RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
http://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Master en Informatique

Option : Systèmes D'information et Réseaux Informatiques

Présenté par :
Mario Habib D. **LEGBAGBO**

Prototype d'un système de contrat intelligent pour la sécurité des données médicales des patients

Sous la supervision :
Professeur Eugène C. **EZIN**
Enseignant - Chercheur à l'UAC

Membres du jury :

Pr Eugène C. EZIN	Professeur titulaire	IFRI-UAC	Président
Dr Maurice COMLAN	Enseignant - Chercheur	ENEAM/UAC	Examinateur
Dr Abel KONNON	Enseignant - Chercheur	INSTI/UNSTIM	Rapporteur

Année Académique : **2020-2021**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux viii

Sigles et abreviations ix

Glossaire x

Introduction 1

1 Généralités sur la techologie blockchain et la cryptographie 4

2 Matériels, Méthodes, Architecture et Modélisation 25

3 Résultats et Discussion 36

Conclusion 46

Bibliographie 47

Bibliographie 47

Webographie 48

Table des matières 49

Annexe 52

Dédicace

Je dédie ce travail à :
Mes parents pour leur soutien moral, matériel, financier et pour leur bénédiction ;
A tous mes oncles ;

Remerciements

Ce mémoire a été réalisé grâce à la participation de plusieurs personnes. Je tiens à remercier toutes celles et ceux qui ont, de près ou de loin, contribué à la réalisation de ce mémoire.
Mes remerciements s'adressent particulièrement à :

- Prof. Eugène C. EZIN, Enseignant - Chercheur à l'UAC, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI), mon maître de mémoire ;
- Dr. Gaston EDAH, Directeur Adjoint de l'IFRI, Maître de conférences des Universités CAMES ;

Je tiens également à exprimer ma profonde gratitude envers la famille CODJIA, le couple ADONONSSI, le couple GAGNON Joseph Diane, le Colonel Adjakou ADJINDA, et Monsieur Herbert HOUNGNIBO pour leur soutien et leur générosité exceptionnels.

Résumé

Le projet **"DSESanté"** ambitieux vise à révolutionner la gestion des dossiers électroniques de santé en exploitant la puissance de la technologie blockchain. Axé sur la création d'une confiance partagée sans nécessiter d'intermédiaire, le projet se donne pour objectifs la transparence, l'immuabilité et la sécurité des données médicales. La méthodologie prévoit une analyse approfondie des besoins du secteur, le développement de contrats intelligents adaptés, et l'intégration de la blockchain dans un environnement interactif. Les résultats attendus incluent le renforcement de la confiance entre les acteurs de la santé, une amélioration substantielle de la sécurité des données, la simplification des transactions, et l'instauration d'une innovation responsable. Ce projet incarne une vision moderne et efficiente de la gestion des données médicales, exploitant pleinement les avantages offerts par la blockchain.

Mots clés : dossiers électroniques santé, blockchain, sécurité des données, confiance.

Abstract

The **"DSESanté"** project aims to revolutionize the management of electronic health records by harnessing the power of blockchain technology. Focused on creating shared trust without the need for intermediaries, the project aims for transparency, immutability, and security of medical data. The methodology involves a thorough analysis of sector needs, the development of tailored smart contracts, and the integration of blockchain into an interactive environment. Expected results include strengthening trust among healthcare stakeholders, substantial improvement in data security, simplification of transactions, and the establishment of responsible innovation. This project embodies a modern and efficient vision of medical data management, fully leveraging the advantages offered by blockchain.

Keywords: electronic records, health, blockchain, data security, trust.

Table des figures

1.1 Stockage de l'information dans un réseau blockchain décentralisé 6
1.2 Stockage d'information centralisé [8] 6
1.3 Mode de stockage des données dans une blockchain [8] 6
1.4 Modification d'une donnée dans une blockchain [8] 7
1.5 Fonctionnement de la Blockchain [8] 7
1.6 L'architecture dun blockchain [7] 8
1.7 Transaction blockchain [8]. 9
1.8 Structure interne du blocs [8]. 10
1.9 Proof of Work Vs Proof of Stake. 11
1.10 Fonctions de hachage. 12
1.11 Liaisons cryptographiques valides entre les blocs 13
1.12 Liaisons cryptographiques invalides entre les blocs 13
1.13 schéma d'un réseau centralisé [5] 15
1.14 Schéma d'un réseau distribué [5] 16
1.15 Schéma d'un réseau décentralisé [5] 16
1.16 Chiffrement et déchiffrement d'un message en cryptographie symétrique 18
1.17 Code de César avec un décalage égal à 3 18
1.18 Echange de messages entre Alice et Bob interceptés par Eve 19
1.19 Chaque interlocuteur dispose de sa paire de clés interceptés par Eve 19
1.20 Echange des clés publiques entre Alice et Bob interceptés par Eve 19
1.21 Chiffrement du message par Bob que seule Alice est en mesure de lire interceptés par Eve 19
1.22 Utilisation de la cryptographie asymétrique pour vérifier l'authenticité et la provenance d'un message interceptés par Eve 19
1.23 Emission d'une transaction puis vérification de son authenticité par le réseau 20
1.24 La signature numérique 21
1.25 : construction d'un nouveau bloc par un mineur 23

2.1 Architecture Globale du système 30
2.2 Diagramme de cas d'utilisation du système 32
2.3 Diagramme de séquence du cas d'utilisation «Gérer les utilisateurs». 33
2.4 Diagramme de séquence du cas d'utilisation «Gérer dossier». 34
2.5 Diagramme de séquence du cas d'utilisation «Gérer le personnel de santé». 35

3.1 Page de connexion 37
3.2 Connexion : Etape 1 37
3.3 Connexion : Etape 2 37

3.4 Page d'enrégistrement d'un patient 38
3.5 Page de recherche d'un patient 38
3.6 Page d'enrégistrement d'un médécin 39
3.7 Page de recherche d'un médécin 39
3.8 Page d'enrégistrement d'un hôpital 40
3.9 Page de recherche d'un hôpital 40
3.10 Page de recherche détaillée des examens 41
3.11 Page d'enrégistrement ou de recherche d'un diagnostic 42
3.12 Page d'enrégistrement ou de recherche de la maladie preésente 42
3.13 Page d'enrégistrement ou de recherche d'un traitement 43
3.14 Page d'enrégistrement ou de recherche d'une maladie familiale 43
3.15 Page d'enrégistrement ou de recherche d'une assurance 44
3.16 Demande de signature pour le transfert des contrats intelligents 54
3.17 Confirmation du transfert 55
3.18 Le déploiement des contrats sur ThirdWeb 55
3.19 Construction de la chaîne de Blocs dans Ganache 56

Liste des tableaux

1.1 Tableau comparatif. 24

2.1 Synthèse des outils et langages utilisés. 26
2.2 Tableau comparatif de la solution classique par rapport à la solution blockchain. . . . 28

3.1 Tableau de la fiche d'enquête 53

Sigles et abreviations

ERC721 :

Ethereum Request for Comment 721 36, *Glossaire* ERC721

P2P :

Peer to Peer 8, *Glossaire* P2P

PoS :

Prof of Stake 10, *Glossaire* PoS

PoW :

Proof of Work 10, *Glossaire* PoW

SHA :

Secure Hash Algorithm 12, 49, *Glossaire* SHA

UML :

Unified Modeling Language 27, *Glossaire* UML

Glossaire

ERC721 :

ERC-721 est un type de jeton créé pour le réseau Ethereum selon les normes de son contrats intelligents. La proposition de création de ce nouveau standard a été présentée par le développeur diète shirley à la fin de 2017. ix

IA :

L'intelligence artificielle (IA) est un processus d'imitation de l'intelligence humaine qui repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique dynamique. Son but est de permettre à des ordinateurs de penser et d'agir comme des êtres humains. 46

P2P :

Le pair-à-pair ou système pair à pair est un modèle d'échange en réseau où chaque entité est à la fois client et serveur, contrairement au modèle client-serveur. Les termes « pair », « nœud » et « utilisateur » sont généralement utilisés pour désigner les entités composant un tel système. ix

PoS :

La **preuve d'enjeu, preuve de participation ou preuve d'intérêt (en anglais : proof of stake)** est une méthode par laquelle une chaîne de blocs d'une crypto-monnaie vise à atteindre un consensus distribué. ix

PoW :

Un système de validation par **preuve de travail (Proof of Work)** est, en informatique, un protocole permettant de repousser, sur un environnement client-serveur, des attaques par déni de service ou d'autres abus de service tels que les spams. ix

QR :

Un code QR, en forme longue quick response code, est un type de code-barres à deux dimensions constitué de modules-carrés noirs disposés dans un carré à fond blanc. Ces points définissent l'information que contient le code. 46

SHA :

L'acronyme **"SHA"** signifie **"Secure Hash Algorithm"** et **"Algorithme de hachage sécurisé"** en français. Comme son nom l'indique, c'est un algorithme qui est spécialisé dans le hachage sécurisé. Cet algorithme est utilisé sur de nombreuses blockchains et est très populaire de par sa protection et sa sécurité. ix

UML :

Le **langage UML (Unified Modeling Language, ou langage de modélisation unifié)** a été pensé pour être un langage de modélisation visuelle commun, et riche sémantiquement et syntaxiquement. ix

Introduction Générale

1 Contexte et justification

Dans le contexte actuel, la première étape de l'admission dans un centre de santé ou clinique est l'enregistrement. L'enregistrement nécessite de remplir des formulaires qui contiennent les informations basiques (nom, premon, âge, carnet de soin, numéro de téléphone, assurance, etc..

Lors du paiement des frais de consultation (frais d'achat de carnet, de consultation, d'analyses, de radio etc..), on remarque que les patients sont obligés de faire le rang devant la caisse afin de procéder aux divers paiements. Il leur sera attribué un numéro selon l'ordre d'arrivée avant la prise des constantes suivie de la recherche de leur dossier classé dans un casier. Le médecin traitant du jour a parfois des difficultés à lire les écrits de ses collègues afin de mieux comprendre les traitements passés du patient. La plupart du temps, il n'existe qu'une seule copie d'un même document papier (dossier du patient) et sa perte aurait donc des conséquences désastreuses et irréversibles. Nous nous sommes tous moqués un jour ou l'autre de l'écriture illisible des médecins parfois difficile à déchiffrer. Ceci pose problème non seulement aux patients qui cherchent à comprendre ce qui leur a été prescrit mais également à d'autres professionnels de la santé qui devront relire ces dossiers plus tard. Si un autre médecin ou un membre du personnel ne peut pas comprendre le contenu de ces dossiers, il pourrait, dans le meilleur des cas, être fortement ralenti dans ses démarches, ou se référer à quelqu'un d'autre pour la lecture. Dans le pire des cas, cette situation pourrait amener à des erreurs médicales et des soins inappropriés pourraient être alors administrés à un patient. Le nombre de patients ne cessant d'augmenter et leurs attentes s'intensifiant, les professionnels de la santé ne peuvent pas se permettre de prendre du retard dans leur service. Si un patient consulte son médecin et souhaite, plus tard, obtenir une réponse à une question spécifique ou simplement lire son dossier médical, les démarches qui s'en suivent peuvent se révéler être assez laborieuses. Généralement, un membre du personnel devra arrêter ce qu'il est en train de faire pour chercher le dossier, en faire une copie et la faire parvenir au patient. Face à cet état de chose, il est indispensable de penser à une solution qui va permettre dans un premier temps de réduire le temps perdu mentionné précédemment, voire l'éliminer tout en rendant la solution très accessible aux utilisateurs. Dans un second temps, il est important de réduire considérablement, voire éliminer les coûts liés à l'intermédiation. C'est dans ce cadre que s'inscrit ce sujet de mémoire visant à mettre en place un système de numérisation des données médicales qui va désormais servir pour le paiement de tous les frais liés aux patients sur le plan national et ou pourquoi pas sur le plan international. Il permettra aussi aux professionnels (médecins) d'accéder à l'ensemble des données de santé afin de mieux comprendre, prévenir et

traiter les maladies et de personnaliser de plus en plus les traitements. De leur côté, les patients se sentiront plus autonomes puisque l'accès à ces données leur permet de prendre des décisions plus éclairées. Elle permettra au centre, notamment, de réduire leur temps de production, de renforcer la communication et la collaboration au sein de leurs équipes, de faciliter l'accessibilité aux documents, de libérer de l'espace dans les bureaux et en dernier point de faire des économies.

2 Problématique

Nous avons identifié plusieurs lacunes dans le domaine de la santé, notamment la lenteur dans la prise de décision concernant le choix des traitements, surtout pour les patients confrontés à des situations médicales critiques nécessitant une intervention rapide. Cette efficacité temporelle est cruciale pour sauver des vies. Pour remédier à ces défis, ce mémoire propose la mise en place d'une planification complète du traitement des patients, de l'admission à la sortie, incluant la facturation pour le centre de santé **POLYCLINIQUE BIOSSO**. Il envisage également l'introduction d'une cryptomonnaie dédiée au paiement des frais et l'utilisation d'une blockchain pour sécuriser et référencer les données, tout en respectant les normes RGPD (Règlement Général sur la Protection des Données). Ces initiatives visent à faciliter des analyses efficaces, assurer une interopérabilité dans la lecture des données, et permettre une compréhension des informations, indépendamment de leur format initial.

3 Objectifs

L'objectif du mémoire est de concevoir et de déployer un système de numérisation et de partage des données médicales des patients qui tournent vers la blockchain **Ethereum**, une technologie de stockage et de transmission d'informations infalsifiables, pour répondre à toutes les situations possibles. Une **cryptononaie** qui pourra être utilisée pour n'importe quel paiement de frais lié aux patients. Accéder à l'ensemble des données de santé pour permettre aux professionnels de disposer de fiables données contextualisés pour mieux comprendre les traitements. La confiance est un élément vital de la satisfaction des patients. Il s'agira de :

- proposer une architecture pour le système à mettre en place ;
- procéder au choix des technologies à utiliser ;
- modéliser le prototype à mettre en place ;
- concevoir le Carnet Médical Numérique (contrat intelligent) ;
- avoir une accessibilité disponible et rapide depuis n'importe où dans l'hôpital sur les données numériques des patients ;
- une traçabilité des traitements ;
- développer et tester l'application proposée ;

4 Organisation du mémoire

Le présent mémoire comporte trois chapitres. Le premier chapitre porte sur l'état de l'art. Le second chapitre aborde les matériels et méthodes. Le troisième chapitre est consacré à l'architecture et modélisation. Le quatrième chapitre présente l'implémentation, résultats et discussions.

Chapitre 1

Généralités sur la techologie blockchain et la cryptographie

Introduction

La blockchain est parfois décrite comme la plus grande invention depuis internet ou comme une réelle révolution qui va changer notre mode de vie. Elle est une technologie qui ne cesse de grandir. Initialement, conçue pour permettre les transactions de bitcoin. Elle est aujourd'hui proposée en vue d'améliorer divers secteurs : la gouvernance, la monnaie, l'énergie, la musique,la santé, l'assurance, ... En d'autres mots, la blockchain semble pouvoir atteindre tous les domaines d'activités. Elle reste cependant un concept neuf et mal compris [6]. Quant au sens de la cryptographie dans la blockchain, elle est une discipline mathématique se trouvant au centre du processus de validation et de vérification des informations échangées au sein d'un réseau, c'est cela qui permet d'assurer la confiance [7].

Dans ce chapitre qui sera consacré à l'état de l'art, nous allons aborder les différentes technologies, qui mises ensemble, permettent à une blockchain de fonctionner. Ceci nous permettra de comprendre comment une fois ces technologies agrégées, le système arrive à un niveau de sécurité très élevé, ce qui nous permettra de l'utiliser notamment dans le domaine de la santé. Tout d'abord, nous allons décrire le plus simplement possible la technologie blockchain afin d'en cerner les grands principes, ses intérêts et ses faiblesses.

1 Notions sur la Blockchain

1.1 Définition

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 permettent 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)[7].

Les blockchains sont regroupées en deux catégories. D'une part nous avons les blockchains privées, dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs et d'autre part les blockchains publiques qui sont quant à elles accessibles à tous.

