MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et d'Informatique

Département de Mathématiques et informatique

Filière : Informatique

MEMOIRE DE FIN D'ETUDES

Pour l'Obtention du Diplôme de Master en Informatique

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

Présenté par :

BENNACEUR MADIHA

ELARICHE ANFEL

THEME :

La sécurité des données personnelles et médicales à l'aide de la blockchain

Devant le jury composé de :

Mme Houcine	Présidente
Mme Benidris	Examinatrice
Mr MIROUD Mohamed El Mustapha	Encadreur

Année Universitaire 2023-2024

Résumé

L'objectif principal de notre projet de fin d'étude est d'approfondir notre compréhension des applications de la blockchain. Nous avons commencé par explorer la technologie blockchain pour en comprendre le fonctionnement. Ensuite nous avons étudié comment elle peut être utilisée pour sécuriser des données sensibles de manière décentralisée. Notre projet se concentre sur la résolution du problème de partage d'informations dans le domaine médical, qui nécessite une sécurité, une confiance et une transparence accrues des accès.

Nous avons proposé une solution basée sur la blockchain et les contrats intelligents afin d'assurer la sécurité du partage des informations des patients entre les différents acteurs de l'industrie médicale. Concrètement, nous avons développé des contrats intelligents sur la plateforme Ethereum, accompagnés d'une interface web intuitive. La solution que nous avons proposée met le patient au centre du protocole de partage et le garde maître de ses données afin de lui garantir une plus grande protection.

Ce projet démontre comment la blockchain peut transformer la gestion des données médicales en garantissant une plus grande fiabilité ainsi qu'une plus grande confidentialité des informations partagées.

Mots-clés:

Blockchain, Bitcoin, cryptographie, confidentialité, Protection des données à caractère sensible, secret médical, protocole d'accès décentralisé, cryptomonnaies, Ethereum, Smart contracts, Solidity.

Abstract

The main objective of our final year project is to deepen our understanding of blockchain applications. We began by exploring blockchain technology to understand how it works. Then, we studied how it can be used to securely handle sensitive data in

a decentralized manner. Our project focuses on solving the problem of information sharing in the medical field, which requires increased security, trust, and transparency in access.

We proposed a solution based on blockchain and smart contracts to ensure the security of patient information sharing among various stakeholders in the medical industry. Specifically, we developed smart contracts on the Ethereum platform, accompanied by an intuitive web interface. The solution we proposed places the patient at the center of the sharing protocol and keeps them in control of their data to ensure greater protection.

This project demonstrates how blockchain can transform the management of medical data by ensuring greater reliability and confidentiality of shared information.

Keywords:

Blockchain, Bitcoin, cryptography, privacy, sensitive data protection, medical confidentiality, decentralized access protocol, cryptocurrencies, Ethereum, smart contracts, Solidity.

ملخص

الهدف الرئيسي من مشروعنا النهائي هو تعميق فهمنا لتطبيقات تقنية البلوكشين. بدأنا باكتشاف تقنية البلوكشين لفهم كيفية عملها. ثم قمنا بدراسة كيفية استخدامها لتأمين البيانات الحساسة بطريقة لا مركزية. يركز مشروعنا على حل مشكلة مشاركة المعلومات في المجال الطبي، والتي تتطلب أمانًا وثقة وشفافية أكبر في الوصول.

لقد اقترحنا حلاً يعتمد على تقنية البلوكشين والعقود الذكية لضمان أمان مشاركة معلومات المرضى بين مختلف الجهات في الصناعة الطبية. على وجه التحديد، قمنا بتطوير عقود ذكية على منصة إيثيريوم، مصحوبة بواجهة ويب بديهية. الحل الذي اقترحناه يضع المريض في مركز بروتوكول المشاركة ويبقيه مسيطرًا على بياناته لضمان حماية أكبر له .

يظهر هذا المشروع كيف يمكن لتقنية البلوكشين أن تحول إدارة البيانات الطبية من خلال ضمان م أكبر وسرية أكبر للمعلومات المشتركة.

Dédicaces

Je dédie ce modeste travail à :
Moi-même avant tout, pour mes efforts et ma détermination à exceller.

Mes chers parents pour leur soutien indéfectible et tous les sacrifices qu'ils ont consentis pour que je réussisse. Votre amour inconditionnel et vos encouragements constants ont été ma source de motivation.

Je le dédie également à :
Ma sœurs et mes frères, ma nièce LYDIA et mon neveu ADAM que j'aime énormément.
Votre joie de vivre et votre présence précieuse ont enrichi ma vie d'une manière unique.

Je tiens également à exprimer ma reconnaissance envers mes merveilleuses amies avec qui j'ai partagé des moments précieux et des souvenirs inoubliables."

ANFEL EL ARICHE

Dédicaces

Avant toute chose, je remercie Allah عز وجل de m'avoir guidé et permis d'atteindre mon rêve.

Je tiens à exprimer ma plus profonde gratitude à ma famille pour son soutien incommensurable tout au long de mes études. À mes parents, qui m'ont inculqué des valeurs de persévérance et de détermination, et à tous mes frères et sœurs, pour leur encouragement constant.

Je remercie également tous ceux qui ont contribué de près ou de loin à l'achèvement de ce travail. Vos conseils, votre aide et votre soutien ont été précieux. Un remerciement particulier à mes professeurs pour leur enseignement et leurs encouragements, ainsi qu'à mon directeur de thèse pour son encadrement et ses conseils avisés.

*Enfin, une pensée spéciale pour mes amis, pour leur amitié, leur soutien moral et pour avoir partagé avec moi tant de moments mémorable*s.

BENNACEUR MADIHA

Remerciements

Tout d’abord, nous tenons à remercier ALLAH le tout puissant pour la force et le courage qu’il nous a accordé pour mener à bien ce modeste travail. Nous remercions également nos petites familles pour l’inconditionnel soutien qu’elles nous ont généreusement offert.

Nous tenons à remercier également tous ceux et celles qui ont contribué à finaliser ce modeste travail.

Nos remerciements vont aussi à monsieur ***MIROUD Mohammed el Mustapha***, notre encadrant, pour nous avoir guidé dans la réalisation de ce projet pour son précieux encadrement, ses conseils avisés et son soutien constant tout au long de ce parcours. Son expertise, sa patience et son dévouement ont été inestimables pour surmonter les défis rencontrés et mener à bien ce projet.

