec des contrats intelligents.

```
npm install web3 --save
```

- ”loadWeb3()” : la fonction de configuration Web3 permettre à communiquer avec la blockchain.
- ”contract = new web3.eth.Contract(contractAbi, contractAddress)” : la fonction qui lire les données des contrats intelligents avec Web3.js.

4.4.2 Vérifiez package.json

Après les installations, j’ouvrirai le dossier du projet nommé DSEsante in VSCode et vérifierai le fichier package.json qui est un fichier créé par npm avec certaines configurations, y compris les packages que nous avons installés.

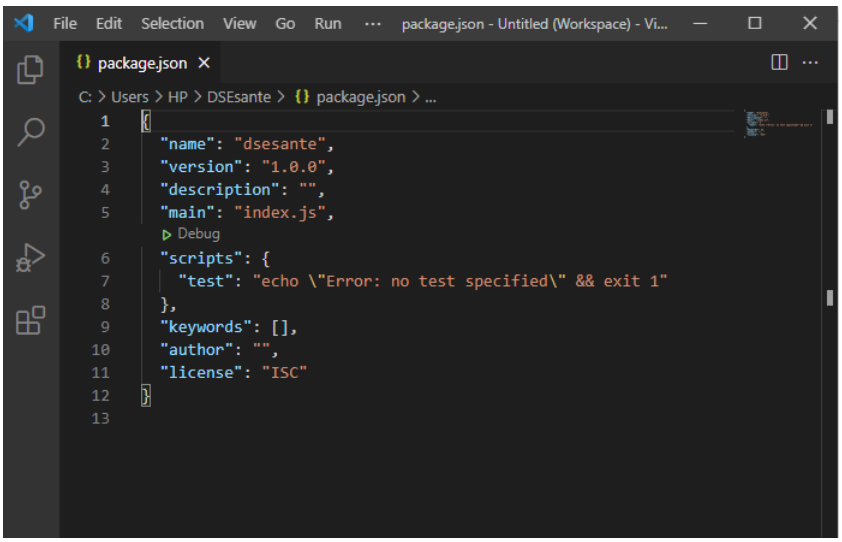


Figure 4.12 – package.json

4.4.3 Développer notre projet

Nous exécutons truffle init, cela configurera la structure de base dans notre répertoire.

```
truffle init
```

On va voire :

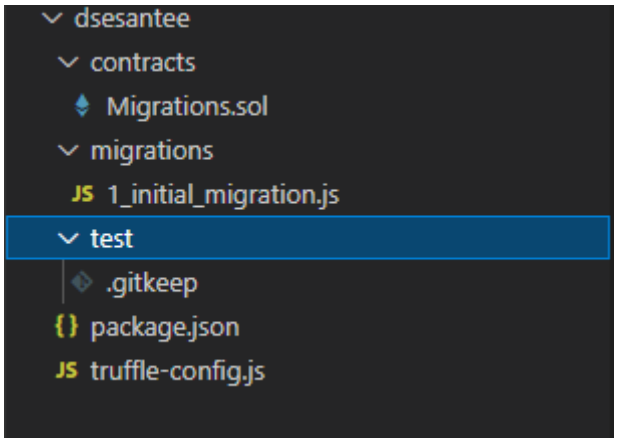


Figure 4.13 – Structure du répertoire

4.4.4 Déployer un contrat intelligent

Pour construire une application de chaîne d'approvisionnement décentralisée, nous créons d'abord le contrat intelligent Ethereum, dans le répertoire "Contracts".

À l'intérieur du formulaire de contrat, nous définissons les variables et les fonctionnalitées et fournir le code pour la structure de chaque fonction.

Nous avons déclaré "acteur" en tant que variable qui effectue une connexion à notre système avec la fonction "setLogin".

```
pragma solidity 0.5.4;

contract login {

      mapping(uint => acteur) public acteurs;

    struct acteur{


        string nom;
        string motdepasse;
    }


  function setLogin(string memory _nom , string memory _motdepasse) public {

        // Require a valid name
        require(bytes(_nom).length > 0);
        // Require a valid mot de passe
        require(bytes(_motdepasse).length > 0);

    }
}
```