1.2 Historique de la blockchain

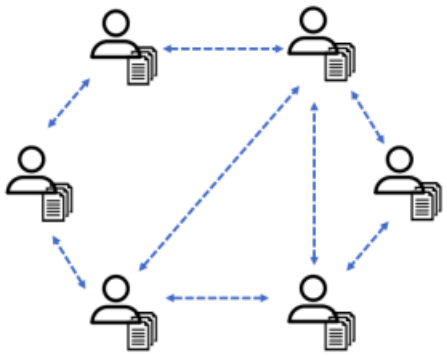
L'histoire de la blockchain est pour le moins étonnante. Comment le Bitcoin, la première monnaie virtuelle **pair à pair**, une invention informatique open source à l'esprit libertarien revendiqué visant à court-circuiter les banques, a-t-il pu donner naissance à l'incroyable phénomène blockchain qui agite tous les milieux d'affaires du monde ? L'aventure commence le 1er novembre 2008. Sous le pseudonyme de Satoshi Nakamoto, une personne, qui n'a toujours pas été identifiée aujourd'hui, publie un message dans une liste de diffusion de spécialistes de la cryptographie (« The Cryptography Mailing List »), avec pour objet « Bitcoin P2P e-cash paper ». Dans des termes très factuels, elle y résume son projet : « J'ai travaillé sur un nouveau système de cash électronique **pair à pair**, sans tiers de confiance. » Satoshi énumère ses principales caractéristiques. D'abord, « la double dépense est rendue impossible au sein d'un réseau **pair à pair**. Pas d'émetteur de monnaie ni d'autre tiers de confiance ». C'est un exploit inédit. Jusqu'alors, les experts considéraient qu'il était impossible de créer un système de paiement **pair à pair** (d'ordinateur à ordinateur) sans tiers de confiance (sans banque par exemple), en raison du problème appelé **« double dépense »**. Sur Internet, l'information est copiée quand elle est transférée (ainsi conservons-nous une version de nos e-mails envoyés par exemple). Avec de l'argent, il ne peut pas en être de même : un montant envoyé par un réseau électronique ne peut pas être gardé, il ne doit pouvoir être dépensé qu'une seule fois [7].

1.3 Caractéristiques principales de la blockchain

Les données stockées dans la blockchain sont immuables et ne peuvent pas être modifiées facilement. Elle est décentralisée ; elle fournit un réseau **peer to peer.** Cette caractéristique de la blockchain permet aux transactions de n'impliquer que deux parties, l'expéditeur et le destinataire. Ainsi, il supprime l'exigence d'« autorisation de tiers », car tout le monde dans le réseau est lui-même en mesure d'autoriser les transactions [8].

1.4 Fonctionnement de la blockchain

Une **blockchain** est une base de données informatiques capable de stocker tous types d'informations (liste de courses, photos, données bancaires, données patients, dossiers de lot, ...). Une des **caractéristiques fondamentales** est que cette base de données est répliquée chez les utilisateurs de cette blockchain. Ainsi, tous les utilisateurs possèdent une copie de la base de données, et sont reliés les uns aux autres directement ou indirectement par un réseau. Ce mode d'organisation représenté sur la 1.1 est dit décentralisé. Il est important de noter que le fait de posséder une copie de la base de données ne permet pas forcément à ce dernier de pouvoir l'exploiter pleinement[8].



Une copie de l'information est gardée par chaque membre du réseau, c'est cette caractéristique qui fait des réseaux blockchains des réseaux décentralisés.

FIGURE 1.1 : Stockage de l'information dans un réseau blockchain décentralisé

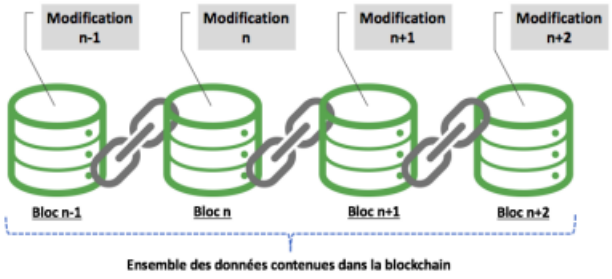
En effet, celle-ci peut être cryptée, par exemple. Cette répartition physique des données s'oppose radicalement au modèle dominant actuel 1.2 qui consiste à stocker les données de manière centralisée avec des utilisateurs qui peuvent y accéder pour lire ou modifier ces données.



Traditionnellement, les réseaux informatiques sont centralisés, avec des utilisateurs se connectant à un serveur central qui donne accès aux informations.

FIGURE 1.2 : Stockage d'information centralisé [8]

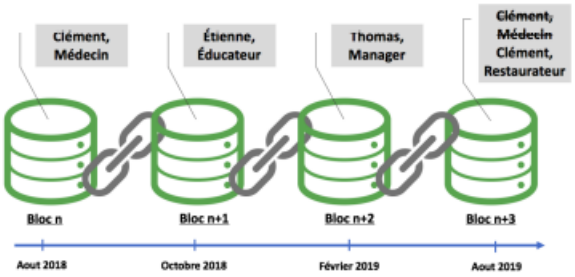
Une autre caractéristique est que chaque modification de la base de données est immuable. Pour cela, chacune des modifications sont liées les unes aux autres. C'est de cette propriété que cette technologie tire son nom : **blockchain ou chaîne de blocs** 1.3 [8].



Le stockage des données se fait sous forme d'une chaîne de blocs. Les informations sont regroupées par paquets qui sont ajoutés à la chaîne, chaque paquet de données est lié au précédent de sorte à ce qu'une modification d'une donnée altère la totalité de la chaîne de données. Ces chaînes de blocs sont par conséquent immuables.

FIGURE 1.3 : Mode de stockage des données dans une blockchain [8]

L'impossibilité de modifier un bloc passé ne signifie pas qu'une donnée ne peut jamais être modifiée 1.10.



L'immuabilité des données n'est pas synonyme d'impossibilité de faire des modifications. Conséquemment, une modification ne se fait pas en remplaçant une inscription passée mais en rajoutant une nouvelle information décrivant ce changement.

FIGURE 1.4 : Modification d'une donnée dans une blockchain [8]

Une blockchain sert à organiser des transactions sous formes de blocs qui sont vérifiées par un grand nombre de participants,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 [8]. Voici un schéma récapitulatif expliquant le fonctionnement d'une blockchain publique lors d'une transaction.

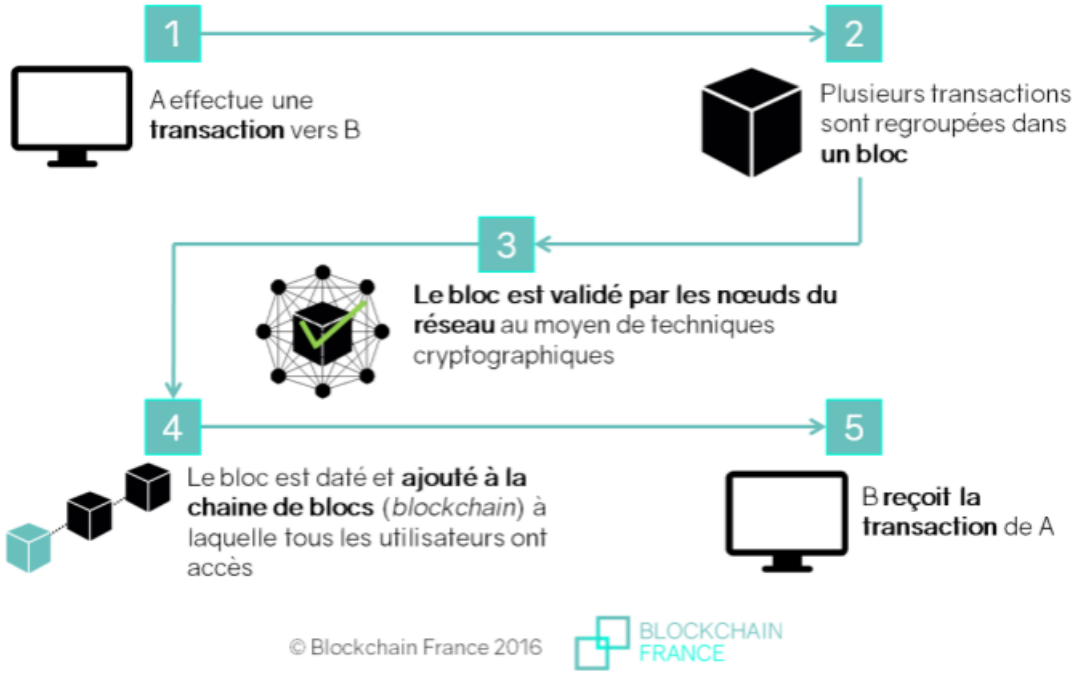


FIGURE 1.5 : Fonctionnement de la Blockchain [8]

1.5 Structure d'une blochaine

La Blockchain a une architecture réseau distribué est 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 [7].

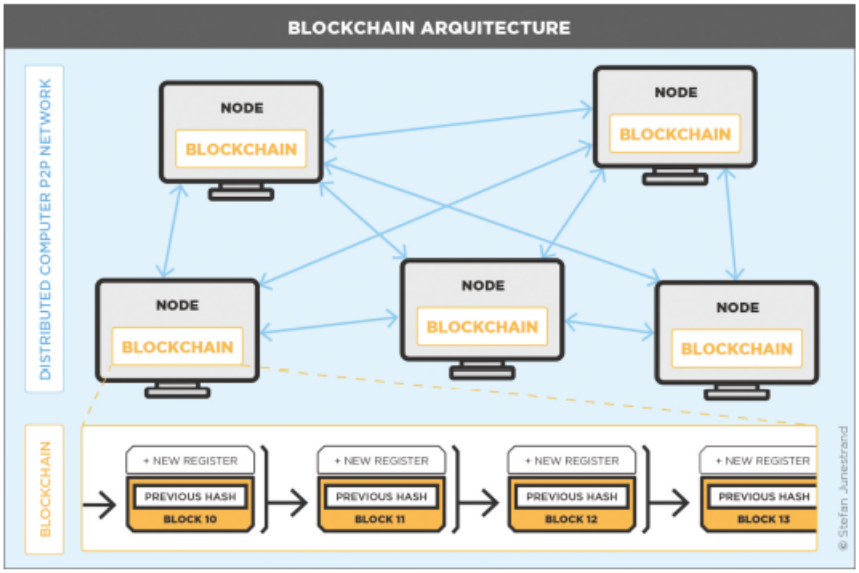


FIGURE 1.6 : L'architecture dun blockchain [7]

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 :

1.6 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 [8]. Les transactions consistent généralement en une adresse de destinataire, une adresse d'expéditeur et une valeur. Input :

- **Txx :** transactions (on peut avoir plusieurs transactions dans un (01) seul bloc).
- **Intput**
- **Pb :** la clé publique
- **Sig :** signature du l'émetteur

- **Output :**
- **Data :** les informations envoyées.
- **Hash(P) :** le haché de clé publique du destinataire

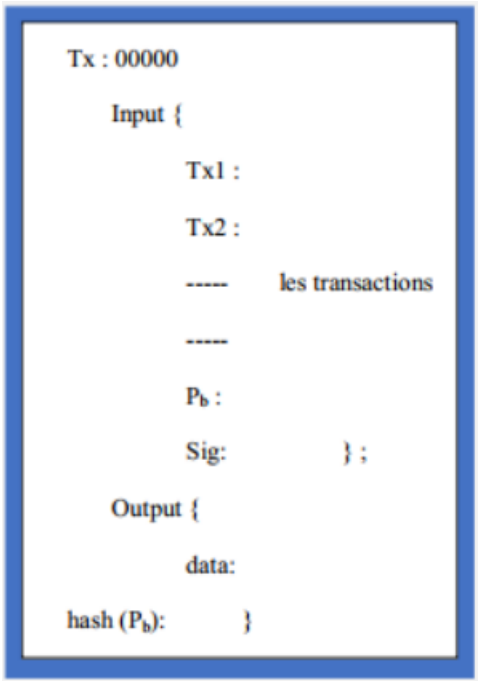


FIGURE 1.7 : Transaction blockchain [8].

1.7 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'entête et le corps de bloc.

Entête de bloc

L'entête 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 [8].

Le corps de bloc **Le corps de bloc** est composé d'une Liste des transactions et un compteur des transactions.

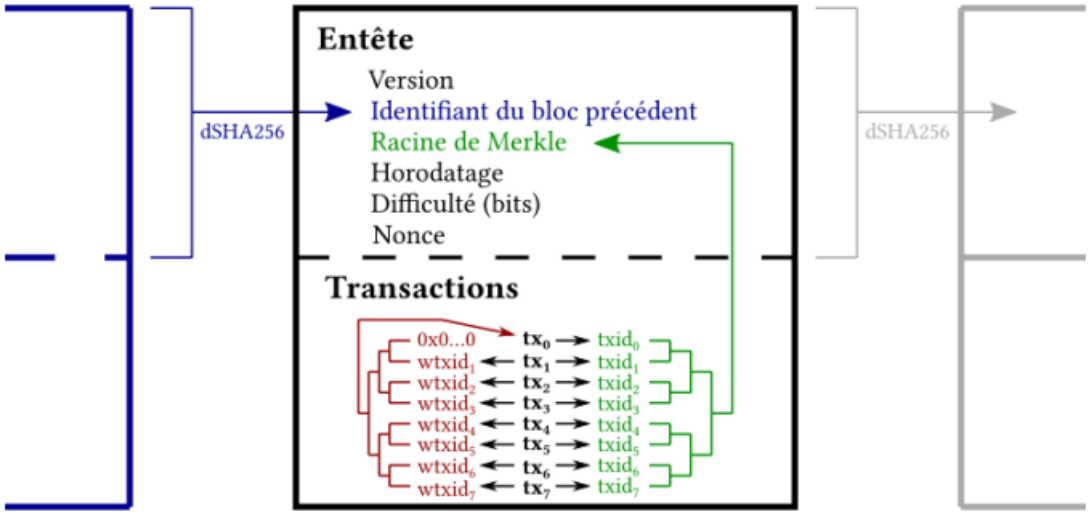


FIGURE 1.8 : Structure interne du blocs [8].

1.7.1 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, est la technique par laquelle le réseau d'une Blockchain assurée le consensus sur le contenu de la blockchain, la manière de la création et la validation des nouveaux blocs. Ainsi la recherche et le développement des nouveaux Protocoles de consensus sont des sources de l'innovation dans l'industrie des Blockchains.

- **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 [7].

- **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 [9].

- **Comparaison entre PoW et PoS**



FIGURE 1.9 : Proof of Work Vs Proof of Stake.

1.8 Fontions de hachage cryptographiques

1.8.1 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 caractères de n'importe quelle longueur et donner une sortie d'une longueur fixe (le hash) [8].

1.8.2 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.

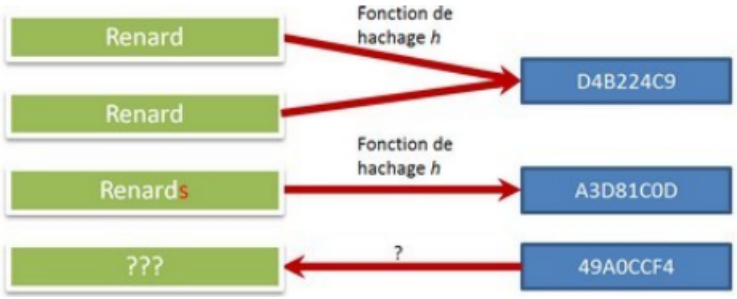


FIGURE 1.10 : Fonctions de hachage.

1.8.3 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. 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 [3].

1.9 Mineurs et les nœuds

1.9.1 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. Les mineurs doivent déterminer pour **«trouver»** un bloc et cela se fait comme suit [8] :

- Un nombre aléatoire est deviné **«Nonce»**.
- Le Nonce est ajouté à la fin de toutes les données du bloc.
- Tout cela est haché selon la méthode **SHA-256**.
- 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 [3].

1.9.2 Les nœuds

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 en valeur porcentage) des nœuds simultanément. Le nombre de nœuds étant très important, en cas de tentative de fraude, cela serait détecté très rapidement [6].