Nous tenons également à remercier toute l’équipe de la faculté des sciences exactes et de l’informatique ***FSEI*** Mostaganem, tous les enseignants et toutes les enseignantes, sans oublier l’ensemble du personnel non-enseignant. Enfin, nous tenons aussi à remercier ***les membres du jury*** pour avoir accepté d’examiner et d'évaluer notre travail.

EL ARICHE Anfel & BENNACEUR Madiha

Liste des figures

Figure N°	Titre de la figure	Page
Figure 1	Construction d'un arbre de Merkle	7
Figure 2	**- Présentation d'une chaîne de blocs (blockchain)**	8
Figure 3	**Fonctionnement de la blockchain**	8
Figure 4	Illustration d'une signature digitale.	10
Figure 5	**Le chiffrement symétrique**	10
Figure 6	De gauche à droite, réseaux centralisés , décentralisés et distribués (Blockchain)	14
Figure 7	Consommation de l'énergie électrique par les blockchains Bitcoin et Ethereum	16
Figure 8	Blockchain dans le secteur de la santé	23
Figure 9	Blockchain dans le secteur de la santé	32
Figure 10	Le secret S et la droite qui lui correspond.	41
Figure 11	Une multitude courbe peuvent passer par un seul point	42
Figure 12	D reconstruction du secret partagé avec un seuil égal à 2	43
Figure 13	Diagramme de profile	45

Figure 14	Diagramme e de contexte statique	48
Figure 15	Diagramme de cas d’utilisation	48
Figure 16	Diagramme de séquence administrateur pour s’authentifier.	49
Figure 17	Diagramme de séquence administrateur pour gestion de patient	51
Figure 18	Diagramme de séquence pour Consultation du donné par le Patient.	52
Figure 19	Diagramme de séquence pour Gestion des Autorisations d'Accès	53
Figure 20	Diagramme de séquence pour Définition de Deux Personnes de Confiance pour les Cas d’Urgence	54

Figure 21	Diagramme de séquence pour Consultation des données autorisées par les patients.	56
Figure 22	Diagramme de classe	57
Figure 23	System environment architecture[	65
Figure 24	Logo Solidity	66
Figure 25	Logo Gana	68
Figure 26	Logo JavaScript.	68
Figure 27	Logo Visual Studio Code	69
Figure 28	Logo MetaMask.	70

Figure 29	Interface principale de l'application.	71
Figure 30	l’interface de patient pour la permission	72
Figure 31	Interface de Délégation des Clés en Cas d'Urgence	73
Figure 32	l’interface d'ajout d'un patient par l’admin	73
Figure 33	Interface montre une des smartContrat	

Liste des tableaux

Tableau N°	Titre du tableau	Page
Tableau 1	Aperçu des Types de Blockchains	17
Tableau 2	Domaines d'application	20
Tableau3	Applications de la blockchain dans le secteur de la santé	27

Liste des abréviations

Abréviation	Expression Complète
ABE	Attribute-Based Encryption
IPFS	L'InterPlanetary File System
POW	Proof of Work
POA	proof of Authority
POS	Proof of Stake
POET	Proof of Elapsed Tim
DPOS	Delegation Proof of stake
TDF	Trap Door fonction

Abréviation	Expression Complète
ABE	Attribute-Based Encryption
PTP	peer to peer

Table des matières

Contents

Introduction Générale 1

Chapitre 1 Concepts de base de la blockchain 4

1.1 Introduction 4

1.2 Les bases cryptographiques 4

1.2.1 Fonctions de hachage 4

1.2.2 Fonction de hachage cryptographique 4

1.2.3 Les structures de données basées sur les fonctions de hachage : 6

1.3 Signatures numériques 9

1.4 La décentralisation dans la blockchain 12

1.4.1 Définition de la décentralisation : 13

1.4.2 Le Consensus distribué : 15

1.4.3 Algorithme de consensus dans Bitcoin 15

1.5 Mécanismes de validation de blocs : 15

1.5.1 La preuve de travail (PoW) : 15

1.5.2 La preuve d'enjeu (Pos) : 16

1.5.3 Preuve d'enjeu délégué (Delegated Proof of Stake) : 16

1.5.4 preuve d'autorité (Proof of Authority) : 17

1.5.5 Preuve du temps écoulé (Proof of Elapsed Tim) : 17

1.6 Les types de blockchains 17

1.6.1 Les Blockchains privées : 18

1.6.2 Les Blockchains publiques : 18

1.6.3 Les Blockchains consortium 19

1.7 Domaines d'application 20

1.7.1 Applications dans le domaine des transports 21

1.7.2 Applications de la blockchain dans le domaine de la Banques 22

1.7.3 Applications de la blockchain dans le domaine de la cybersécurité 22

1.7.4 Applications de la blockchain dans le domaine de la Chaîne d'approvisionnement (Supply Chain) : 22

1.7.5 Applications de la blockchain dans le domaine de la Santé (Healthcare) ... 23

1.8 Les Contrats Intelligents ("Smart Contracts") 24

1.9 Conclusion 24

Chapitre 2 Application de la blockhain dans domaine médical 26
2.1 Introduction 26
2.2 Blockchain de soins de santé. 26
2.2.1 Etat actuel de la recherche scientifique sur l'impact de la technologie blockchain dans le secteur de la santé 26
2.2.2 Gestion des données médicales 29
2.2.3 Apports de la blockchain dans le domaine de la santé 29
2.2.4 Un Modèle de Blockchain pour les Soins de Santé 30
2.2.5 Avantages techniques d'une blockchain dans le domaine de la santé 32
2.2.6 Avantages de la blockchain en matière de soins de santé : 33
2.3 Sécurité des soins de santé 33
2.3.1 Les 4 critères fondamentaux de la sécurité de l'information 33
2.3.2 Sécurité et confidentialité des données à caractère médical : 34
2.3.3 Exigences de base pour le partage et la protection des données médicales 36
2.4 Conclusion 36
Chapitre 3 Conception de notre protocole de contrôle d'accès décentralisé 38
3.1 Introduction 38
3.2 Problématique traitée au cours de notre projet 39
3.3 Travaux antérieurs : 39
3.4 Notre contribution : 40
3.4.1 Partage de clé secrète de Shamir 40
3.4.2 Système de partage de secret de Shamir 43
3.5 Le Rôle de la Technologie Blockchain dans la Facilitation de l'Échange de Données Médicales" 44
3.6 Description générale de notre modèle de contrôle d'accès aux données des patients 44
3.7 Environnement système et architecture 45
3.8 Méthodes d'analyse et de conception 46
3.8.1 Les besoins attendus de protocole de contrôle d'accès 46
3.9 La description textuelle de deux scénarios d'utilisation de notre protocole 49
3.10 Diagramme de séquence 51
3.10.1 Diagramme de Séquence : Authentification 51
3.10.2 Diagramme de Séquence : Ajout d'un Patient par l'Administrateur 52
3.10.3 Diagramme de Séquence : Consultation de la donnée par le Patient 52
3.10.4 Diagramme de Séquence : Gestion des Autorisations d'Accès: 53