Figure 4.14 – Fonction de login

Si l'acteur n'exist pas il va inscrire avec la fonction "Inscription". Par entrant : le nom, le prénom, pour la case "acteur" Chacun choisit une des options selon sa condition :(patient, médecin, laboratoire, pharmacie, assureur, hôpital), l'adresse, numéro de téléphone et l'email.

```
pragma solidity 0.5.4;


contract Inscription {


    mapping(uint => acteur) public acteurs;


    struct acteur{

        string nom;
        string prenom;
        string acteur;
        string addr;
        uint tele;
        string email;
    }



    function setInformation(string memory _nom , string memory _prenom ,
    string memory _acteur ,string memory _addr , uint _tele , string memory _email) public {

    }
}
```

Figure 4.15 – fonction d'inscription

L'administrateur recevoir touts les demandes d'inscription et il l-accepter et envoyer des mails a les demandeurs.

```
pragma solidity 0.5.4;

contract Admin {
    string private acces;


 function ajouteAuBlockchain(string memory _acces) public {
     acces = _acces;

    }

}
```

Figure 4.16 – fonction d'ajouter

Les professionnels de santé après l'entrure au dossier de patient, ils ajoutent des fichiers qui continents des radios, analyses, médicaments ... Les variables déclaré des fichiers ajoutés sont : identificateur , hachage, la taill, type, le nom, description , le temps d'ajouter et l'adresse de l'acteur qui ajouter ce fichier.

```
struct File {
  uint fileId;
  string fileHash;
  uint fileSize;
  string fileType;
  string fileName;
  string fileDescription;
  uint uploadTime;
  address payable uploader;
}
```

Figure 4.17 – les variables de dossier médecal

Et pour la fonction ”uploadFile”, il obtient toutes les dernières variables et les ajoute au contrat intelligent. Et l’afficher après.

```
function uploadFile(string memory _fileHash, uint _fileSize, string memory _fileType, string memory _fileName, string memory _fileDescription)
    //Assurez-vous que le hachage du fichier existe
  require(bytes(_fileHash).length > 0);

    // Assurez-vous que le type de fichier existe
  require(bytes(_fileType).length > 0);

    // Assurez-vous que la description du fichier existe
  require(bytes(_fileDescription).length > 0);

    // Assurez-vous que le fichier fileName existe
  require(bytes(_fileName).length > 0);

    //Assurez-vous que l'adresse de l'uploader existe
  require(msg.sender!=address(0));

    // Assurez-vous que la taille du fichier est supérieure à 0
  require(_fileSize>0);

    // Incrémenter l'identifiant du fichier
  fileCount ++;

    // Ajouter un fichier au contrat
  files[fileCount] = File(fileCount, _fileHash, _fileSize, _fileType, _fileName, _fileDescription, now, msg.sender);

    // Déclencher un événement
  emit FileUploaded(fileCount, _fileHash, _fileSize, _fileType, _fileName, _fileDescription, now, msg.sender);
}
```


Figure 4.18 – Fonction d’ajouter au dossier médical

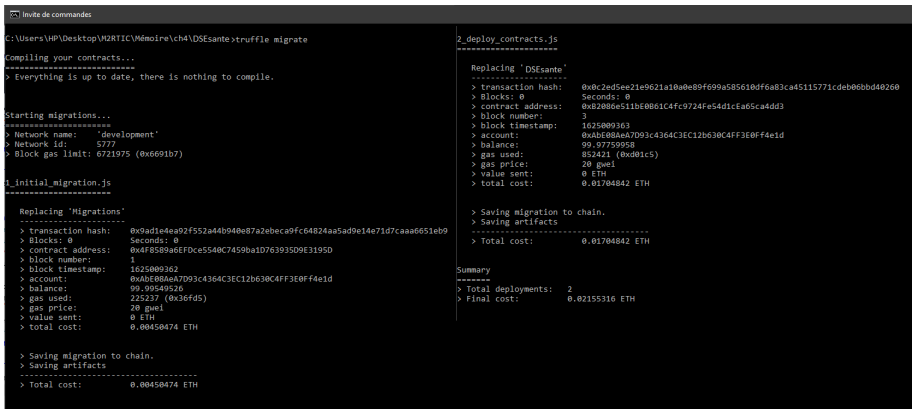
4.4.5 Exécuter le projet DSEsanté

- Tout d’abord, pour compiler le contrat intelligent et s’assurer qu’il n’y a pas d’erreurs, nous exécutons ce script de compilation depuis la ligne de commande : truffle compile

```
C:\Users\HP\Desktop\M2RTIC\Mémoire\ch4\DSEsante>truffle compile

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.
```

- Puis pour migrer le contrat intelligent vers le réseau blockchain personnel, nous lançons ce script de migration depuis la ligne de commande : truffle migrate



- Enfin pour démarrer notre projet nous exécutons la commande suivante : npm run start

4.5 Les interfaces du système

Dans cette partie, nous allons présenter quelques interfaces, commençant par l'accueil.