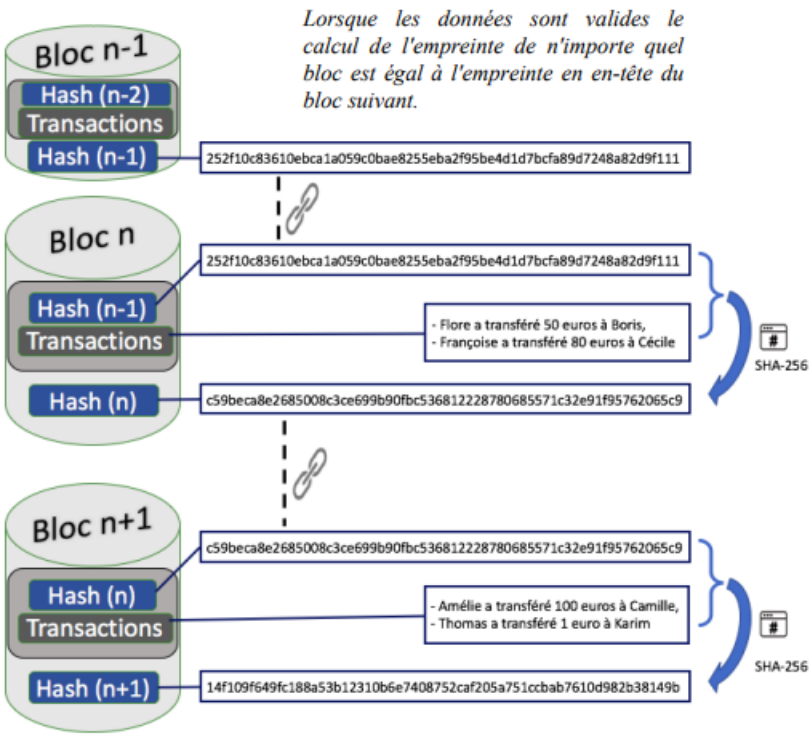


FIGURE 1.11 : Liaisons cryptographiques valides entre les blocs

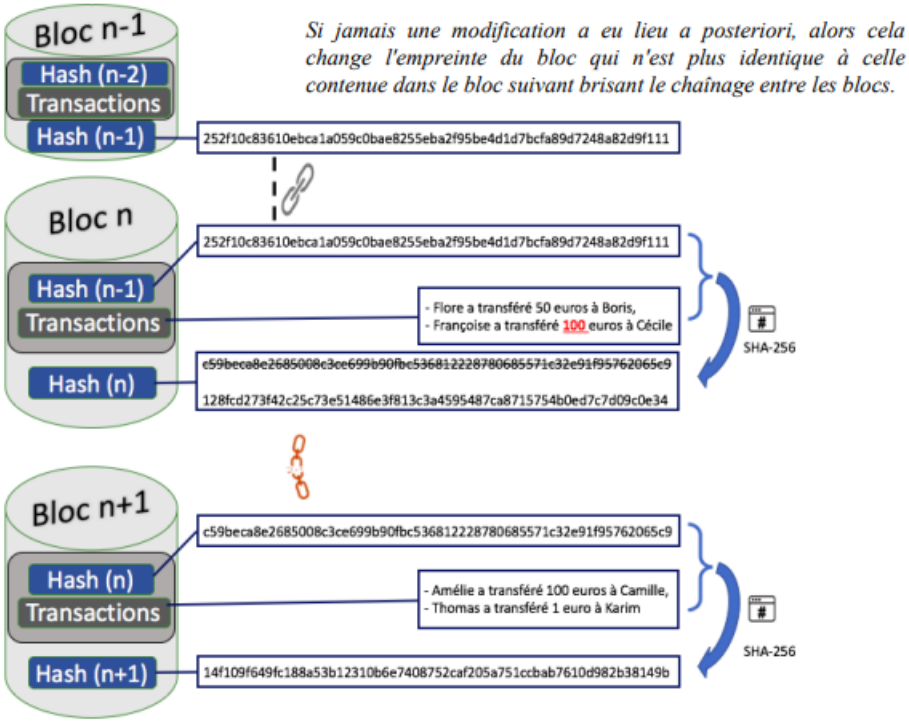


FIGURE 1.12 : Liaisons cryptographiques invalides entre les blocs

Cependant, comme nous allons voir ci-après, un bloc ne se constitue pas simplement des transactions et de l'empreinte, il comporte également une **preuve de travail** qui permet d'empêcher qu'un piratage massif ou simplement un nombre d'utilisateurs malicieux majoritaire prennent le contrôle du réseau.

1.10 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 [9].

1.10.1 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[2].

1.10.2 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.

1.10.3 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 [2]. 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 smartscontracts dans une blockchain réside dans la garantie que les termes du contrat ne pourront pas être modifiés. Un smartcontract qui ne serait pas dans la blockchain serait un programme dont les termes pourraient être changés en cours d'exécution [5].

1.10.4 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 :** 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 [5].

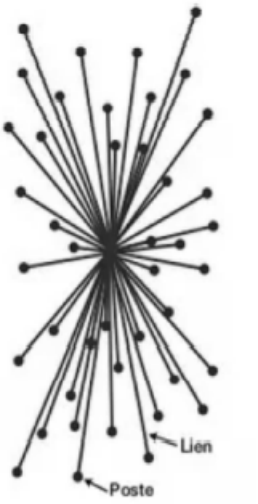
1.10.5 Inconvénients de contrats intelligents

- 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 [9].

1.10.6 la blockchaine en tant que transaction signées

Types de réseaux et réseau pair à pair décentralisé

Avant d'aborder les differénts types de réseau, il convient de définir les différentes manières possibles d'organiser un réseau. Nous allons donc voir à quoi s'appliquent les terminologies **"centralisé, décentralisé, distribué"** que l'on rencontre souvent. [5] Dans un réseau centralisé,1.13

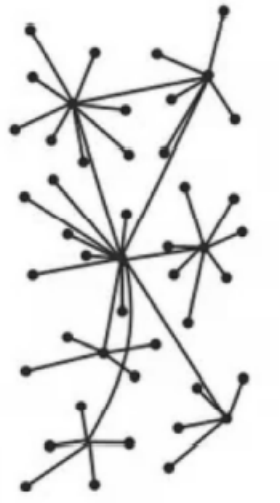


Dans un réseau centralisé une entité dispose des données et prend seule les décisions de modification.

FIGURE 1.13 : schéma d'un réseau centralisé [5]

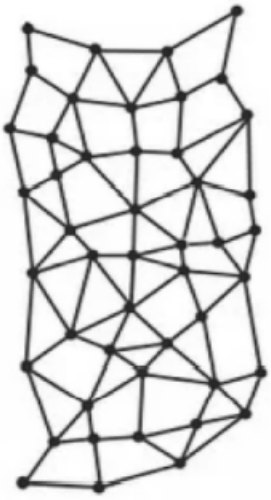
nous pouvons voir que les différents postes (utilisateurs) sont reliés à un serveur unique. Du point de vue technique, c'est le réseau le plus simple à construire. Cependant, il présente de nombreux

défauts, dont notamment le fait d'être un point de défaillance unique (notion souvent retrouvée dans la littérature sous son appellation anglaise : (Single Point of Failure). Le système distribué signifie que le traitement est partagé entre plusieurs nœuds, mais que les décisions peuvent toujours être centralisées tout en utilisant des données provenant de tous les nœuds du système. Ce genre de système peut permettre de répartir des opérations informatiques trop lourdes à supporter pour un seul nœud du réseau. Cependant, après un traitement partiel mais complémentaire de chacun des nœuds, une autorité centrale prend une décision.



Dans un réseau distribué, les données sont partagées, mais un organisme central prend les décisions.

FIGURE 1.14 : Schéma d'un réseau distribué [5]



Dans un réseau décentralisé la prise de décision est une résultante du comportement de chacun des nœuds du réseau.

FIGURE 1.15 : Schéma d'un réseau décentralisé [5]

Le système décentralisé signifie qu'il n'y a pas de point unique où la décision est prise. Chaque nœud prend une décision ayant son propre comportement, et le comportement du système qui en résulte est une réponse globale de la somme du comportement des nœuds dans le système.[5]

2 Généralités sur la cryptographie

2.1 Définition

La cryptographie est une science permettant de convertir des informations "en clair" en informations codées, c'est à dire non compréhensibles, puis, à partir de ces informations codées, de restituer les informations originales [2].

2.2 Caractéristiques de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur **intégrité** et **leur authenticité**. Nous avons des cryptographies symétrique et asymetrique.

- **La confidentialité :** consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.
- **L'intégrité :** vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.
- **L'authentification :** consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- **La non répudiation :** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction [2].

2.3 Chiffrement symétrique

2.3.1 Définition

Le chiffrement symétrique, que l'on nomme couramment chiffrement conventionnel, basé sur des fonctions mathématiques réversibles. Le chiffrement symétrique repose sur un principe de clé unique pour chiffrer et déchiffrer.
Cette clé possède plusieurs appellations :

- Clé secrète ;
- Clé privée.

On parle de chiffrement conventionnel puisque c'est le premier chiffrement par clé à avoir été découvert et utilisé [**?**].

2.3.2 Principe de fonctionnement

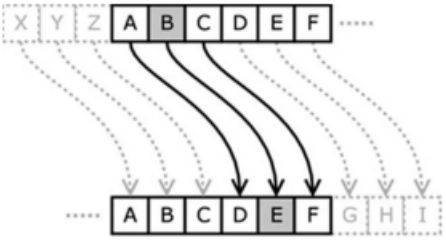
- **cryptographie symétrique** ;

La **cryptographie symétrique** suppose la création d'une clé de chiffrement et déchiffrement unique que l'émetteur et le destinataire du message doivent se partager dans un secret absolu. La sécurité de la cryptographie symétrique dépend fortement de l'échange de cette clé entre les deux communicants. Il existe des méthodes de cryptage symétrique plus avancées dites **polyalphabétique** où le chiffrement d'une lettre sera différent en fonction de sa position dans le message.[8]

La cryptographie symétrique permet de chiffrer un message avec une clé. Une fois chiffré c'est cette même clé qui va permettre de déchiffrer le message.



FIGURE 1.16 : Chiffrement et déchiffrement d'un message en cryptographie symétrique



Le code de César est un bon exemple de chiffrement symétrique. La clé de chiffrage est la même pour chiffrer et déchiffrer le message, à savoir décaler les lettres de l'alphabet dans un sens puis dans l'autre.

FIGURE 1.17 : Code de César avec un décalage égal à 3

- **cryptographie asymétrique** ;

Nous pouvons voir sur la figure 1.18 et 1.19 un avantage majeur de la cryptographie asymétrique. L'échange des clés peut se faire en présence d'un espion sans que cela n'affecte la sécurité des messages échangés par la suite.

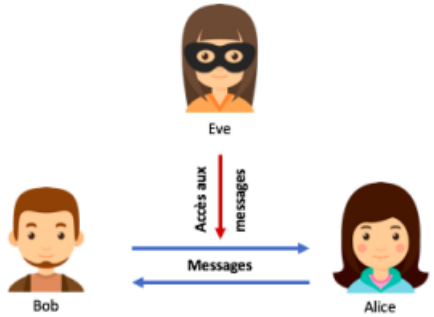


FIGURE 1.18 : Echange de messages entre Alice et Bob interceptés par Eve

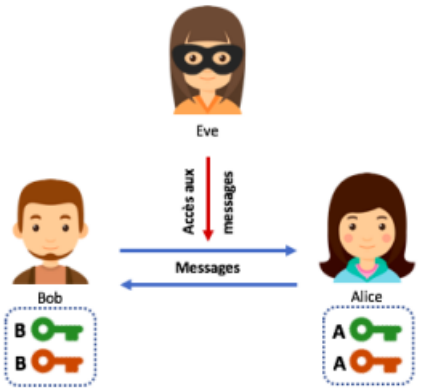


FIGURE 1.19 : Chaque interlocuteur dispose de sa paire de clés interceptés par Eve

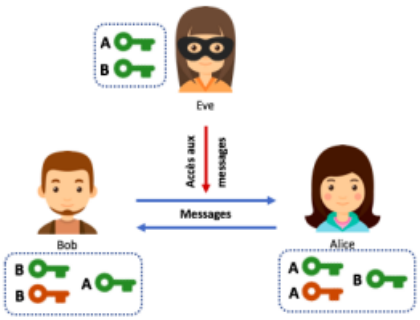


FIGURE 1.20 : Echange des clés publiques entre Alice et Bob interceptés par Eve

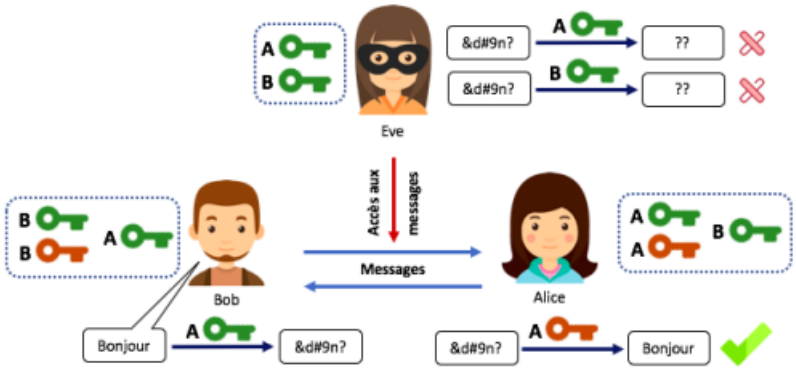


FIGURE 1.21 : Chiffrement du message par Bob que seule Alice est en mesure de lire interceptés par Eve

- Comment ces fonctions à sens unique et porte dérobée servent le cryptage de messages ?

La clé utilisée pour chiffrer le message est appelée **clé publique** alors que la seconde qui permet d'exploiter cette porte dérobée est appelée **clé privée**.

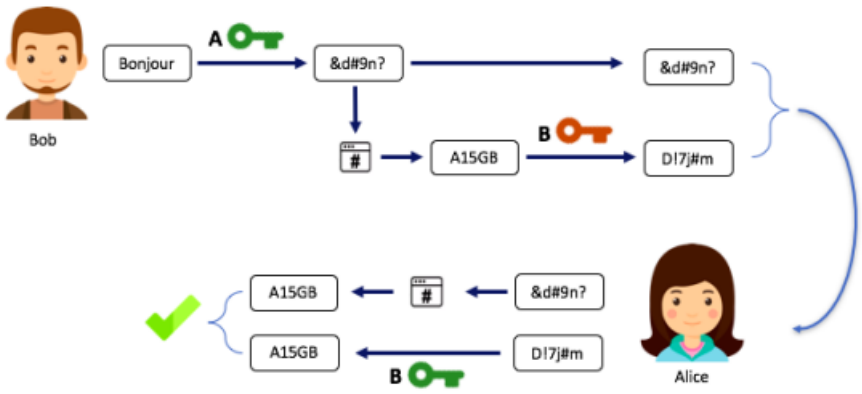


FIGURE 1.22 : Utilisation de la cryptographie asymétrique pour vérifier l'authenticité et la provenance d'un message interceptés par Eve

Une autre application différente du chiffrement consiste à utiliser la cryptographie asymétrique afin de signer électroniquement un message. Cette technologie permet également de vérifier que le

message n'a pas été altéré entre son émission et sa réceptionainsi que de vérifier l'authenticité de la provenance d'un message. Alice va calculer l'empreinte de hachage du message crypté. Elle va également utiliser la **clé publique** de Bob sur le second message que Bob a crypté ave sa **clé privée**. Si les deux résultats sont égaux, alors cela signifie deux choses :

- Le message a été envoyé par une personne possédant la clé privée de Bob (donc Bob qui est normalement le seul à la posséder) ;
- Le message n'a pas été altéré entre son émission et sa réception (rappelons-nous que la moindre modification d'un fichier entraîne une modification totale de son empreinte) ;

2.4 Interêt de la cryptographie asymétrique dans un réseau blockchain

2.4.1 Gestion des identités sur le réseau

Nous allons illustrer la propriété consistant à pouvoir identifier l'auteur et l'intégrité d'un message. Dans la blockchain Bitcoin, la cryptographie asymétrique permet de gérer les identités sur le réseau. En effet, chaque compte dispose d'une clé publique et d'une clé privée. Nous pouvons assimiler la clé publique à l'adresse bitcoin d'une personne. Une adresse Bitcoin est l'équivalent d'un numéro de compte. Comme pour les comptes bancaires, il est possible de disposer de plusieurs adresses Bitcoin. Toutes les adresses bitcoin sont en clair sur le réseau mais ne permettent pas d'identifier la personne physique qui la possède.[8]

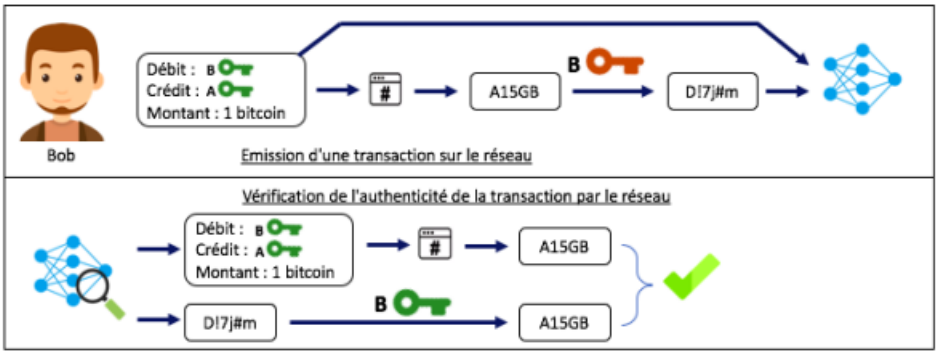


FIGURE 1.23 : Emission d'une transaction puis vérification de son authenticité par le réseau

Si Bob désire envoyer un certain montant à Alice, alors il doit émettre (accompagnée de l'empreinte de la transaction cryptée par la clé privée de l'émetteur) sur le réseau de la blockchain un message comportant :

- l'adresse à laquelle débiter les fonds ;
- l'adresse à laquelle créditer les fonds ;
- le montant de la transaction ;

Ainsi, le principal problème, contre lequel il faut se prémunir, est l'usurpation d'identité. Pour vérifier que la transaction émane bien de Bob, le réseau va simplement d'un côté, hacher le message, puis de l'autre, décrypter le hachage envoyé par Bob à l'aide de la clé publique de ce dernier. Si les deux empreintes sont égales, alors nous pouvons être certains de deux choses :

- c'est bien Bob qui a émis cet ordre ;
- les données de l'ordre sont conformes à ce que souhaite Bob (notamment le montant et le destinataire) ;

2.4.2 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 entretemps. 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 [4].