3.10.5 Diagramme de Séquence : Définition de Deux Personnes de Confiance pour les Cas d'Urgence via un Smart Contract 54
3.10.6 Diagramme de Séquence : Consultation des données autorisées par les patients 55
3.11 Diagramme de classe 57
3.12 Implémentation 57
3.12.1 Inscription d'un Utilisateur de Type Patient : 58
3.12.2 La procédure de chiffrement à l'aide de la clé publique de Bob suit les étapes suivantes 59
3.12.3 Inscription d'un utilisateur de type personnel médical : 59
3.12.4 Procédure d'autorisation d'accès en lecture et en écriture 59
3.12.5 Description du protocole de récupération de clé secrète : 61
3.13 Discussion de notre proposition de solution 62
3.13.1 Sécurité et protection de la vie privée : Notre protocole utilise un chiffrement extrêmement 62
3.14 Conclusion 63
Chapitre 4 Réalisation d'un prototype d'application 64
4.1 Introduction 64
4.2 Outils de développement 64
4.2.1 Généralités sur Ethereum 64
4.2.2 Solidity 65
4.2.3 Xampp 65
4.3 4.2.4 Ganache 66
4.3.1 JavaScript 66
4.3.2 Truffle 67
4.3.3 Node.js 67
4.3.4 Langage PHP 67
4.4 Environnement de développement 67
4.4.1 Visual Studio Code 67
4.4.2 MetaMask 68
4.5 Outil de gestion de la bibliographie 69
4.5.1 Zotero 69
4.6 Organigrammes de l'application 69
4.4.1 Interfaces d'authentification 69
4.6.1 L'interface de patient pour la permission 70
4.6.2 Interface de Délégation des Clés en Cas d'Urgence 70

4.6.3 Interface de Délégation des Clés en Cas d'Urgence 70
4.6.4 L'interface d'ajout d'un patient par l'administrateur 71
4.7 SmartContrast 73
4.8 Conclusion 73
Conclusion Générale 1
Bibliographie 3

Introduction Générale

La blockchain est une technologie décentralisée novatrice utilisée pour partager, répliquer et synchroniser des données à travers différentes localisations géographiques. Elle garantit des transactions fiables dans n'importe quel environnement peu fiable, sans nécessiter d'administrateur ou d'autorité centrale pour contrôler tous les aspects liés aux données. Un réseau blockchain repose sur un algorithme de consensus, approuvé par toutes les entités pour toute nouvelle transaction. La blockchain présente de nombreux avantages, tels que la sécurité, la confiance, l'open source, la traçabilité et la transparence, ce qui la rend très populaire pour son application dans divers secteurs.

La sécurité des données personnelles et médicales est un enjeu majeur dans notre société numérique. Ces informations sensibles sont souvent la cible de cyberattaques, exposant les individus à des risques économiques, sociaux et psychologiques. Le secteur de la santé, en particulier, est confronté à des défis uniques en matière de protection des données, car les violations de sécurité peuvent avoir des conséquences graves sur la vie des patients. Dans ce contexte, la blockchain émerge comme une technologie prometteuse pour renforcer la sécurité et la confidentialité des données personnelles et médicales.

Ces dernières années, un manque de mesures de sécurité adéquates a entraîné de nombreuses violations de données, exposant les patients à des menaces économiques, à d'éventuels stigmates sociaux et à des tourments psychologiques. Nous pouvons citer par exemple le piratage des données psychiatriques des patients de la clinique du nom de Vastaamo en Finlande.

Les données des patients constituent un atout précieux. Malgré les préoccupations en matière de confidentialité, 90 % des Américains, selon certains sondages, accordent de la valeur à l'accès en ligne à leurs dossiers de santé. Une grande partie des ressortissants des pays développés partage cet avis. Un grand défi pour que les systèmes de données de santé deviennent plus intelligents est de savoir comment rassembler, stocker et analyser les données personnelles de santé sans susciter de violations de la vie privée. Pour de tels

systèmes, les préoccupations en matière de confidentialité se sont avérées être des obstacles à l'adoption de systèmes de données de santé à grande échelle. En effet, à cause de la nature sensible et de grande valeur des données médicales, elles sont devenues l'une des cibles principales des pirates informatiques.

Ce mémoire de fin d'études de master se concentre sur l'étude de la blockchain, ses mécanismes et ses applications dans le domaine de la santé. Nous proposons une solution permettant une gestion décentralisée et sécurisée des données de santé. La blockchain offre la possibilité de partager sélectivement les informations médicales avec les professionnels de santé tout en conservant la propriété des données par le patient. De plus, elle peut introduire la transparence dans la gestion des litiges entre patients et médecins en offrant un stockage sécurisé et infalsifiable des données médicales. Nous détaillons la conception, la modélisation et la réalisation d'un protocole décentralisé de gestions des droits d'accès aux données médicales, basé sur la blockchain. Nous avons divisé notre rapport en quatre chapitres :

Lors du premier chapitre, nous présentons des concepts cryptographiques importants dans notre thème, tels que les fonctions de hachage cryptographiques, le chiffrement symétrique et asymétrique ainsi que la signature numérique. Nous explorons ensuite le mode de fonctionnement de la blockchain, sa structure et ses différents types.

Lors du second chapitre, nous abordons les différentes applications de la blockchain et montrons comment elle peut répondre à divers problèmes, en particulier dans le domaine de la santé.

Lors du troisième chapitre, nous décrivons comment appliquer la blockchain aux dossiers médicaux et présentons la modélisation de notre protocole.

Enfin, le cinquième chapitre est consacré à la réalisation et à l'implémentation de notre protocole de gestion d'accès décentralisé sur la blockchain. Nous y présentons les outils de développement adoptés, l'environnement de développement et les interfaces utilisateurs.

En conclusion, la blockchain présente des avantages potentiels significatifs dans le domaine de la santé, notamment en matière de sécurité, de transparence et de contrôle des données par les patients. Cependant, pour que cette technologie puisse être pleinement

exploitée dans ce secteur, il est essentiel de continuer à la développer et à surmonter les défis liés à son adoption à grande échelle.