1. Page d'accueil

   Représente la page principale de notre site elle offre la possibilité au utilisateur (admin, patient, professiennels de santé) d'acceder chacun au sa espace pour saisir les informations et de passer vers les pages d'inscription ou d'authentification.

Figure 4.19 – Page daccueil

2. Page d'administrateure

   Si vous êtes un administrateur, vous pouvez avoir la liste des demandes d'accès aux notre blockchain. Et vous pouvez accéder à vos informations personnelles pour les modifier si vous voulez.

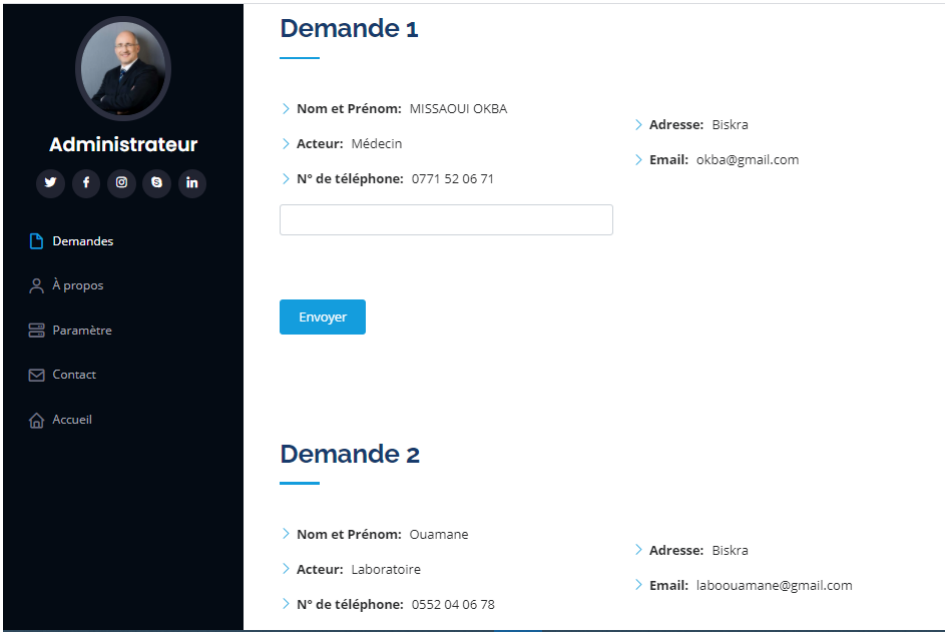


Figure 4.20 – Page d'administrateure

3. Page connexion

   Lorsque vous avez déjà un compte soit un professionnel de santé, oubient un patient vous pouvez l'accéder à travers set page.