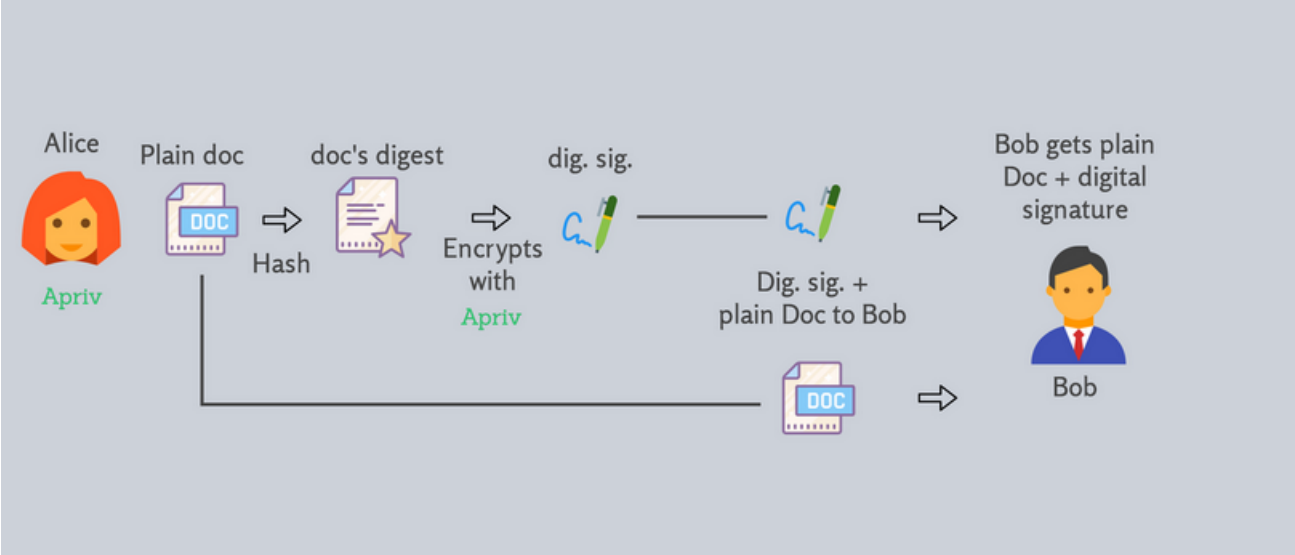


FIGURE 1.24 : La signature numérique

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

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 [5].

2.5 Types de blockchains

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

2.5.1 Blockchains publiques

En principe la Blockchain est publique, c'est-à-dire accessible par n'importe qu'elle personne, chaque personne peut devenir utilisateur, créer 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 [3].

2.5.2 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 qui accorde des droits et des restrictions spécifiques aux participants du réseau. Cela signifie essentiellement que les blockchain privées sont plus centralisées [6].

2.5.3 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 [6].

2.6 les types de fautes dans un réseau

Dans un réseau, il est essentiel de distinguer les différents types de fautes qu'un nœud peut commettre.[3]

- **Faute de performance :** un nœud du réseau peut rendre un résultat au mauvais moment, trop tôt ou trop tard. Cette erreur est facilement détectable par les autres nœuds du réseau ;
- **Faute d'omission :** un nœud ne rend pas de décision, et l'erreur est détectée par les autres nœuds. ;
- **Faute de panne :** une panne du système informatique de la part d'un nœud l'empêche de rendre une décision.
- **Faute byzantine :** un nœud va non seulement communiquer une information potentiellement fausse, mais aussi une information potentiellement différente à chacun des autres nœuds avec lequel il communique. Le nœud va aussi potentiellement falsifier les informations d'un autre nœud. Par exemple, un nœud victime d'une faute byzantine va diffuser une information émanant d'un autre nœud mais en la modifiant. Ce type de faute est très compliqué à gérer dans la mesure où dans les systèmes complexes elles sont très difficiles à repérer.réseau blockchain à une faute byzantine dans un réseau informatique classique. Un utilisateur peut, en effet, envoyer des données erronées ou essayer de falsifier des informations émanant d'autres nœuds. Ainsi, pour créer une blockchain robuste et sécurisée, il est nécessaire que cette dernière soit résistante aux fautes byzantines ;

2.6.1 Preuve de travail

C'est grâce à la preuve de travail que la blockchain Bitcoin est résistante aux fautes byzantines. Cela permet, d'une part, de ne pas submerger le réseau de propositions de nouveaux blocs. Aussi, les mineurs étant rémunérés en bitcoin, ils ont donc tout intérêt à ce que la blockchain se porte bien, faute

de quoi le bitcoin perd de sa valeur. D'autre part, comme il faut investir de grosses sommes d'argent pour pouvoir proposer des blocs, cela dissuade fortement les mineurs à y inclure des transactions non valides qui correspondraient à du gaspillage.

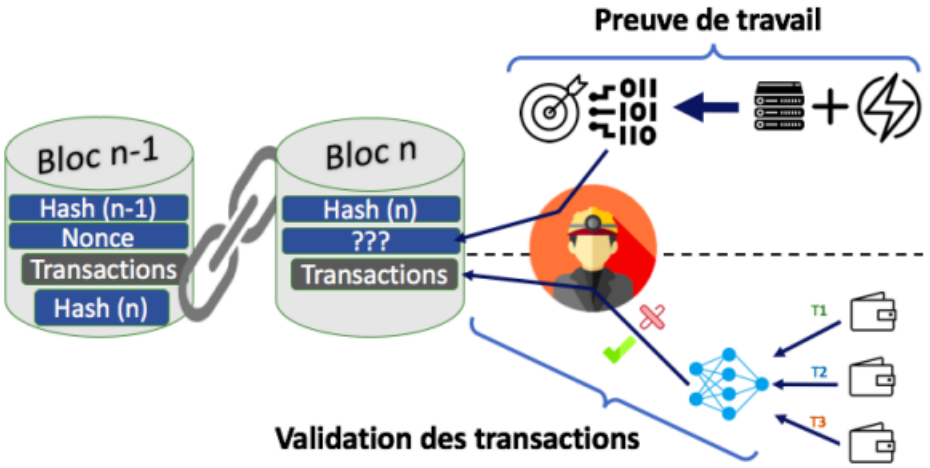


FIGURE 1.25 : : construction d'un nouveau bloc par un mineur

Parallèlement à la collecte des transactions et leur vérification, les mineurs doivent chercher une empreinte de hachage satisfaisant un certain niveau de difficulté, c'est la preuve de travail. Cette recherche est une course entre tous les mineurs. C'est uniquement lorsque cette empreinte est trouvée qu'un mineur peut proposer son bloc au réseau. Le mineur qui remporte la course empoche une récompense en bitcoins et c'est sa version de la blockchain qui devient la nouvelle réalité partagée par tous les mineurs pour redémarrer la course pour le prochain bloc.

2.7 Blockchain aujourdhui

2.7.1 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 bit coin, comme beaucoup d'autres cryptomonnaies, est mis en circulation via 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 cryptomonnaies sur des plateformes d'échange [1].

2.7.2 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 [1].

2.7.3 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 cryptomonnaie, 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 [6].

2.7.4 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 plugandplay destinés à être utilisés au sein d'entreprises privées [1].

TABLE 1.1 : Tableau comparatif.

Caractéristiques	**Bitcoin**	**Ethereum**	**Hyperledger**
Cryptocurrency	Bitcoin	Ether	Non
Smart Contract	Non	Oui (Smart contracts)	Oui (Chain code)
Type de Blockchain	Publique	Publique	Privée
Méthode de consensus	Proof of Work	Proof of Work	Méthodes variées

Conclusion

Dans ce présent chapitre, nous avons abordé la blockchain qui est donc dans sa forme originelle une base de données, décentralisée dans un réseau pair à pair. Etant décentralisée, il est particulièrement compliqué de la pirater. Chaque bloc de données est lié cryptographiquement au précédent, ce qui en fait un recueil de données immuables. Si le partage de la base de données entre des entités ayant des intérêts divergents peut paraître une faiblesse, ce défi est surmonté grâce à la méthode de consensus qui permet de créer de la confiance entre ces entités. La blockchain apparaît alors comme une nouvelle technologie pouvant créer de la confiance entre des entités ou des organisations qui peuvent être amenées à échanger de la valeur et/ou des informations entre elles. Il existe plusieurs cryptomonnaies sur le marché dont Bitcoin, Ether Ripple et plusieurs d'autres encore. Dans le chapitre suivant, nous aborderons les matériels de travail ainsi que les méthodes utilisées pour mettre en place le prototype proposé.

Chapitre 2

Matériels, Méthodes, Architecture et Modélisation

Introduction

Dans ce chapitre, nous abordons la méthodologie, les choix techniques, les matériels, l'architecture, et la modélisation. Nous commencerons par effectuer des choix, tels que le type de blockchain et l'architecture du système que nous souhaitons mettre en place. En outre, nous examinerons les matériels et les technologies à utiliser dans la mise en œuvre du prototype, en mettant l'accent sur l'application de la blockchain dans les soins de santé. La blockchain, souvent décrite comme un outil instaurant la confiance entre des acteurs, a évolué avec les avancées technologiques et l'intérêt croissant des entreprises internationales. Cette technologie se révèle être un allié important dans le domaine des soins de santé grâce à ses fonctionnalités, notamment son immutabilité qui en fait un excellent support pour authentifier des données sensibles telles que des consentements d'essais cliniques, et la possibilité d'éditer des smart contracts automatisant de nombreux processus. Ensuite, nous nous pencherons sur l'architecture et la modélisation du système. Détaillons d'abord l'architecture du système que nous avons l'intention de mettre en place. La phase de modélisation débutera par une analyse du contexte, nous permettant d'identifier les diverses fonctionnalités que nous mettrons en lumière à travers différents types de diagrammes.

1 Matériels et outils

La finalité de ce travail est de mettre en place une plateforme basée sur la blockchain pour stocker les données de santé. Pour permettre aux différents utilisateurs (les acteurs de santé) d'interagir avec la plateforme, l'architecture tiendra également compte des clients (applications web). L'ordinateur sur lequel nous avons implémenté la solution, possède des caractéristiques suivantes :

- système d'exploitation Ubuntu 22.04.3 LTS : ;
- type du système d'exploitation : 64-bit ;
- mémoire RAM : 8.0 GIB ;

- processeur : Intel Core i7 ;

1.1 Outils et Langages de programmation

Les principaux outils et langages que nous avons utilisés pour la réalisation de notre système sont répertoriés dans le tableau 2.1 :

TABLE 2.1 : Synthèse des outils et langages utilisés.

Outils et langages	Définition des outils et langages
Plateforme décentralisée basée sur la technologie de la blockchain	Crypto-monnaie native d'**Ethereum** qui s'appelle Ether **(ETH)**
Interfaces de développement	• **Visual Studio Code 1.46.1 :** Pour écrire les codes pour la réalisation de notre solution. • **Ganache v7.5.0 :** Ganache est un environnement de développement personnel pour Ethereum, utilisé par les développeurs pour créer, tester et déboguer des contrats intelligents localement. Ganache permet aux développeurs de travailler efficacement sur leurs projets Ethereum en fournissant un environnement de test pratique et réaliste. https://trufflesuite.com/ganache/ • **Remix IDE :** Est une application Web qui peut être utilisée pour écrire, déboguer et déployer des contrats intelligents Ethereum. Pour écrire du code dans **Solidity**, puis de le déployer sur une blockchain. https://remix.ethereum.org
Framework	• **Thirweb :** C'est un cadre de développement qui nous permet d'intégrer des fonctionnalités web3 dans notre application grâce à son interface de ligne de commande (CLI) et de déployer nos contrats sur le réseau de test. https://thirdweb.com • **Quasar :** Pour la réalisation de notre API. Quasar est un framework de développement web basé sur Vue.js, conçu pour simplifier la création d'applications web modernes et réactives. https://quasar.dev
Langages de programmation	• **Solidity :** Pour la réalisation de notre Smart contract.
Langage de modélisation	UML
Portefeuille	**MetaMask :** c'est un portefeuille logiciel de crypto-monnaie utilisé pour interagir avec la blockchain Ethereum. Il permet aux utilisateurs d'accéder à leur portefeuille Ethereum via une extension de navigateur ou une application mobile, qui peut ensuite être utilisée pour interagir avec des applications décentralisées.

2 Méthodes

la méthode implique une utilisation judicieuse de la technologie blockchain, des contrats intelligents, (standard de token non fongible), ainsi que des outils comme MetaMask et ThirdWeb pour créer un système décentralisé de gestion des dossiers de santé. Cette approche vise à assurer la sécurité, l'intégrité et la transparence des données tout en incitant la participation active des acteurs médicaux.

2.1 Comparaison entre la solution classique et la solution blockchain

TABLE 2.2 : Tableau comparatif de la solution classique par rapport à la solution blockchain.

	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 dhospitalisatio • 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 participati + premium).
Statut	Etat	Privé.
Sécurité	Hébergeur de donnée de santé	Blockchain
Hébergeur de donnée de santé	Non	Oui

2.1.1 Avantage

Notre mise en œuvre de la blockchain dans **DSESanté** abordera les problèmes majeurs soulignés ci-dessus :

- Traçabilité et Gestion des Accès ;
- Sécurité et Immutabilité ;
- Accessibilité et Efficacité ;
- Réduction des Erreurs ;
- Amélioration de la Communication ;
- Autonomie des Patients ;

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.

2.2 Enquête

Pour analyser les résultats de l'enquête ou sondage à **POLYCLINIQUE BIOSSO**, nous avons élaboré une fiche **(voir Annexe)**. L'idée est de réussir à les synthétiser pour obtenir des indicateurs clés sur le projet afin d'obtenir une analyse des résultats fiable et donc interprétable ainsi :

- Beaucoup de patients s'inquiètent sur le conflit des données (en réponse : Les conflits de données sont inexistants car seules de nouvelles données peuvent être ajoutées à la blockchain, les anciennes données ne peuvent pas être modifiées et les nouvelles entrées ne peuvent pas contredire les entrées précédentes) ;
- Pour d'autres patients malheureusement, il est fréquent que les prestataires de soins de santé, qui n'ont qu'une vue incomplète de l'ensemble des antécédents médicaux de leurs patients, gaspillent du temps et de l'argent pour des tests et des traitements inutiles ;
- Dix (10) professionnels de santé sur quinze (15) espèrent que les principaux bénéfices de la blockchain s'appliqueront aux essais cliniques et aux dossiers médicaux ;
- Douze (12) professionnels de santé sur vingt (20) pensent que la blockchain va les aider à accéder à de nouveaux marchés et à de nouvelles informations fiables et sécurisées. Les participants au réseau peuvent collaborer en toute confiance lorsqu'ils échangent des informations, tout en conservant le contrôle de l'accès aux données ;

3 Contexte

Le système est subdivisé en trois grandes parties, réparties en cinq blocs distincts. La première partie, consiste à créer des contrats intelligents et à les déployer sur la blockchain **Ethereum** en incluant les étapes d'authenfication, de confirmation, de signature, et autres. La deuxième partie, consiste à

concevoir une application **web** pour permettre aux différents utilisateurs du système d'interagir avec la Blockchain. En fonction du type d'utilisateur, un utilisateur peut envoyer des requêtes à travers l'application **web**. La troisième partie, consite à réaliser un algorithme de chiffrement symétrique pour chiffrer des documents avant de les envoyer sur la Blockchain. L'application décentralisée est nommée **"DSESanté"**. L'idée générale de la solution peut être interprétée par la figure 2.1.