Chapitre 1

Concepts de base de la blockchain

1.1 Introduction

Tout au long de ce chapitre, nous explorerons les fondements de la cryptographie essentiels à la compréhension de la blockchain. Nous plongerons en détail dans la signature digitale, les fonctions de hachage et les différentes structures de données qui en découlent. Par la suite, nous nous pencherons sur la blockchain elle-même : ses caractéristiques distinctives, son fonctionnement, ainsi que la décentralisation dans la blockchain et l'algorithme de consensus . Ce chapitre revêt une importance cruciale, offrant les connaissances de base nécessaires pour appréhender la technologie blockchain et ses mécanismes sous-jacents. Pour ceux qui souhaitent approfondir leur compréhension, nous fournirons également des références bibliographiques pertinentes.

1.2 Les bases cryptographiques

1.2.1 Fonctions de hachage

Les fonctions de hachage sont des outils mathématiques essentiels en cryptographie. Elles ont principalement trois propriétés : Elles prennent des données de taille variable en entrée et génèrent des empreintes numériques de taille fixe en sortie, agissant comme des signatures uniques pour les données d'origine. Ces empreintes garantissent une représentation compacte et sécurisée des informations, facilitant leur vérification et leur gestion. La troisième propriété des fonctions de hachage est qu'elles sont efficacement calculables.

1.2.2 Fonction de hachage cryptographique

Pour qu’une fonction de hachage soit considérée comme étant cryptographique, il y a des propriétés supplémentaires qu’elle doit posséder. Elle doit être :

- Résistante aux collisions
- Résistante à la préimage
- Et Puzzle-friendly , cette dernière propriété n'est pas obligatoire pour les fonctions de hachage cryptographiques, mais elle est utile pour la blockchain**[1].**

❖ La Résistance aux collisions

Une collision se produit lorsque deux entrées distinctes X et Y produisent la même empreinte.

$$X \neq Y \text{ mais } H(X) = H(Y)$$

La résistance aux collisions quant à elle, c'est le fait qu'il soit impossible de trouver deux entrées différentes qui ont la même empreinte. En pratique tout du moins. En théorie, si la taille de l'empreinte est fixe et que le nombre d'entrées n'est pas limité, il existe bien plus d'entrées qu'il n'existe d'empreintes disponibles. Cependant, les fonctions de hachages cryptographiques sont conçues de telle sorte qu'il est excessivement long de trouver une collision.

Considérez la méthode simple suivante pour rechercher une collision pour une fonction de hachage avec une taille de sortie de 256 bits : Nous aurons donc 2^{256} sorties possibles ou empreintes possibles pour notre fonction de hachage. Si l'on calcule l'empreinte de (2^{256} +1) valeurs, alors nous sommes sûrs de tomber sur une collision étant donné que nous avons calculé plus d'empreintes que de sorties possibles. Cependant, le problème avec cet algorithme, c'est qu'il prend énormément de temps et est en définitive infaisable. Par exemple, si l'on prend tous les ordinateurs ayant été construits par l'homme et qu'ils étaient en train de calculer des empreintes pour trouver des collisions depuis que l'univers existe, la probabilité qu'ils soient arrivés à en trouver une pour SHA256 (utilisée par Bitcoin) est moins importante que celle que le lecteur de ce document soit percuté par une météorite dans les deux prochaines secondes**[1].**

❖ Résistance à la préimage

La résistance aux pré-images est un concept crucial dans le domaine des fonctions de hachage. Il garantit la sécurité et l'intégrité des données en rendant impossible, sur le plan informatique, la détermination de l'entrée d'origine à partir de sa valeur de hachage. Cette propriété est vitale dans diverses applications

cryptographiques, garantissant la confidentialité et l'authenticité des informations**[2]**.

Cette propriété consiste à voir la fonction de hachage comme une fonction à sens unique, c'est-à-dire que nous pouvons facilement calculer l'empreinte d'une entrée mais que nous ne pouvons pas faire l'inverse et trouver l'entrée à partir d'une empreinte.

- **Puzzle-friendly**

La caractéristique de convivialité des puzzles des fonctions de hachage, également connue sous le nom de "puzzle-friendly", désigne la capacité d'une fonction de hachage à rendre difficile la recherche de l'entrée correspondante à une empreinte donnée. Cette caractéristique est essentielle car elle garantit qu'il n'y a pas de raccourci, de stratégie ou d'astuce pour trouver plus rapidement l'entrée correspondante. En d'autres termes, même si vous connaissez l'empreinte (ou le résultat) d'une fonction de hachage, il est difficile de trouver l'entrée d'origine sans passer par un processus de force brute, c'est-à-dire essayer toutes les combinaisons possibles jusqu'à ce que la bonne soit trouvée. Cela rend la tâche pratiquement impossible lorsque l'espace de recherche est suffisamment grand, assurant ainsi la sécurité de la fonction de hachage**[1].**

1.2.3 Les structures de données basées sur les fonctions de hachage :

Nous allons dans cette section présenter deux structures de données essentielles à la blockchain et qui sont basées sur les fonctions de hachage cryptographiques.

- **Les arbres de merkle**

Également appelés arbres de hachage, les arbres de Merkle sont un composant indispensable de la technologie blockchain, assurant la vérification sécurisée et efficace des données. Un arbre de Merkle est une structure de hachage utilisée en informatique et en cryptographie. Le hash de la racine résume toutes les données contenues individuellement dans chaque nœud de l'arbre. Les arbres de Merkle sont essentiels pour réduire les quantités de données qui doivent être conservées dans une blockchain à des fins de vérification. Dans le réseau Bitcoin, les arbres de Merkle sont utilisés pour la vérification des données. Cette méthode efficace consiste à utiliser des hachages au lieu d'un fichier

d'informations complet. Un arbre de Merkle est un arbre de valeurs hachées, comme illustré dans la **figure 2 c**i-dessous **[3].**