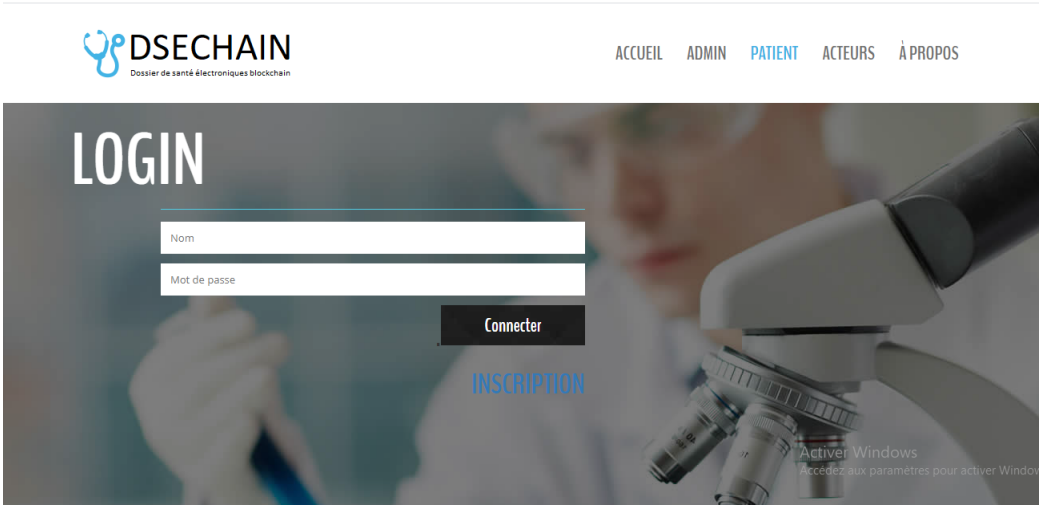


Figure 4.21 – Page connexion

4. Page d'inscription

   A partir de cette page l'utilisateur peut créer un compte en saisissant quelques informations personnelles comme le nom, prénom, mot de passe, email, l'adresse, némuro de téléphone ainsi que son identité (patient, médecin, pharmacie ...).

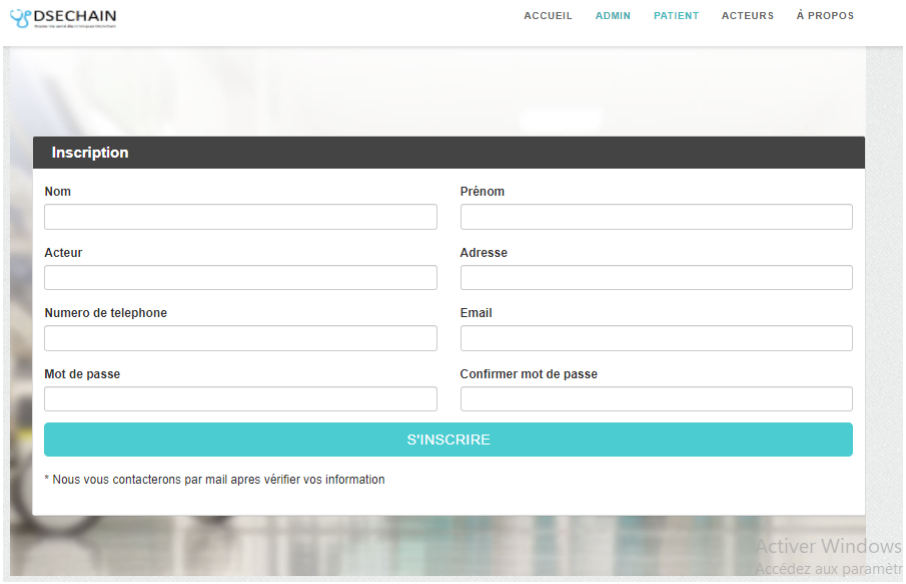


Figure 4.22 – Page d'inscription

5. Page patient

   C'est la page qui montre que le patient est déjà dans notre système. Il trouve une liste des professionnels de santé qui peuvent ajouter des données médicales ou consulter à son dossier de santé électronique stocké sur la blockchain. Il peut aussi modifier ses informations ou contacter les médecins.

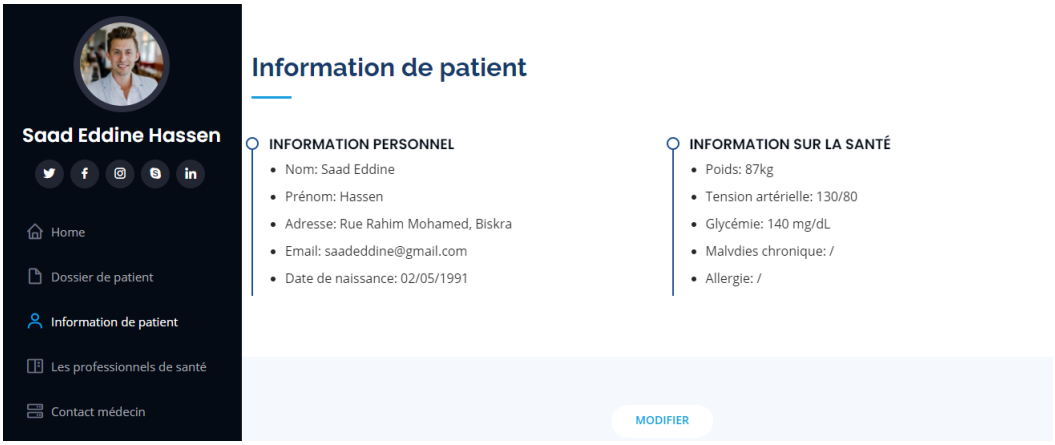


Figure 4.23 – Page de patient

6. Page dossier de patient

   Les professionnels de la santé ajoutent des dossiers médicaux à cette page, et les dossiers médicaux ont un nom, une taille et un téléchargeur qui a ajouté ce fichier.