3.1 Architecture Globale

Notre architecture globale est représentée ici en cinq (05) blocs qui sont :

1. Les contrats intelligents (smarts contracts) ;
2. ThirdWeb ;
3. Le réseau blockchain (Ganache, Goeli, Ethereum, ...) ;
4. MetaMask ;
5. DSESanté ;

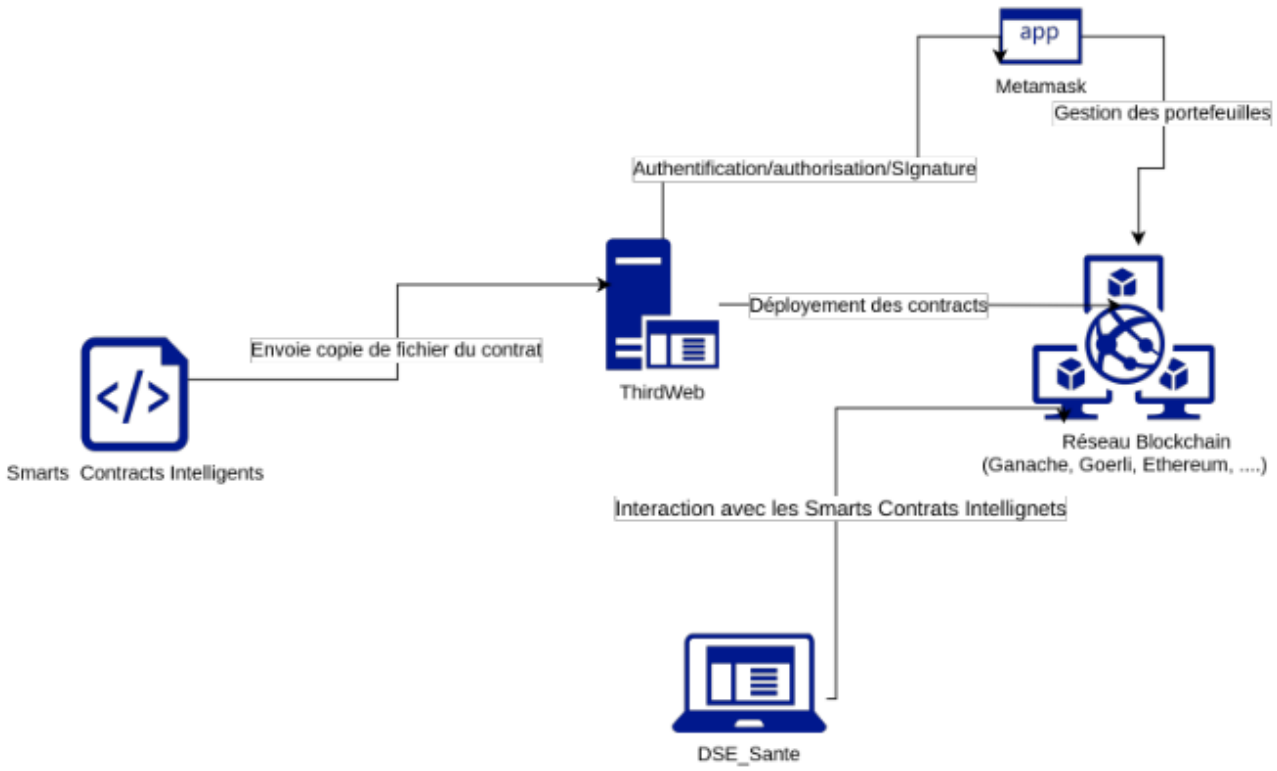


FIGURE 2.1 : Architecture Globale du système

3.2 Contrat intelligent

Les contrats intelligents sont des programmes informatiques auto-exécutables opérant sur la technologie de la blockchain, un registre distribué décentralisé. Ils automatisent l'exécution, la mise en œuvre et l'application de contrats, éliminant ainsi le besoin d'intermédiaires. Nous proposerons cinq (05) contrats dans le cadre de notre réalisation. Ces contrats seront basés sur des conditions prédéfinies et s'exécuteront de manière autonome une fois que ces conditions sont remplies, les rendant transparents, immuables et sécurisés.

4 Modélisation

Dans cette section du chapitre, nous présenterons le diagramme de cas d'utilisation pouvant nous aider à définir le fonctionnement du système.

4.1 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.

4.2 Diagrammes UML

4.2.1 Diagramme de cas d'utilisation du système

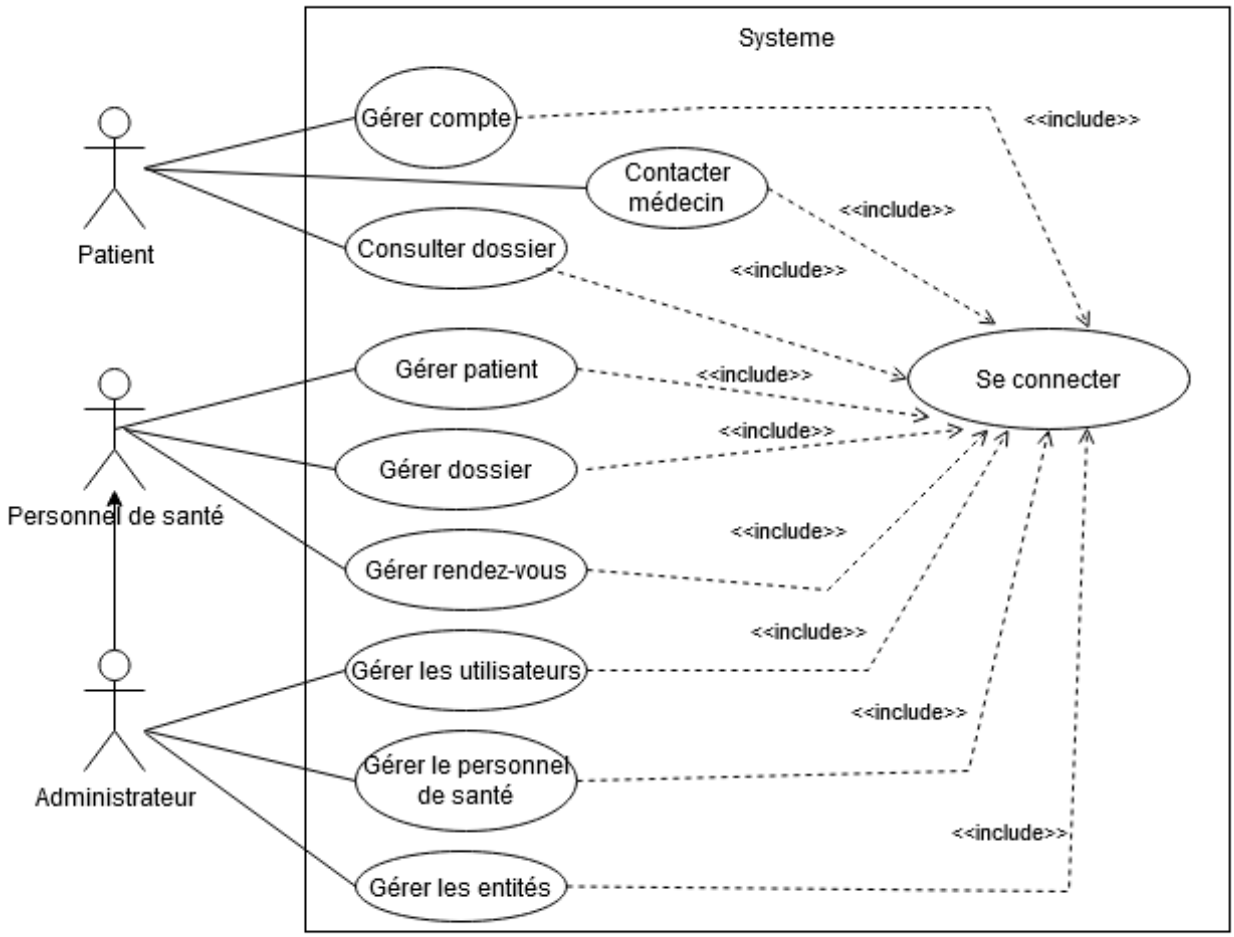


FIGURE 2.2 : Diagramme de cas d'utilisation du système

4.2.2 Diagramme de séquence

- **Diagramme de séquence du cas d'utilisation «Gérer les utilisateurs»**

Le personnel de santé peut ajouter un nouveau patient en remplissant un formulaire avec les données de ce dernier. L'administrateur affiche la liste des patients et ajoute également un nouveau patient dans le système. Il accorde des permissions au personnel de santé (lecture/écriture ou lecture) par rapport aux patients pour lesquels le contrat est créé, et la liste des nouveaux patients s'affiche dans le système.

La figure 2.3 ci-dessous illustre le diagramme de séquence, avec l'administrateur pour la gestion des patients et le personnel de santé pour la gestion des patients.

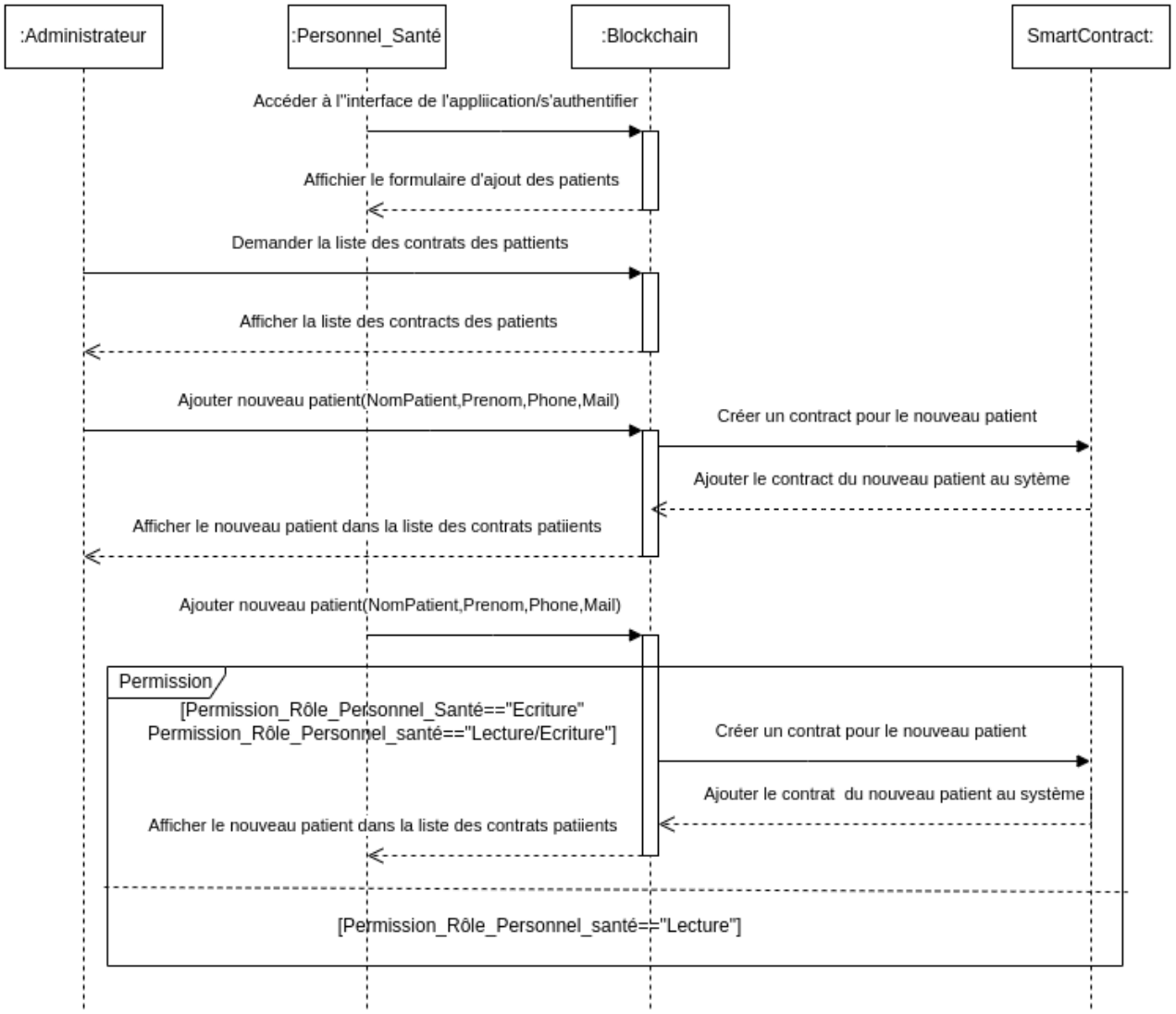


FIGURE 2.3 : Diagramme de séquence du cas d'utilisation «Gérer les utilisateurs».

- **Diagramme de séquence du cas d'utilisation «Gérer dossier»**

Le personnel de santé s'authentifie, puis affiche la liste des patients. Ensuite, il sélectionne un patient, demandant ainsi l'autorisation du patient. Si le patient accorde son autorisation, les informations de celui-ci s'affichent et le personnel de santé peut les consulter.

La figure 2.4 ci-dessous illustre le diagramme de séquence du cas d'utilisation «Gérer dossier».

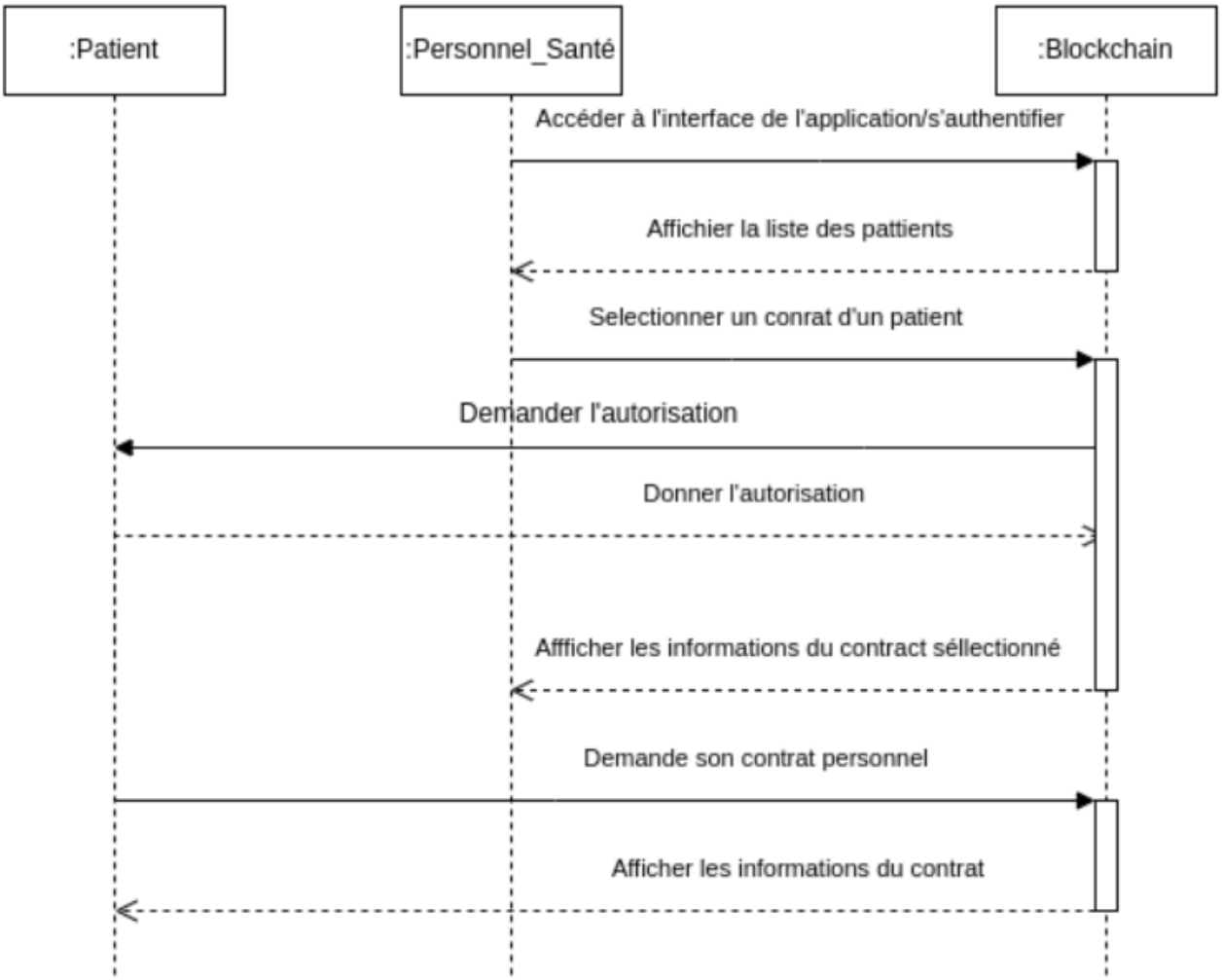


FIGURE 2.4 : Diagramme de séquence du cas d'utilisation «Gérer dossier».

- **Diagramme de séquence du cas d'utilisation «Gérer le personnel de santé»**

L'administrateur s'authentifie, ajoute un nouveau personnel de santé en remplissant un formulaire avec ses données, lui affecte un rôle, crée le contrat du personnel de santé, l'ajoute au système, et enfin, il s'affiche dans la liste du personnel de santé. La figure 2.5 ci-dessous illustre le diagramme de séquence du cas d'utilisation «Gérer le personnel de santé».