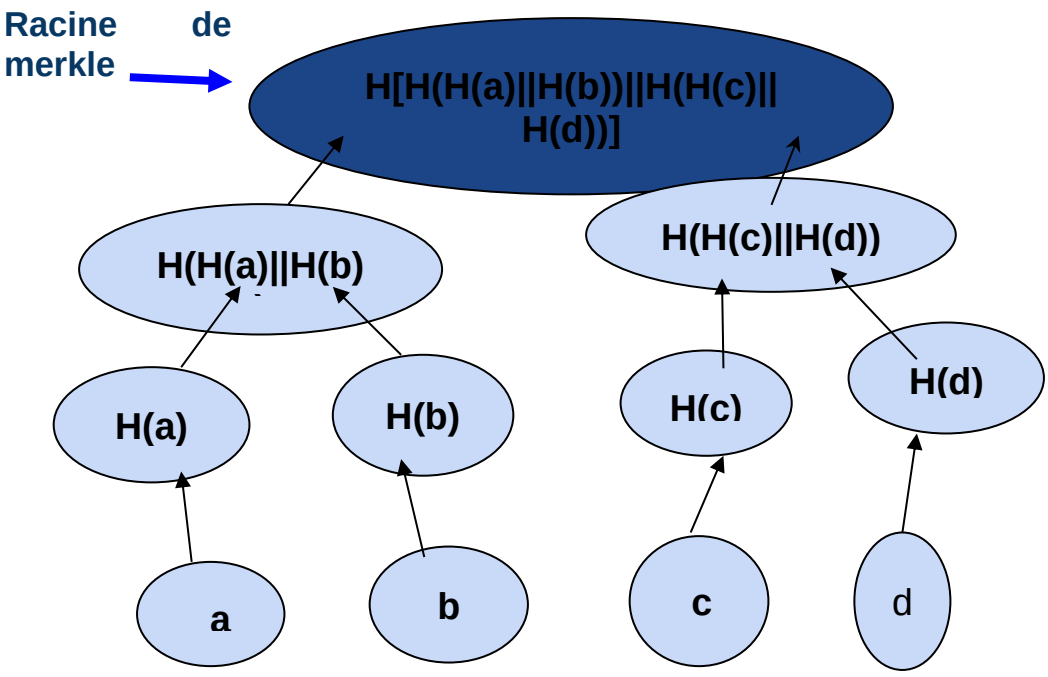

Figure 2 -Construction d'un arbre de Merkle [4].

❖ **La chaîne de blocs (BLOCKCHAIN)**

Une blockchain est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie [5].

La blockchain est une technologie de stockage et de transmission d'informations. Cette technologie possède en particulier trois caractéristiques majeures : elle est transparente, sécurisée, et fonctionne sans organe central de contrôle"[6].

Transparente : car chacun peut consulter l'ensemble des échanges inscrits sur une blockchain depuis sa création

Sans organe de contrôle : puisque la blockchain est fondée sur des relations de Pair-à-Pair [6].

Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne de blocs. La structure de cette dernière est exprimée dans la **figure 3 ci-**dessous :

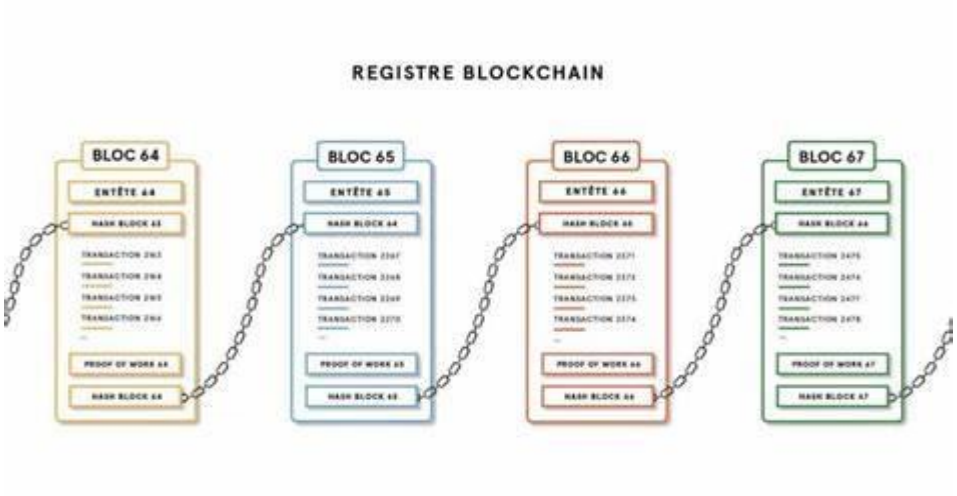

Figure 3 - Présentation d'une chaîne de blocs (blockchain)[7].

❖ Le fonctionnement de la blockchain

Pour fonctionner, la blockchain nécessite l'utilisation d'une monnaie ou d'un jeton (aussi appelé token) programmable. Vous pouvez par exemple utiliser le Bitcoin.

Dans une blockchain, l'ensemble des transactions est enregistré sous forme de blocs. Chacun des blocs doivent ensuite être validés par les nœuds du réseau (ordinateurs) qui utilisent une méthode de cryptographie algorithmique. Dès que le bloc est validé, il est ajouté à la chaîne de blocs et devient visible de tous les utilisateurs. Voir le schéma **(Figure 4)** ci-dessous qui illustre ce principe de fonctionnement [8**].**

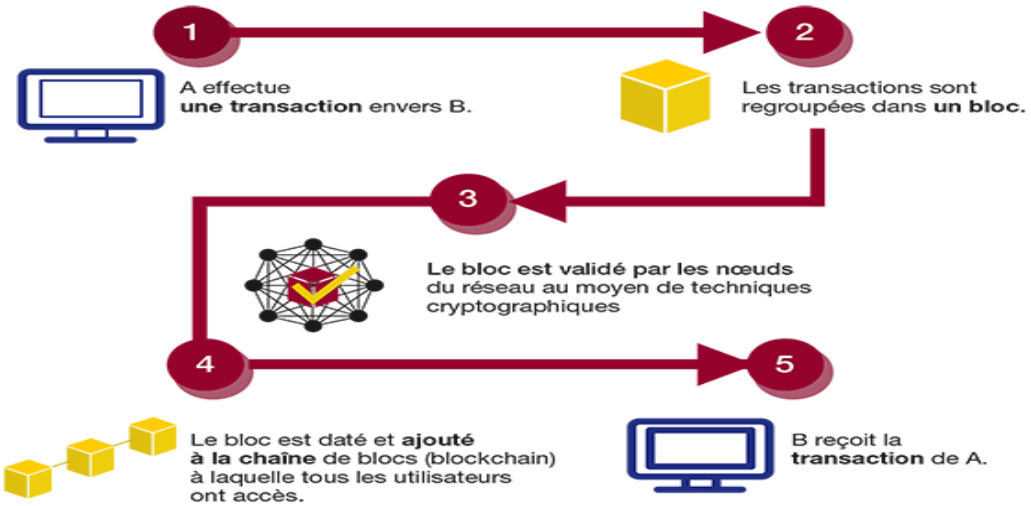

Figure 4 -Fonctionnement de la blockchain [9].