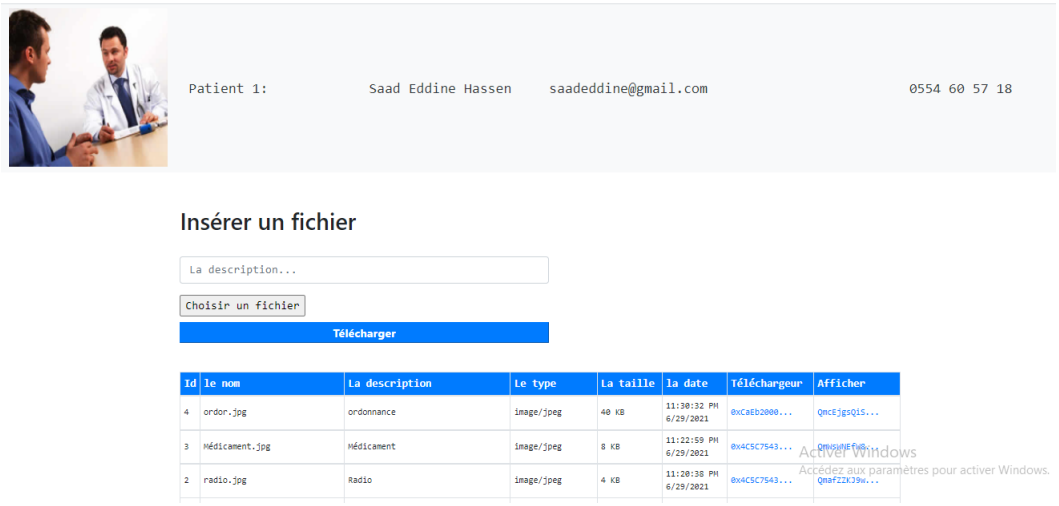


Figure 4.24 – Page dossier de patient

4.6 Conclusion

Dans ce chapitre, nous avons réalisé un système de blockchain en utilisant les outils de développement cités plus haut. Ce qui nous a permis d'obtenir un système de suivi des patients et qui offre la possibilité de faire la collection de style de vie d'un patient et de faire une liaison entre les professionnels de santé et les patients.

Conclusion générale

Le secteur de la santé en particulier contient des données très sensibles et privées. En effet, la plupart des données médicales sont stockées dans différentes institutions médicales, ce qui entraîne leur dispersion. Et cela rend difficile pour les patients d'acquérir tous leurs dossiers médicaux auprès des diverses institutions médicales qu'ils ont visitées.

Pour cette raison, on a exploré les techniques de la blockchain, c'est une technologie permettant de stocker et de transmettre des informations de manière transparente et sécurisée sans modification ou suppression des données.

Notre travail était de réaliser un système de gestion des dossiers de santé électroniques des patients en utilisant la technologie blockchain. Pour cela, nous avons réalisé un système qui se compose d'un site web pour la gestion de DSE des patients et une blockchain pour le stockage des données médicales des patients.

Ce projet a été très bénéfique pour nous, car il nous a permis de renforcer et enrichir nos connaissances théoriques dans le domaine de la blockchain et les crypto-monais, ainsi que dans le domaine de la conception. Il nous a encore donné l'occasion d'apprendre quelques principes de la cryptographie et les appliquer dans notre réalisation.

Donc, pour la raison de la situation sanitaire que nous vivons actuellement et pour le manque de moyens de communications et de recherche, nous n'avons pas pu réaliser certains points dans notre application. Donc telle qu'elle est actuellement, elle offre un minimum de services et reste toujours perfectible. Au terme de notre travail, on énonce des perspectives :

- Remplacer la saisie des clés des membres (clé publique et clé privée) de la blockchain par un code à scanner (un code QR ou en utilisant la carte chifa).
- Utiliser et bénéficier du Cloud pour résoudre le problème du stockage des données médicales.