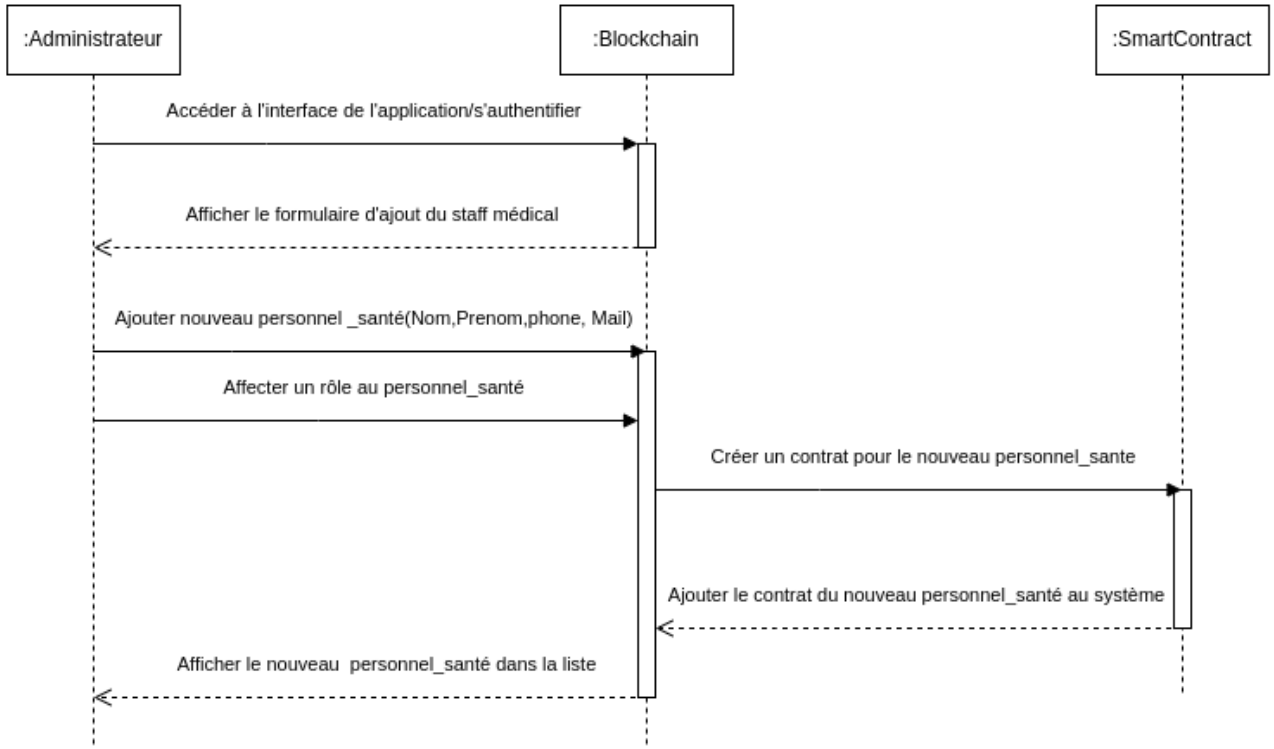


FIGURE 2.5 : Diagramme de séquence du cas d'utilisation «Gérer le personnel de santé».

Conclusion

Face aux nombreux défis posés par la santé et aux besoins suscités en termes de décentralisation, de traçabilité et de confiance, la blockchain offre des réponses. Bien qu'elle n'ait pas la prétention de résoudre tous les problèmes, elle ouvre la porte vers de nouveaux horizons, offrant ainsi des champs d'investigation inédits aux acteurs du domaine. Dans ce chapitre, nous avons présenté les outils et les langages de programmation utilisés pour la réalisation de notre système, accompagnés d'une modélisation UML à travers des diagrammes, exposant le développement de notre système. En conclusion, le prochain chapitre examinera les résultats et entamera les discussions.

Chapitre 3

Résultats et Discussion

Introduction

Ce chapitre est consacré à la réalisation de l'application et présenter l'implémentation du système, les résultats ainsi que les discussions.

1 Implémentation du système

2 Présentation des résultats

L'architecture globale 2.1 que nous avons élaborée représente une avancée significative dans la gestion des données médicales, fusionnant harmonieusement cinq composants essentiels. Les contrats intelligents, au cœur de notre système, sont des programmes autonomes déployés sur la blockchain locale (Ganache) grâce au cadre de développement ThirdWeb. Deux de ces contrats, basés sur le ERC721, offrent une méthode standardisée (non-fongible) pour Ajouter des examens et Rapports médicaux, automatisant ainsi des processus cruciaux dans le domaine de la santé. Notre réseau blockchain, constitué de Ganache, Goeli, Ethereum, etc., constitue une toile de fond sécurisée pour le déploiement transparent de ces contrats. MetaMask joue le rôle d'une interface sécurisée, assurant une connexion fluide entre notre environnement DSESanté, développé avec Vue.js, et les contrats intelligents déployés. Cette symbiose révolutionnaire vise à améliorer la communication, la collaboration, l'accessibilité aux documents et à réaliser des économies substantielles pour les centres de santé. En résumé, notre architecture propose une solution complète et novatrice pour la gestion efficace des données médicales, exploitant la puissance de la blockchain et de la technologie Web3.

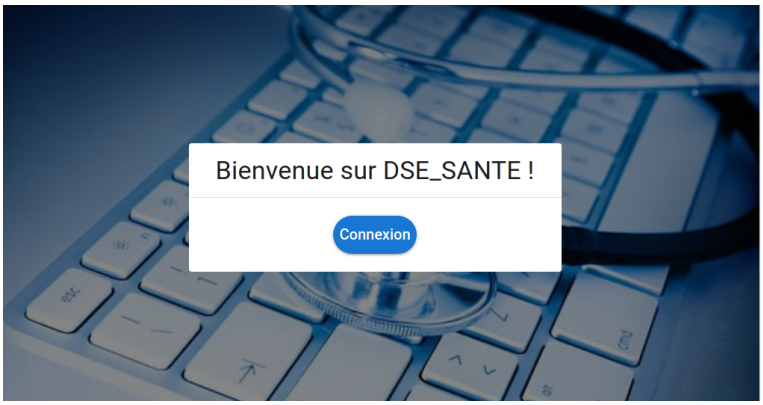


FIGURE 3.1 : Page de connexion

La procédure pour accéder à **"DSESanté"** se décompose en deux étapes intuitives. Tout d'abord, appuyez sur **"Connexion"**, où vous sélectionnerez votre compte et procéderez à l'authentification. Ensuite, dans la deuxième étape, cliquez simplement sur **"Connecter"** pour accéder. Cette démarche simple garantit une expérience conviviale et sécurisée pour tous les utilisateurs de **"DSESanté"**.

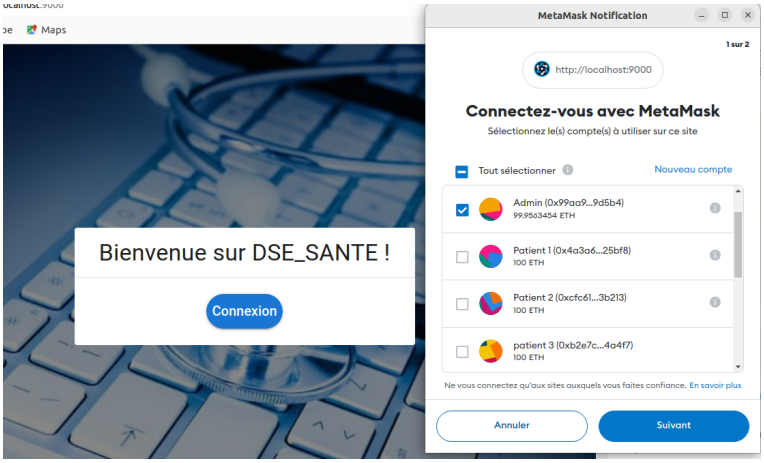


FIGURE 3.2 : Connexion : Etape 1

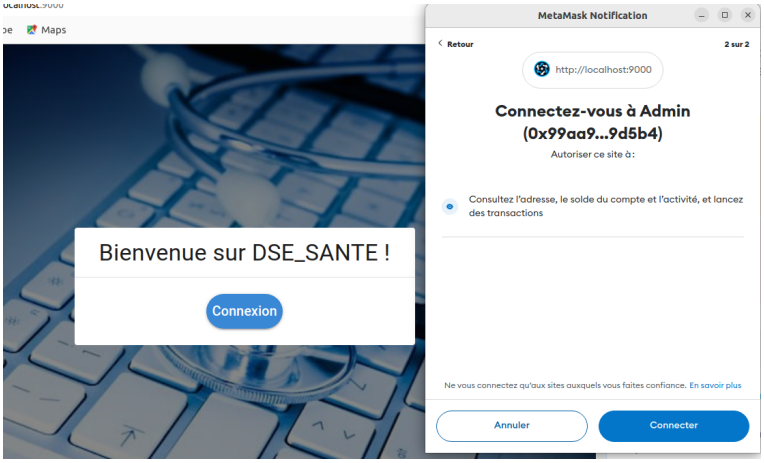


FIGURE 3.3 : Connexion : Etape 2

2.1 Les interfaces du système

2.1.1 Page d'enrégistrement et de recherche d'un patient

La figure 3.4 ci-dessous montre notre page qui permet d'enregistrer un patient sur la Blockchain et la figure 3.5 facilite la recherche d'un patient dans la liste à l'aide de son numéro d'identifiant.

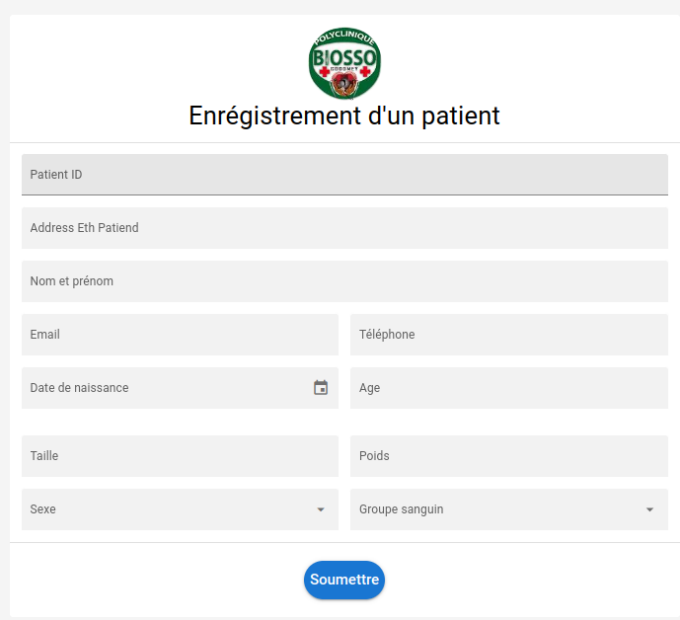


FIGURE 3.4 : Page d'enrégistrement d'un patient

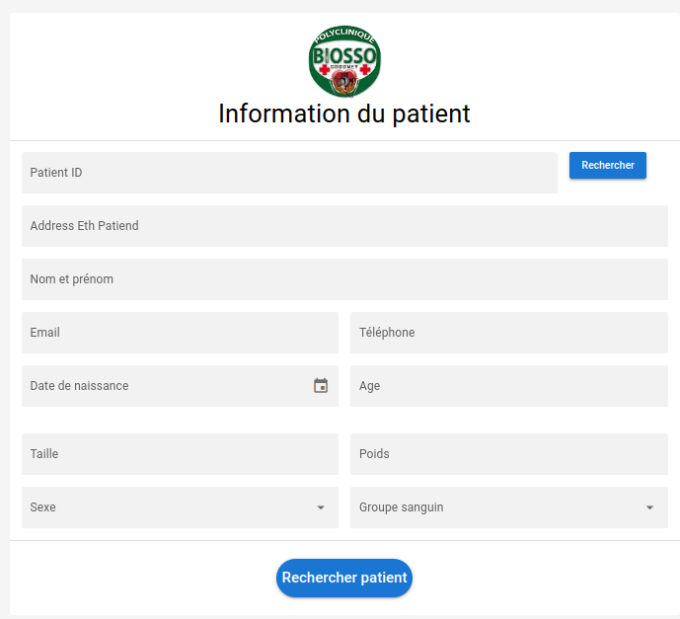


FIGURE 3.5 : Page de recherche d'un patient

2.1.2 Page d'enrégistrement et de recherche d'un médécin

La figure 3.6 ci-dessous montre notre page qui permet d'enregistrer un médécin sur la Blockchain et la figure 3.7 facilite la recherche d'un médécin dans la liste à l'aide de son numéro d'identifiant.

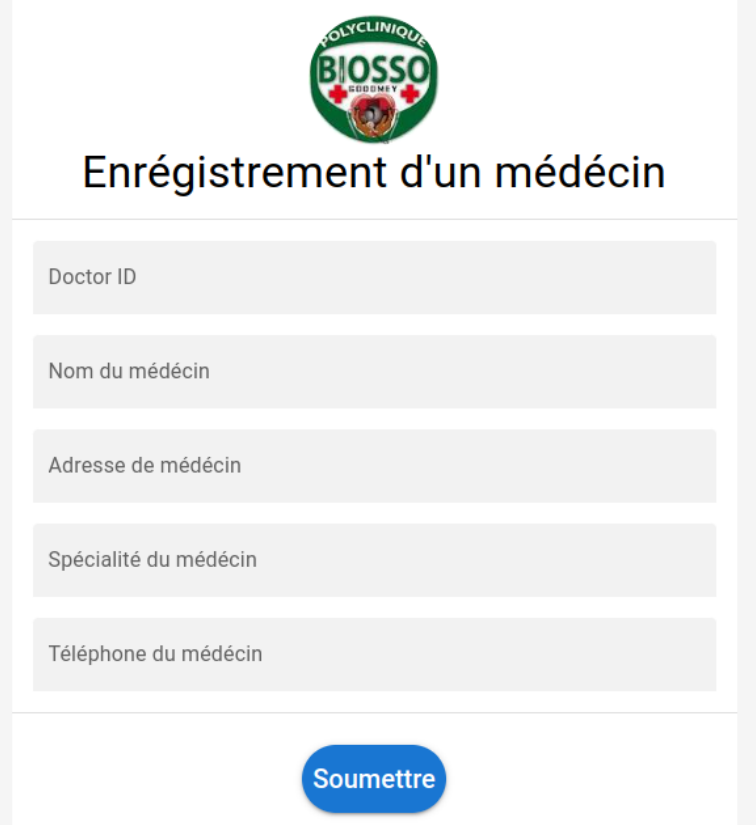


FIGURE 3.6 : Page d'enrégistrement d'un médécin



FIGURE 3.7 : Page de recherche d'un médécin

2.1.3 Page d'enrégistrement et de recherche d'hôpital

La figure 3.8 ci-dessous montre notre page qui permet d'enregistrer un hôpital sur la Blockchain et la figure 3.9 facilite la recherche d'un hôpital dans la liste à l'aide de son numéro d'identifiant.

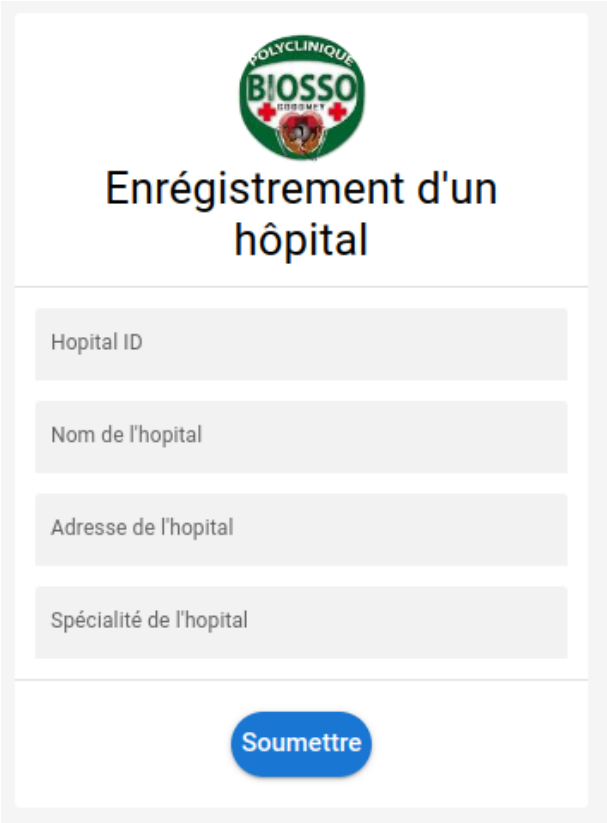


FIGURE 3.8 : Page d'enrégistrement d'un hôpital

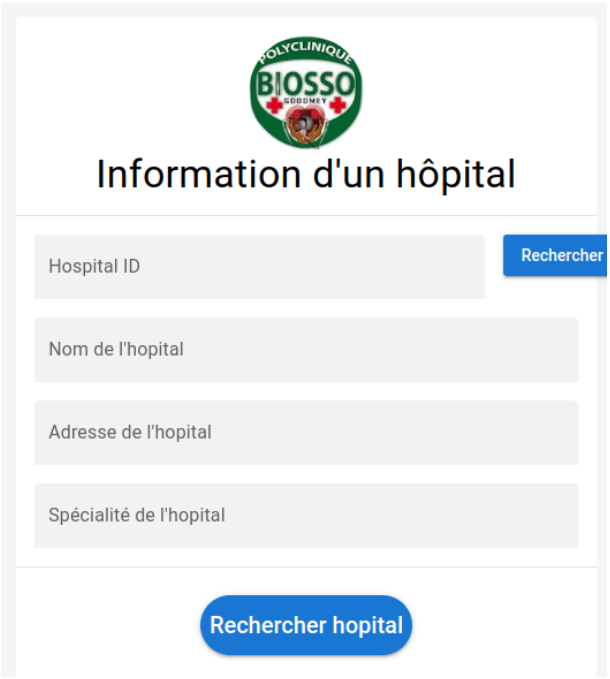


FIGURE 3.9 : Page de recherche d'un hôpital

2.1.4 Page d'enrégistrement et de recherche d'examen

La figure 3.10 ci-dessous montre notre page qui permet d'enregistrer un examen sur la Blockchain et peut également faciliter la recherche d'un examen dans la liste à l'aide du numéro d'identifiant d'un patient.