1. **L'utilisateur A réalisé une transaction vers l'utilisateur B**
2. **Les transactions sont enregistrées au sein d'un bloc**
3. **Le bloc est validé par les nœuds (serveurs) du réseau grâce à un algorithme cryptographique**
4. **Le bloc est horodaté et ajouté à la blockchain, il est accessible à tous ses utilisateurs**
5. **L'utilisateur B reçoit la transaction en provenance de l'utilisateur A [8].**

1.3 Signatures numériques

Une signature numérique est l'équivalent électronique d'une signature écrite ; elle peut être utilisée pour garantir que le signataire revendiqué a bien signé les informations. De plus, une signature numérique peut être utilisée pour détecter si les informations ont été modifiées après leur signature (c'est-à-dire pour détecter l'intégrité des données signées). Ces garanties peuvent être obtenues si les données ont été reçues lors d'une transmission ou récupérées depuis un stockage. Un algorithme de signature numérique correctement implémenté, répondant aux exigences de cette norme, peut fournir ces services. **La figure 5** représente une illustration d'un schéma de signature **[10].**

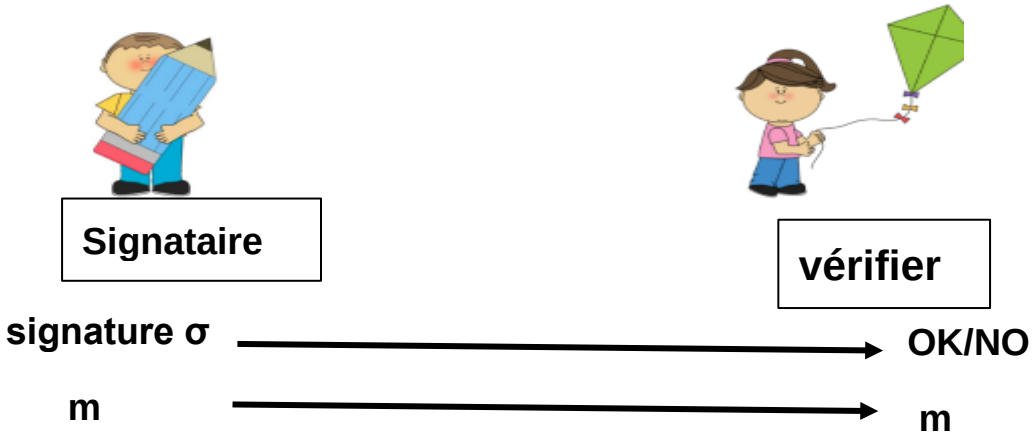

Figure5- Illustration d'une signature digitale.

Chiffrement symétrique (chiffrement à clé secrète) :

C'est une opération permettant de passer d'une information lisible et claire, à une information incompréhensible et cela dans le but de garantir la confidentialité dans le réseau. **La figure 6** ci-dessous illustre nos propos.

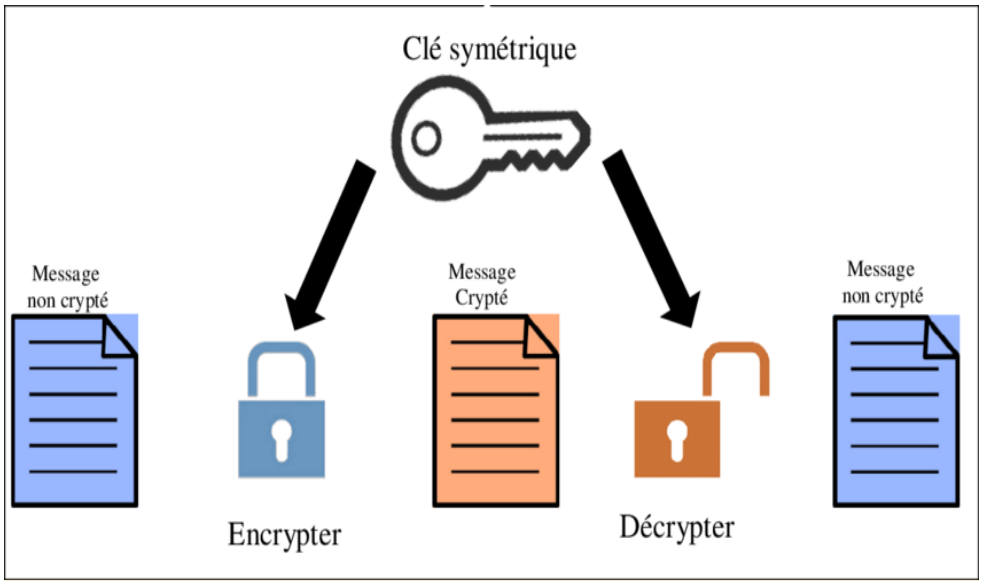

Figure 6-Le chiffrement symétrique

Vocabulaire de base :

Alice va se mettre d'accord avec Bob sur le crypto système qu'ils vont utiliser. L'information qu'Alice veut transmettre à Bob est le texte clair Le processus de transformation d'un message "m", à l'aide de la clé de chiffrement "k" pour qu'il devienne incompréhensible pour Rochelle est appelé chiffrement ou codage. Le

message ainsi généré est le message chiffré “C” ou « ciphertext » , qui a été obtenu grâce à la fonction de chiffrement E(encryptions). **C = E (k, m)**

Le processus de transformation du message chiffré en message clair est appelé déchiffrement ou décodage et utilise une fonction de déchiffrement, D (décryptions). On demande que pour tout message clair m :

D (k, C) = D (k, E (k, m)) = m (puisque E (k, m) = c)

Autrement dit, on demande que tout message codé provienne d’un et d’un seul message clair. Dans les systèmes de chiffrement symétriques, les clés de chiffrement K qui permettent de chiffrer et de déchiffrer les messages sont identiques. Au contraire de algorithmes asymétriques qui utilisent des clés de chiffrement et de déchiffrement différentes.