Bibliographie

[1] Sofia DELLYS, Sabrina et BENBOUABDELLAH. *Applications de la technologie blockchain*. PhD thesis, Université Akli Mohand Oulhadje-Bouira, 2020.

[2] Oussama Abderraouf Ayad. État de l'art de la blockchain. Master's thesis, Université Constantine 2, 2019.

[3] Marion PIGNEL. *LA TECHNOLOGIE BLOCKCHAIN Une opportunitépour l'économie sociale ?* JUIN 2019.

[4] Sirine HAMLAOUI. Blockchain for the drug supply chain management. Master's thesis, Université Mohamed khieder -BISKRA-, 2020.

[5] SIDI AISSA Ikram et KEDDAR Souria. Proposition d'un système à base de blockchain pour la gestion des opérations sur les véhicules au niveau national. Master's thesis, Université Aboubakr Belkaïd– Tlemcen – Faculté de technologie, juin 2018.

[6] Quelles sont les entreprises leader dans la technologie blockchain. `https://hubinstitute.com/2020/hubday/retail/replay-blockchain-cryptomonnaie-entreprise-bitcoin`. Accessed : 2021-01-28.

[7] GHOGGALI BRAHIM EL KHALIL. SystÈme des crÉdits ban-caire basÉ sur la technologie blockchain. Master's thesis, Université Mouhammed Khide -Biskra- Fac-ulte des Sciences Exactes et science Naturelle et de la Vie, 2020.

[8] M'HAMED MANCER. Conception et réalisation d'un modèle de blockchain intelligent. Master's thesis, Université Mohamed khieder -BISKRA-.

[9] How transactions are verified in bitcoin blockchain - longest chain rule ex-plained. Accessed : 2021-01-12.

[10] La blockchain de bitcoin : fonctionnement et caractéristiques, bitconseil. https://bitconseil.fr/blockchain-bitcoin/, 2019-10-12. Accessed : 2021-01-12.

[11] AHMED OUAZZANI. La blockchain : Applications dans lesecteur financier. Master's thesis, Université bdelmalek Essaadi LA FACULTÉ POLYDISCI-PLINAIRE À LARACHE, 2018.

[12] Ameer Rosic. What is hashing? https://blockgeeks.com/guides/what-is-hashing/, 2020-05-04.

[13] Alexander Marko. What is the algorithm sha 256. explain the miningcrypto algorithms. Accessed : 2021-01-20.

[14] Qu'est-ce que la blockchain?, lafinance pour tous. ,https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles\%20economies/blockchain/quest-ce-que-la-blockchain/, 2020-01-23.

[15] Amelia Wallace. Protection of personal data in blockchain technology : An investigation on the compatibility of the general data protection regulation and the public blockchain. Master's thesis, Université stockholm, 2018.

[16] Ameer Rosic. Smart contracts : The blockchain technology that will re-place lawyers, blockgeeks. https://blockgeeks.com/guides/smart-contracts/, 2020-11-25.

[17] Cedric Strub. Contribution de la blockchain au management des donnéesde santé. Master's thesis, Université Strasbourg, july 2020.

[18] SAMUEL CANGÉ. Pourquoi les contrats intelligents sont aussi impor-tants pour la blockchain? https://cryptonaute.fr/pourquoi-les-contrats-intelligents-importent-pour-la-blockchain/, 2020-11-12. Accessed : 2021-01-25.

[19] Matthieu QUINIOU et Christophe DEBONNEUIL. Blockchain. https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf, 2019-04.

[20] Alain Ceccato. Le dictionnaire des développeurs. https://dico.developpez.com/html/812-Securite-chiffrement-symetrique.php, 2005-03-14.

[21] FRAN RAJEWSKI. Coup de projecteur sur les rançongiciels : les modes de chiffrement. https://blog.emsisoft.com/fr/27699/rancongiciels-chiffrement/, 2017-06-21.

[22] Massimo Musumeci. Comment fonctionne la signature numérique. https://blogs.pme.ch/massimo-musumeci/2020/08/06/comment-fonctionne-signature-numerique/, 2020-08-06.

[23] Équipe d'assistance SSL. Qu'est-ce qu'une fonction de hachage cryptographique ? https://www.ssl.com/fr/faq/qu\%27est-ce-qu\%27une-fonction-de-hachage-cryptographique/, 2015-11-10.