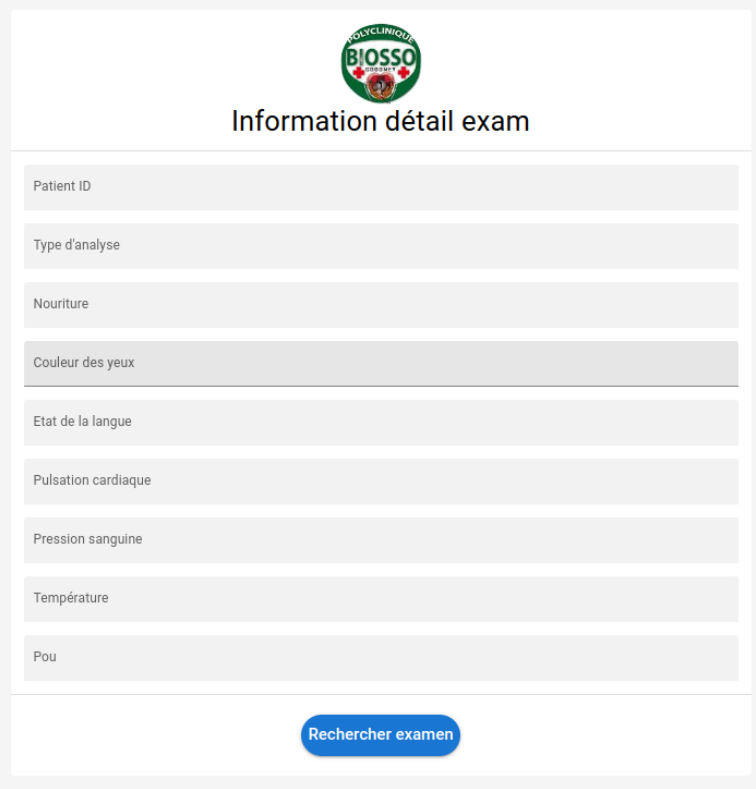


FIGURE 3.10 : Page de recherche détaillée des examens

2.1.5 Page d'enrégistrement ou de recherche d'un diagnostic

La figure 3.11 ci-dessous montre notre page qui permet d'enregistrer un diagnostic sur la Blockchain et peut également faciliter la recherche dans la liste à l'aide du numéro d'identifiant d'un patient.

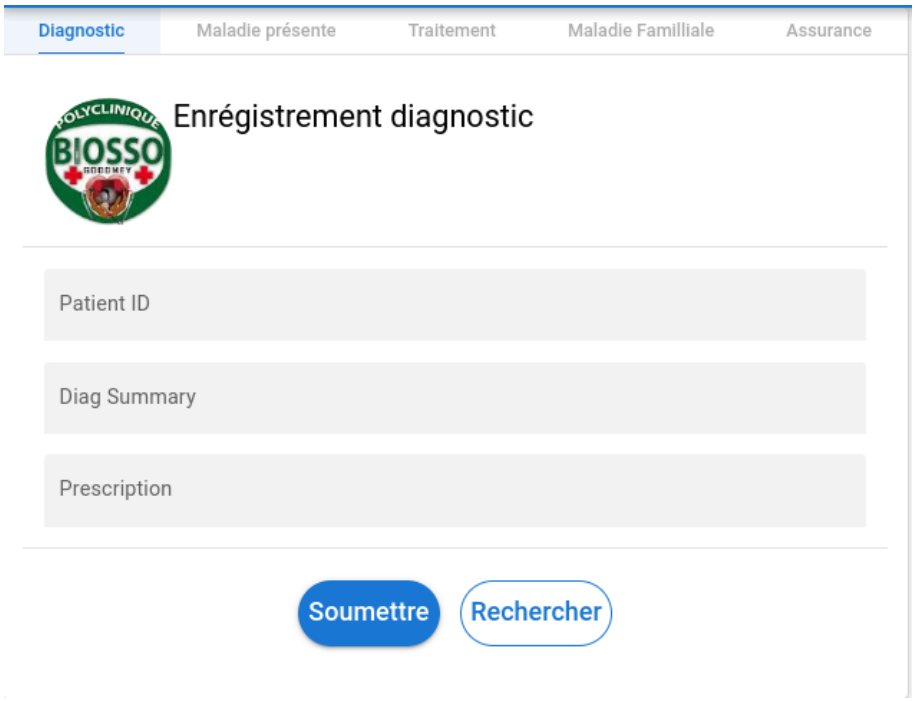


FIGURE 3.11 : Page d'enrégistrement ou de recherche d'un diagnostic

2.1.6 Page d'enrégistrement ou de recherche d'une maladie présente

La figure 3.12 ci-dessous montre notre page qui permet d'enregistrer une maladie présente sur la Blockchain et peut également faciliter la recherche dans la liste à l'aide du numéro d'identifiant d'un patient.



FIGURE 3.12 : Page d'enrégistrement ou de recherche de la maladie preésente

2.1.7 Page d'enrégistrement ou de recherche d'un traitement

La figure 3.13 ci-dessous montre notre page qui permet d'enregistrer le traitement d'un patient sur la Blockchain et peut également faciliter la recherche dans la liste à l'aide du numéro d'identifiant d'un patient.

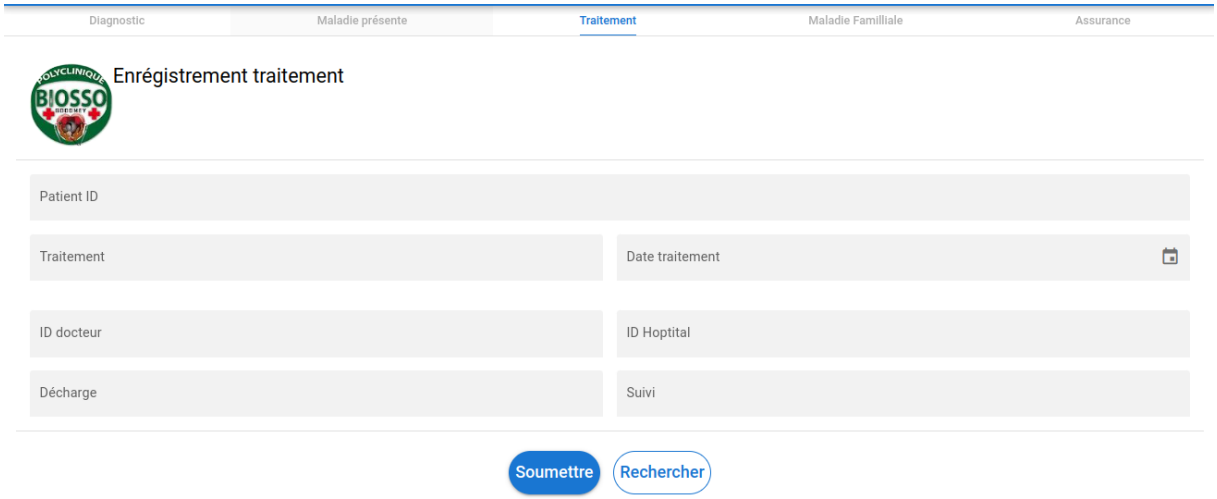


FIGURE 3.13 : Page d'enrégistrement ou de recherche d'un traitement

2.1.8 Page d'enrégistrement ou de recherche d'une maladie familiale

La figure 3.14 ci-dessous montre notre page qui permet d'enregistrer une maladie familiale d'un patient sur la Blockchain et peut également faciliter la recherche dans la liste à l'aide du numéro d'identifiant d'un patient.



FIGURE 3.14 : Page d'enrégistrement ou de recherche d'une maladie familiale

2.1.9 Page d'enrégistrement ou de recherche d'assurance

La figure 3.15 ci-dessous montre notre page qui permet d'enregistrer le nom de l'assureur d'un patient tout en prenant en compte le taux d'assurance sur la Blockchain. Elle facilite également la recherche dans la liste à l'aide du numéro d'identifiant d'un patient.

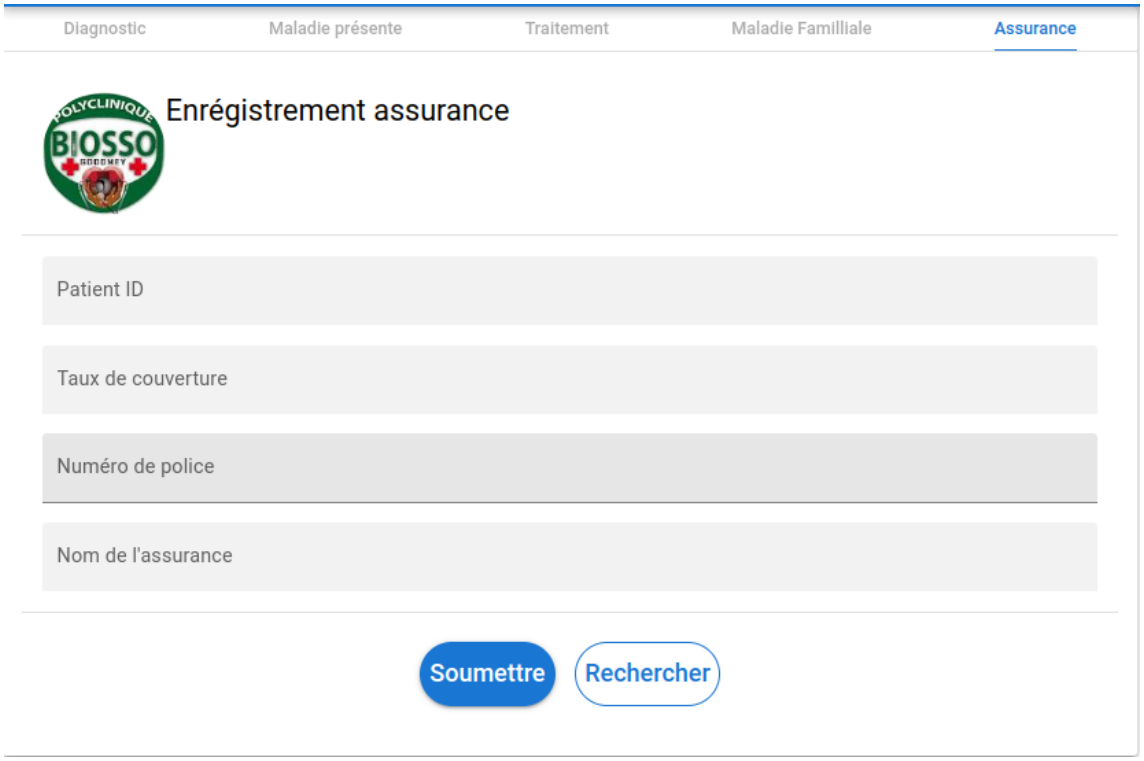


FIGURE 3.15 : Page d'enrégistrement ou de recherche d'une assurance

3 Avantages et limites

3.1 Avantage de prototype proposé

Notre prototype d'application, utilisant la technologie Blockchain pour stocker des données médicales, présente plusieurs avantages significatifs. Il garantit la sécurité et l'intégrité des données grâce à la cryptographie et à la décentralisation, tout en offrant une transparence totale. Les patients ont un contrôle total sur l'accès à leurs informations médicales, éliminant ainsi le besoin d'intermédiaires. De plus, la Blockchain facilite la gestion des identités, améliore l'interopérabilité des systèmes de santé et permet la traçabilité des traitements. Elle peut également favoriser la recherche médicale tout en assurant la conformité réglementaire, ce qui en fait une solution prometteuse pour le secteur de la santé.

3.2 Limites

Notre travail consiste à élaborer une application exploitant la technologie de la Blockchain afin de stocker des données dans le domaine de la santé. Cependant, le prototype actuellement en développement présente certaines limitations. Il ne comporte pas de fonctionnalité permettant d'envoyer

automatiquement au patient les informations liées à ses données de soins dès que les diagnostics et autres informations sont ajoutés à la blockchain.

3.3 Discussion de notre solution

La solution proposée pour sécuriser les données médicales des patients en utilisant des contrats intelligents avec la technologie de la blockchain offre bien plus qu'une simple sécurité des données. En effet, grâce à la nature immuable et transparente de la blockchain, chaque transaction et interaction médicale peut être enregistrée de manière chronologique, formant ainsi un historique complet et inaltérable des traitements et des soins reçus par le patient. Cette fonctionnalité permet aux professionnels de la santé d'accéder facilement à un profil médical précis et complet, facilitant ainsi la prise de décision clinique et la coordination des soins. De plus, cette traçabilité accrue des données médicales contribue à renforcer la confiance entre les patients et les prestataires de soins, car elle garantit l'intégrité et la confidentialité de leurs informations de santé tout en permettant une transparence accrue dans la gestion des dossiers médicaux. Ainsi, la technologie de la blockchain offre non seulement une protection des données, mais également une solution robuste pour la création et la gestion d'un historique médical complet et fiable pour chaque patient.

Conclusion

Dans ce chapitre, nous avons exposé les résultats de notre solution, visant à assurer la sécurité des données de santé et le partage des informations des patients entre les différents acteurs par le biais de Smart contrats. Nous avons présenté les résultats des tests de notre application après son implémentation, illustrés à travers diverses captures d'interfaces. Par la suite, nous avons abordé les avantages et les limites de notre solution. Enfin, nous avons discuté de notre application et fourni des réponses à d'éventuelles interrogations. La conclusion générale synthétise notre travail et met l'accent sur les perspectives.

Conclusion générale et perspectives

Le secteur de la santé, en particulier, renferme des données très sensibles et privées. Actuellement, ces informations médicales sont dispersées dans différentes institutions médicales, compliquant ainsi la tâche des patients qui souhaitent accéder à l'ensemble de leurs dossiers. C'est dans ce contexte que nous avons exploré les techniques de la blockchain, une technologie offrant la possibilité de stocker et de transmettre des informations de manière transparente et sécurisée, tout en préservant l'intégrité des données.

Notre projet s'est focalisé sur la mise en place d'un système de gestion des dossiers de santé électroniques des patients en utilisant la technologie blockchain. Cette réalisation comprend un site web dédié à la gestion de DSESanté des patients et une blockchain dédiée au stockage sécurisé des données médicales. Cette initiative a été bénéfique, renforçant nos connaissances théoriques dans le domaine de la blockchain, des cryptomonnaies et de la conception. De plus, elle nous a permis d'acquérir des compétences en cryptographie, que nous avons appliquées dans le cadre de notre projet.

Bien que notre solution offre actuellement un ensemble de services, elle reste perfectible. À la fin de notre travail, nous identifions des perspectives d'amélioration pour continuer à développer et à optimiser notre système. 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 QR ;
- Utiliser et bénéficier du Cloud pour résoudre le problème du stockage des données médicales ;
- Grâce aux données qu'elle contiendra, il sera possible d'ouvrir le champ du big data et de l'IA sur nos données de santé pour ouvrir de nouveaux horizons thérapeutiques et sociétaux, le tout en gardant le contrôle de nos données ;

Bibliographie

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

[2] S. CANGÉ. Pourquoi les contrats intelligents sont aussi importants pour la blockchain ?. - la-finance pour tous. https://cryptonaute.fr/ pourquoi-les-contrats-intelligents-importent-pour-la-blockchain//.
consulté le 25 janvier 2021,.

[3] A. Marko. What is the algorithm sha 256 ?. explain the miningcrypto algorithms. https://blockgeeks.com/guides/ what-is-hashing//.
consulté le 20 janvier 2021,.

[4] M. Musumeci. Comment fonctionne la signature numérique. https://blogs.pme.ch/massimo-musumeci.
consulté le 06 juillet 2020,.

[5] A. Rosic. Caractéristiques principales de la blockchain. https://fr.acervolima.com/caracteristiques-de-la-blockchain/.
consulté le 29 novembre 2021,.

[6] A. Rosic. Caractéristiques principales de la blockchain. https://fr.acervolima.com/caracteristiques-de-la-blockchain/.
consulté le 29 novembre 2021,.

[7] A. Rosic. La cryptographie et la blockchain. https://www.editions-eni.fr/.
consulté le 27 juin 2022,.