- **Exemple d’algorithmes de chiffrement symétrique :**

Aes (Advanced encryptions standard, en réalité c’est un standard, le vrai nom de l’algorithme est Randal), c’est l’algorithme de chiffrement symétrique le plus utilisé à l’heure actuelle. Il est possible de l’implémenter en utilisant trois tailles de clé différentes : 128, 192 ou 256 bits

Fonction à porte dérobée (trapdoor functions) :

- Ce sont des fonctions **X←Y** avec le triplet d'algorithmes suivant :

(G, F, $\boldsymbol{F^{-1}}$)

- G () : est un algorithme de génération de clés aléatoires ($\mathbf{P_K}$, $\boldsymbol{S_K}$).
- F ($\mathbf{P}$,.) est un algorithme déterministe qui définit une fonction X→Y
- F-1 ($\mathbf{P_K}$,.) définit une fonction inverse de F ($\mathbf{P_K}$”.,.) qui est définie sur Y→X

Nous avons : ∀ x ∈ X : $\boldsymbol{F^{-1}}$ ($\mathbf{S_K}$, F ($\mathbf{P_K}$, x)) = x

- **Quant est ce qu' une TDF est sûre ?**
  - Nous disons que (G, F, $\boldsymbol{F^{-1}}$) est sûre, si F ($\mathbf{P_K}$,.) est une fonction à sens

  Unique. Ce qui signifie qu'elle peut être facilement évaluée mais qu'il est infaisable de l’inverser sans posséder la clé secrète “$\mathbf{s_K}$”.
- Exemple de TDF :
  - **Le RSA** : rivest Shamir Adleman, est une fonction TDF encore très utilisée à travers le monde.

Le chiffrement asymétrique (chiffrement à clé publique) :

Cette méthode est basée sur l'utilisation d'une paire de clés pour chaque entité du réseau. Une clé publique qui peut être connue par toutes les entités et une clé privée qui n'est connue que par l'entité propriétaire. Les deux clés sont mathématiquement liées. Le chiffrement se fait en utilisant la clé publique du destinataire, et le déchiffrement est effectué par le récepteur en utilisant sa propre clé privée. Cette méthode garantit que seul le destinataire peut déchiffrer le message [11]**.**

Définition : un système de chiffrement asymétrique est un triplet de trois algorithmes :

1. G () : un générateur de paires de clé ($\mathbf{P_K}$, $\mathbf{S_K}$).

2.E($\mathbf{P_K}$,m) : un algorithme qui prend comme entrée m ∈ M et en sortie c ∈ C

3.D(SK, c) : un algorithme déterministe qui prend en entrée c ∈ C et fourni en sortie m ∈ M.

- Bien sûr, nous avons également : ∀ les output de G($\mathbf{P_K}$, $\mathbf{S_K}$): ∀ ∈ M D(sk, E($\mathbf{P_K}$,m)) = m

La majorité des algorithmes et schéma de chiffrement asymétrique utilisent des fonctions à porte dérobée ou trapdoor fonction (TDF). La section qui suit décrit ce genre de fonction.

- **Remarque :** Le RSA est une fonction à porte dérobée et pas un algorithme de chiffrement asymétrique, les algorithmes de chiffrement asymétriques utilisent des fonctions TDF lors de leur implémentation. Nous allons lors du chapitre 3, au cours de la section implémentation présenter une manière correcte et sûre d'utiliser une TDF afin d'implémenter un chiffrement asymétrique.

1.4 La décentralisation dans la blockchain

La décentralisation est un concept important qui n'est pas unique au Bitcoin. L'idée de compétition entre les paradigmes de centralisation et de décentralisation se manifeste dans une variété de technologies numériques différentes.

On parvient à la décentralisation dans la blockchain grâce à plusieurs mécanismes et principes fondamentaux. Tout d'abord, le concept de consensus distribué est essentiel :

Au lieu de reposer sur une autorité centrale pour valider les transactions, la blockchain utilise des algorithmes de consensus qui permettent à l'ensemble du réseau de parvenir à un accord sur l'état du système. Cela élimine le besoin d'une autorité centrale et répartit le pouvoir entre tous les participants du réseau.

Ensuite, la nature même de la technologie blockchain, qui est décentralisée par conception, contribue à sa décentralisation. Chaque nœud du réseau contient une copie de toutes les transactions, ce qui rend le réseau résilient aux pannes et aux attaques

De plus, l'ouverture et la transparence des transactions sur la blockchain favorisent la confiance et l'adoption généralisée, renforçant ainsi la décentralisation. Enfin, le développement de protocoles et de gouvernance décentralisés permet aux utilisateurs de participer activement à la prise de décision et à l'évolution du réseau, garantissant ainsi sa décentralisation à long terme.

1.4.1 Définition de la décentralisation :

Il n'y a pas de nœud central, et chaque nœud est égal. Les enregistrements de Les transactions sont effectués par plusieurs nœuds répartis dans différents endroits, et chaque nœud enregistre et conserve un compte complet. Tous les nœuds peuvent superviser la transaction et témoigner conjointement pour celle-ci.

- La décentralisation est essentielle au fonctionnement et à la sécurité du réseau Bitcoin. Elle signifie que le réseau fonctionne d’utilisateur à utilisateur.

- Une blockchain suit un réseau P2P. Il s'agit essentiellement d'un cadre de réseau multi-réseaux intégré entre pairs, composé de cryptographie, d'algorithmes et d'expressions mathématiques visant à résoudre les limitations classiques de la synchronisation de bases de données distribuées à l'aide d'algorithmes de consensus distribués.

- La figure 8 montre les différentes topologies de réseau ; centralisé, décentralisé et distribué (type réseau de la technologie de Blockchain

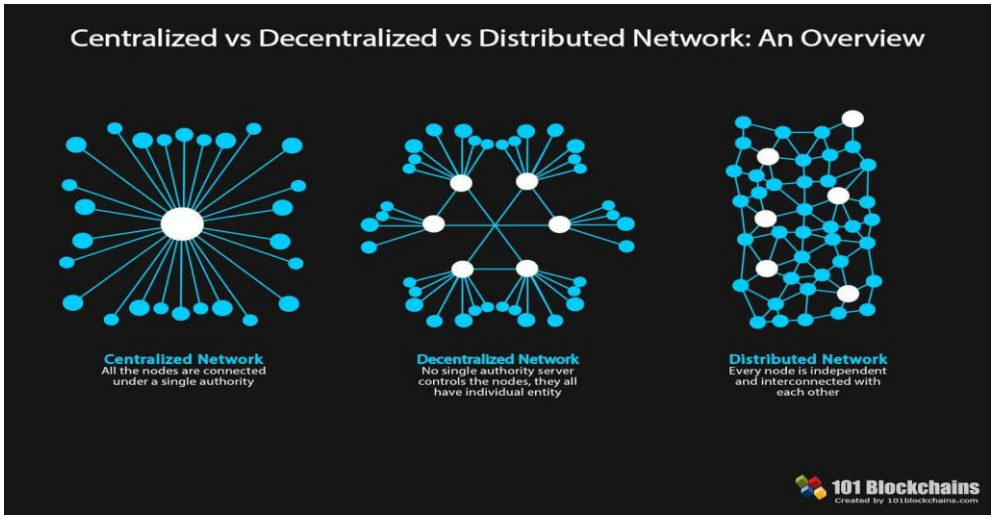

Figure8-De gauche à droite, réseaux centralisés, décentralisés et distribués (Blockchain)[12].