[24] Quelle est la différence entre une blockchain privée et publique ? https://www.luno.com/learn/fr/article/what-is-the-difference-between-a-private-and-public-blockchain. Accessed : 2021-01-23.

[25] Blockchain privées, publiques et à consortium — quelles sont les différences ? https://academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference#consortium-blockchains. Accessed : 2021-01-24.

[26] Blockchain. https://www.ionos.fr/digitalguide/web-marketing/vendre-sur-internet/blockchain/, 2018-09-20.

[27] l'Université Paris 2. Les domaines d'application de la blockchain. https://www.masterassasfinance.com/single-post/2018/03/08/Les-domaines-dapplication-de-la-Blockchain, 2021-03-17.

[28] Cas d'usage pour la blockchain (partie i). https://solutions.lesechos.fr/tech/c/cas-dusage-blockchain-partie-i-10382/, 2018-02-19.

[29] Christopher Rodriguez. Blockchain un danger pour l'industrie bancaire et la banque privée ? Master's thesis, Université Paris, july 2017.

[30] Bitcoin : la mise à jour taproot promet de nouvelles fonctionnalités. https://www.journaldunet.com/patrimoine/guide-des-finances-personnelles/, 2021-06-15.

[31] Bitcoin et monnaie virtuelle : Comment investir dans la crypto monnaie ? https://www.cafedelabourse.com/archive/article/bitcoins-monnaie-virtuelle-investir-crypto-monnaie, 2021-06-18.

[32] JAKE FRANKENFIELD. Hyperledger fabric. https://www.investopedia.com/terms/h/hyperledger-fabric.asp, 2021-03-21.

[33] Anca Petre et Nassima Haï. Opportunités et enjeux de la technologie blockchain dans le secteur de la santé. https://doi.org/10.1051/medsci/2018204, 2018-11-19.

[34] et autres Xia Q, Sifah E. Blockchain-based data sharing for electronic medical records in cloud environments. information. 44, 2017.

[35] Koo MB Linn LA. Blockchain for health data and its potential use in health it and health care. :https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf, 2021-01-07. Accessed : 2021-04-06.

[36] et autres Brodersen C, Kalis B. Blockchain : Securing a new health interoperability. :https://pdfs.semanticscholar.org/8b24/dc9cffeca8cc276d3102f8ae17467c7343b0.pdf, 2016. Accessed : 2021-04-06.

[37] Asokan V Asokan GV. Leveraging "big data" to enhance the effectiveness of "one health" in an era of health informatics. 4 :311–314, 2015.

[38] Engelhardt M. An introduction to blockchain technology in the healthcare. :https://timreview.ca/article/1111, 2017. Accessed : 2021-04-07.

[39] et autres Liam Bell, William J Buchanan. Applications of blockchain within healthcare. 2573-8240 :1–7.

[40] Anca Petre et Nassima Haï. Opportunités et enjeux de la technologie blockchain dans le secteur de la santé.

[41] Natalie Marleret autre Wendy Charles. Blockchain compliance by design : Regulatory considerations for blockchain in clinical research. *United States*, 2019-11-08.

[42] Ken Miyachi et autres Tim Ken Mackey. Combating health care fraud and abuse : Conceptualization and prototyping study of a blockchain antifraud framework. *Medical internet research*, 22, 2020-09-10.

[43] Santé, industrie pharmaceutique et blockchain. `https://blockchainpartner.fr`.

[44] Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid. Using blockchain for electronic health records. *IEEE Access*, 7 :147782–147795, 2019.

[45] et autres Ibrar Yaqoob, Khaled Salah. Blockchain for healthcare data management : Opportunities, challenges, and future recommendations. 7, 2019-11-06.

[46] Vincent Renotte. La blockchain s'empare de votre dossier médical. `https://medium.com/@vincent.renotte/la-blockchain-sempare-de-votre-dossier-medical-e8ed834fd338`, 2018-09-29.

[47] Dimiter V. Dimitrov. Blockchain applications for healthcare data management. pages 1–6, 2019-01.

[48] Thiago Vieira Asaph Azaria, Ariel Ekblaw and Andrew Lippman. Medrec : Using blockchain for medical data access and permission management. pages 1–6, 2016.