[8] A. Rosic. Smart contracts : The blockchain technology that will replace lawyers, blockgeeks. https://blockgeeks.com/guides/smart-contracts/.
consulté le 25 novembre 2020.

[9] A. Rosic. What is hashing ?. https://blockgeeks.com/guides/ what-is-hashing//.
consulté le 05 mai 2020,.

Webographie

[18] Wikipédia - l'encyclopédie libre (19 mars 2022). Intelligence artificielle. Consulté le 2 Octobre 2022 à l'adresse https://fr.wikipedia.org/wiki/Intelligence_artificielle

[19] Qu'est-ce que l'IA ? En savoir plus sur l'intelligence artificielle. Consulté le 2 Octobre 2022 à l'adresse https://www.oracle.com/fr/artificial-intelligence/what-is-ai/

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

. v

Table des figures vi

Liste des tableaux viii

Sigles et abreviations ix

Glossaire x

Introduction 1

1 Contexte et justification 1
2 Problématique 2
3 Objectifs 2
4 Organisation du mémoire 3

1 Généralités sur la techologie blockchain et la cryptographie 4

Introduction 4
1 Notions sur la Blockchain 4
1.1 Définition 4
1.2 Historique de la blockchain 5
1.3 Caractéristiques principales de la blockchain 5
1.4 Fonctionnement de la blockchain 5
1.5 Structure d'une blochaine 8
1.6 Transaction 8
1.7 Blocs 9
1.7.1 Processus de consensus 10
1.8 Fontions de hachage cryptographiques 11
1.8.1 Hachage 11
1.8.2 Fonctions de hachage 11
1.8.3 Hachage **SHA-256** 12
1.9 Mineurs et les nœuds 12

1.9.1 Mineurs . . . 12
1.9.2 Les nœuds . . . 12
1.10 Contrats intelligents . . . 14
1.10.1 Définition . . . 14
1.10.2 Caractéristiques . . . 14
1.10.3 Fonctionnement . . . 14
1.10.4 Avantages de contrats intelligents . . . 14
1.10.5 Inconvénients de contrats intelligents . . . 15
1.10.6 la blockchaine en tant que transaction signées . . . 15
2 Généralités sur la cryptographie . . . 17
2.1 Définition . . . 17
2.2 Caractéristiques de la cryptographie . . . 17
2.3 Chiffrement symétrique . . . 17
2.3.1 Définition . . . 17
2.3.2 Principe de fonctionnement . . . 18
2.4 Interêt de la cryptographie asymétrique dans un réseau blockchain . . . 20
2.4.1 Gestion des identités sur le réseau . . . 20
2.4.2 La signature numérique . . . 21
2.5 Types de blockchains . . . 21
2.5.1 Blockchains publiques . . . 21
2.5.2 Blockchains privées . . . 22
2.5.3 Blockchains consortiums (hybride) . . . 22
2.6 les types de fautes dans un réseau . . . 22
2.6.1 Preuve de travail . . . 22
2.7 Blockchain aujourdhui . . . 23
2.7.1 Bitcoin . . . 23
2.7.2 Crypto-monnaies . . . 23
2.7.3 Ethereum . . . 24
2.7.4 Hyperledger Fabric . . . 24
Conclusion . . . 24

2 Matériels, Méthodes, Architecture et Modélisation 25
Introduction . . . 25
1 Matériels et outils . . . 25
1.1 Outils et Langages de programmation . . . 26
2 Méthodes . . . 28
2.1 Comparaison entre la solution classique et la solution blockchain . . . 28
2.1.1 Avantage . . . 29
2.2 Enquête . . . 29
3 Contexte . . . 29
3.1 Architecture Globale . . . 30
3.2 Contrat intelligent . . . 30
4 Modélisation . . . 31
4.1 Acteurs du système . . . 31
4.2 Diagrammes UML . . . 32

4.2.1 Diagramme de cas d'utilisation du système . . . 32
4.2.2 Diagramme de séquence . . . 32
Conclusion . . . 35

3 Résultats et Discussion **36**
Introduction . . . 36
1 Implémentation du système . . . 36
2 Présentation des résultats . . . 36
2.1 Les interfaces du système . . . 38
2.1.1 Page d'enrégistrement et de recherche d'un patient . . . 38
2.1.2 Page d'enrégistrement et de recherche d'un médécin . . . 38
2.1.3 Page d'enrégistrement et de recherche d'hôpital . . . 40
2.1.4 Page d'enrégistrement et de recherche d'examen . . . 41
2.1.5 Page d'enrégistrement ou de recherche d'un diagnostic . . . 41
2.1.6 Page d'enrégistrement ou de recherche d'une maladie présente . . . 42
2.1.7 Page d'enrégistrement ou de recherche d'un traitement . . . 43
2.1.8 Page d'enrégistrement ou de recherche d'une maladie familiale . . . 43
2.1.9 Page d'enrégistrement ou de recherche d'assurance . . . 44
3 Avantages et limites . . . 44
3.1 Avantage de prototype proposé . . . 44
3.2 Limites . . . 44
3.3 Discussion de notre solution . . . 45
Conclusion . . . 45

Conclusion **46**

Bibliographie **47**

Bibliographie **47**

Webographie **48**

Table des matières **49**

Annexe **52**
Introduction . . . 52
4 Fiche d'enquête . . . 52
5 Autres captures . . . 54

Annexe

4 Fiche d'enquête

Vous pouvez nous aider à améliorer la qualité des services en nous donnant votre opinion. Toutes les informations recueillies dans ce questionnaire sont strictement anonymes et confidentielles. En se basant sur votre séjour en tant que patient ou personnel de santé à la **POLYCLINIQUE BIOSSO**. Est-ce-que vous êtes d'accord avec les déclarations suivantes :
O = oui ; N = non ; 1 = pas d'accord ; 2 = d'accord ; 5 = parfaitement d'accord.
Vous pouvez choisir qu'une seule réponse par question.

-	Information / Communication/ Relations interpersonnelles	O	N	1	2	3
-	**RUBRIQUE PATIENT**	-	-	-	-	-
1	Êtes-vous à votre premier passage dans un centre de santé ?					
2	Comment trouvez-vous le service d'accueil et les rendez-vous ? ?					
3	Comment percevez-vous la communication entre le médecin et le patient ?					
4	Le médecin vous a-t-il fourni des explications claires concernant vos problèmes, votre état de santé, votre traitement et le déroulement de vos examens ?					
5	Possédez-vous l'historique complet de vos soins, depuis la naissance jusqu'à aujourd'hui ?					
6	Pouvez-vous fournir avec précision vos antécédents médicaux, y compris les pathologies passées et les traitements effectués ?					
7	Disposez-vous des résultats d'examens, des comptes rendus d'hospitalisation et d'autres antécédents médicaux (observations, prescriptions, comptes rendus opératoires, anatomopathologie, feuilles de température, lettres de sortie, etc.) ?					
8	Souhaitez-vous disposer d'une carte sécurisée contenant l'ensemble de vos données de santé ?					
-	**RUBRIQUE PERSONNEL DE SANTE**	-	-	-	-	-
9	Pouvez-vous effectuer des vérifications d'authenticité des médicaments utilisés par le passé et assurer la traçabilité des ordonnances médicales de vos patients ?					
10	Pouvez-vous garantir l'immutabilité (conservation permanente des données qu) di peuvent pas être altérées ni supprimées.es informations sur les fiches des patients stockées dans les archives ?					
11	En tant que professionnel de la santé, disposez-vous d'un historique complet et d'une traçabilité des maladies et traitements de vos patients depuis le début de votre carrière ?					
12	En tant que professionnel de la santé, avez-vous déjà rencontré quelqu'un qui possède un registre d'antécédents médicaux ?					
13	Souhaitez-vous que vos patients aient accès à leurs données de santé au moyen d'une clé de sécurisée ?					

TABLE 3.1 : Tableau de la fiche d'enquête

5 Autres captures

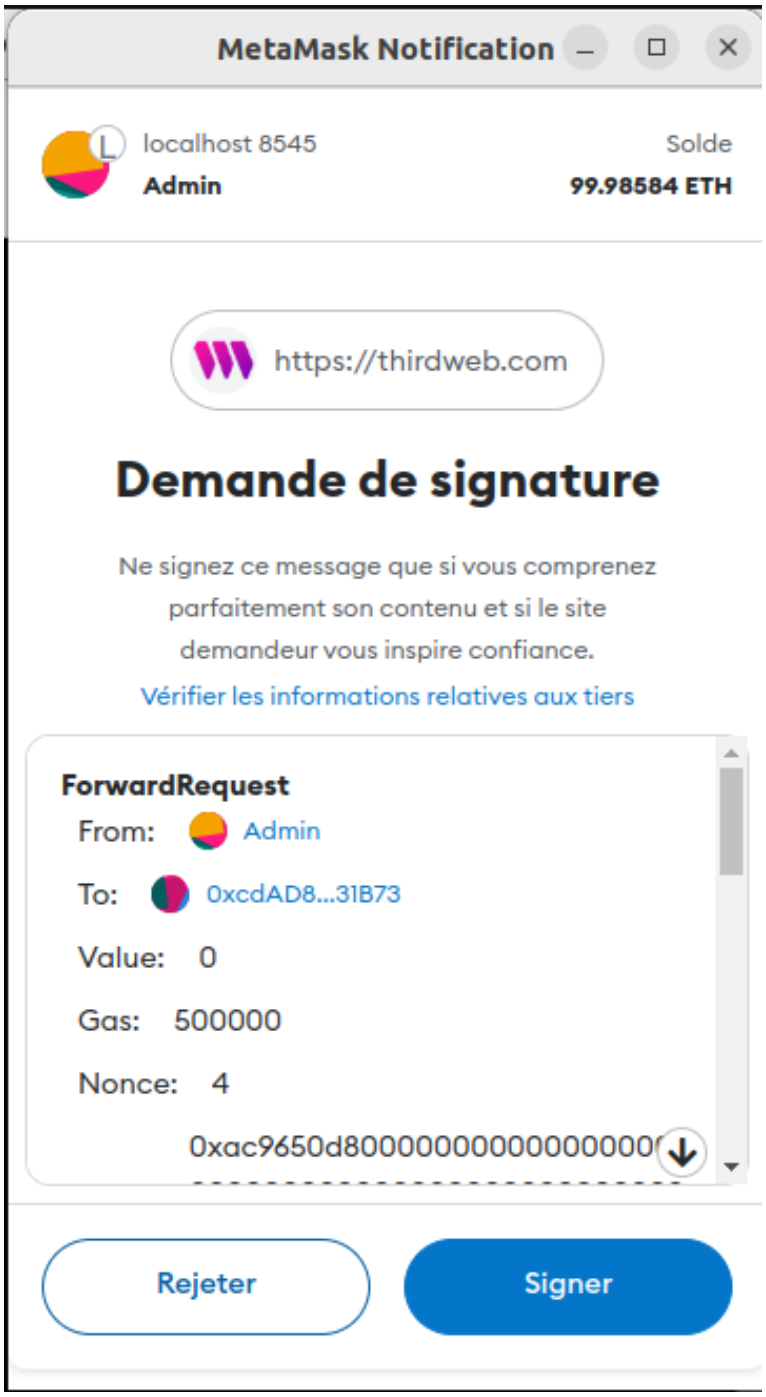


FIGURE 3.16 : Demande de signature pour le transfert des contrats intelligents

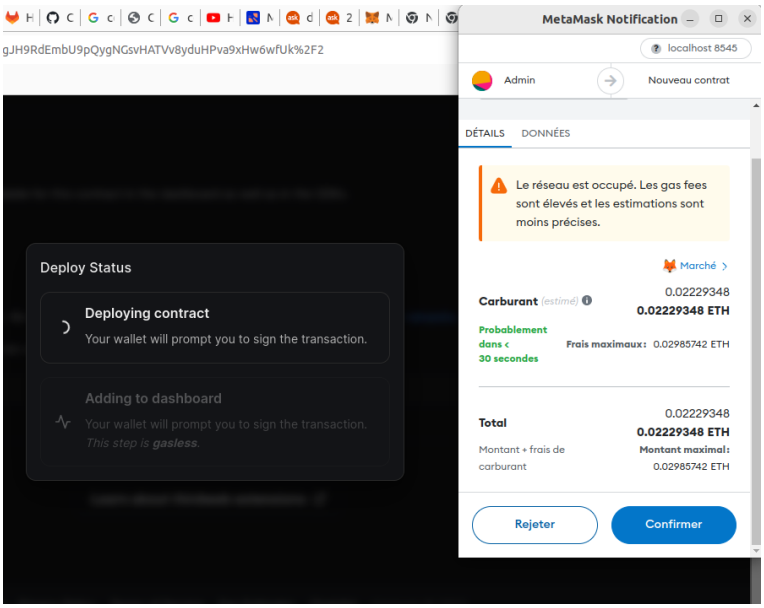


FIGURE 3.17 : Confirmation du transfert

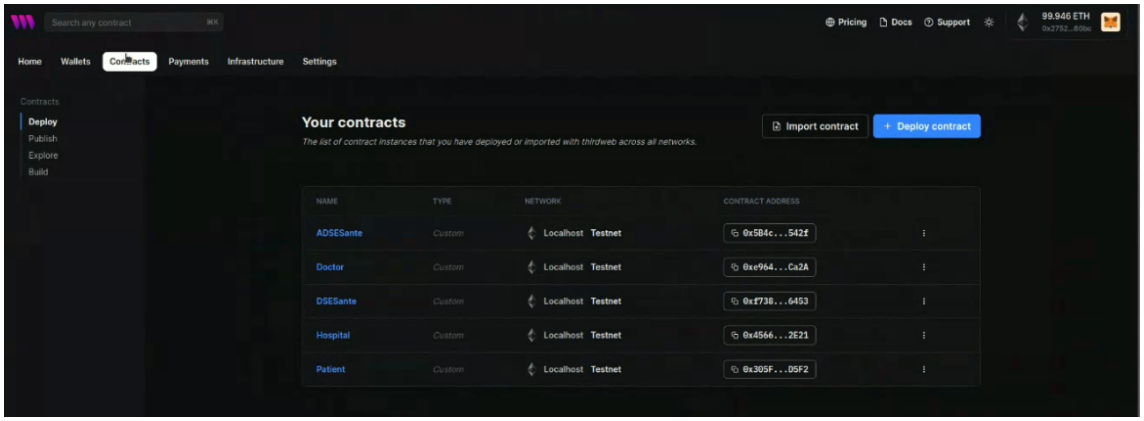


FIGURE 3.18 : Le déploiement des contrats sur ThirdWeb

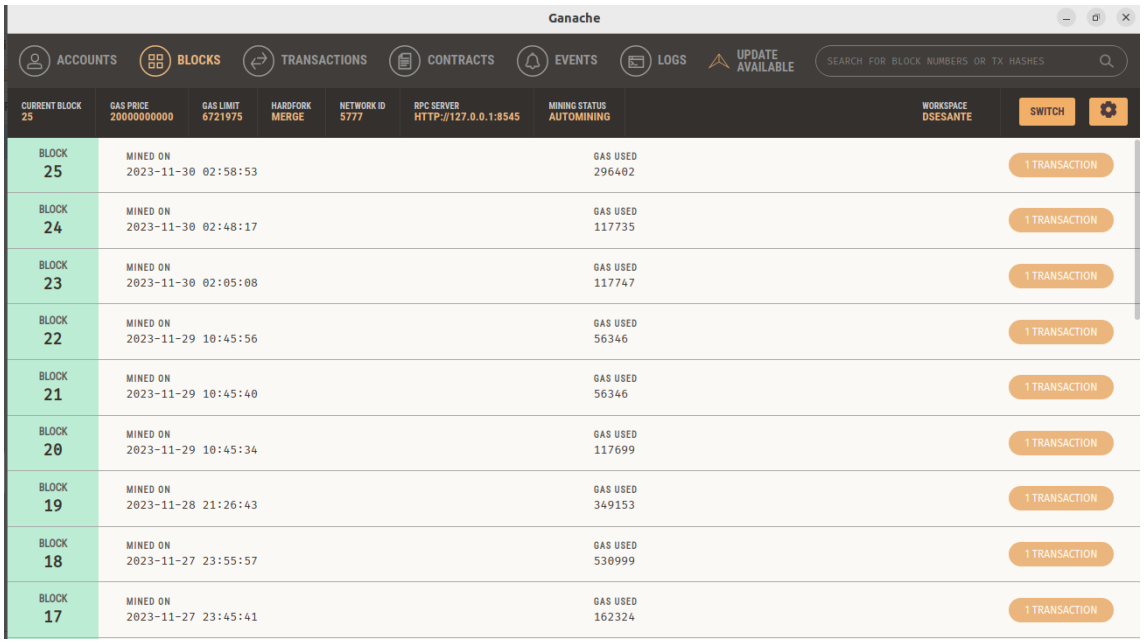


FIGURE 3.19 : Construction de la chaîne de Blocs dans Ganache