Le reseau Peer-to-peer (Le Peer-to-peer network):

La preuve de travail (proof-of- network) est un mécanisme utilisé dans les systèmes informatiques, notamment dans les cryptomonnaies comme le Bitcoin, pour parvenir à un consensus décentralisé. Les participants, appelés mineurs, doivent effectuer un travail complexe et coûteux en puissance de calcul pour prouver qu'ils ont accompli une tâche spécifique. Ce travail est vérifié par le réseau pour valider les transactions et protéger le système contre les attaques malveillantes[11]**.**

Le minage (le mining) :

Le minage, dans le contexte des cryptomonnaies et des blockchains, fait référence au processus de validation et de sécurisation des transactions sur un réseau décentralisé. Le minage est essentiel pour maintenir l'intégrité et la sécurité du réseau, en empêchant les fraudes et les attaques malveillantes tout en garantissant le consensus décentralisé.

- Bitcoin est décentralisé dans sa gestion des transactions principalement en raison de deux facteurs clés :

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

1.4.2 Le Consensus distribué :

La notion de consensus distribuée possède diverses applications et elle est étudiée depuis des décennies en informatique. L'application traditionnelle est la fiabilité dans les systèmes distribués. Imaginez que vous êtes responsable de l'infrastructure backend d'une grande entreprise de réseau social comme Facebook. Les systèmes de ce genre ont généralement des milliers, voire des millions de serveurs, qui forment ensemble une base de données distribuée massive enregistrant toutes les actions se déroulant dans le système. Chaque élément d'information doit être enregistré sur plusieurs nœuds différents de cette infrastructure backend, et les nœuds doivent être synchronisés quant à l'état global du système.

1.4.3 Algorithme de consensus dans Bitcoin

L'algorithme de consensus joue un rôle important dans le contexte de la Blockchain.

Le but est d'obtenir que tous les participants s'accordent sur un seul état de la Blockchain. Le mécanisme de consensus a les objectifs suivants :

- S'assurer d'avoir un bloc valide dans la chaîne de blocs.
- Parvenir À un accord ´équitable pour toutes les parties concernées
- Il faut s'assurer qu'il n'y aura pas d'adversaires puissants pour réussir à bifurquer la chaîne.
- Rendre le réseau plus solide face aux divers types d'attaques.

1.5 Mécanismes de validation de blocs :

Les mécanismes de consensus jouent un rôle crucial dans les plateformes blockchain. Sans eux, la blockchain se résumerait simplement à une base de données figée et dénuée d'intelligence. Dans cette optique, nous présentons quelques-uns des algorithmes de consensus les plus utilisés [11]:

1.5.1 La preuve de travail (PoW) :

Cet algorithme de consensus est utilisé par de nombreuses blockchains telles que le bitcoin, le lite coin et l'Ethereum. La preuve de travail est basée sur la fonction de minage pour l'ajout de nouveaux blocs à la blockchain. Chaque bloc contient une signature qui est

issue de l'exécution d'une fonction de hachage sur ce bloc. Ce dernier ne peut être ajouté à la blockchain si sa signature ne commence pas par certains caractères prédéfinis, pour cela les mineurs doivent changer plusieurs fois une chaîne de caractère inclus dans le bloc dit « le nonce » jusqu'à l'obtention d'une signature répondant au critère prédéfini (la suite de caractère nécessaire). Le mineur ayant résolu le problème reçoit une récompense et des frais de transaction [13].

1.5.2 La preuve d'enjeu (Pos) :

Contrairement à la preuve de travail, la preuve d'enjeu consomme moins d'énergie de calcul. Les différents nœuds du réseau appelés « minters » déposent une partie de leurs cryptomonnaies pour pouvoir ajouter un nouveau bloc à la blockchain et l'algorithme sélectionne aléatoirement un minter parmi les minters pour créer le bloc durant un intervalle de temps limité.

La figure 9 illustre la consommation de l'énergie électrique par les deux blockchains : Bitcoin et Ethereum. On remarque sur les deux diagrammes que la blockchain Bitcoin utilisant Pow est largement plus gourmande en énergie que la blockchain Ethereum utilisant Pos.

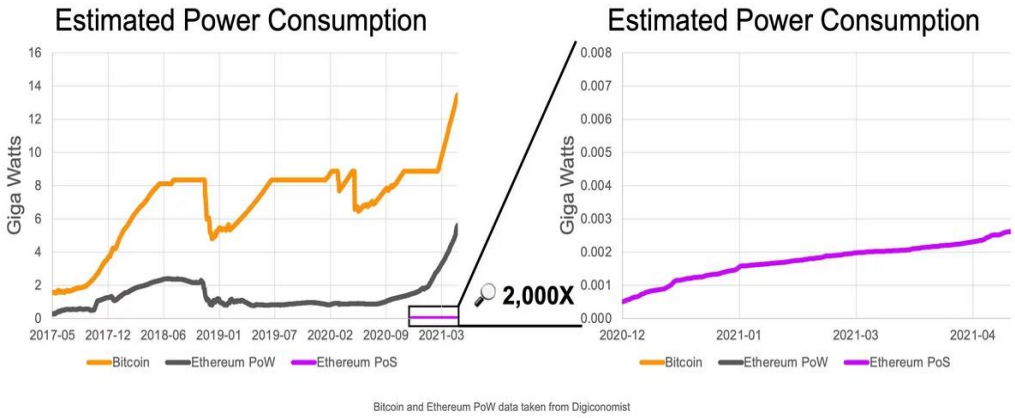

Figure 9- Consommation de l'énergie électrique par les blockchains Bitcoin et Ethereum[13].

1.5.3 Preuve d'enjeu délégué (Delegated Proof of Stake) :

Utilise des délégués d'actionnaires pour valider la blockchain et résoudre les problèmes de consensus dans un modèle conçu de manière démocratique. Dans le DPoS, n'importe quel actionnaire, même ceux possédant la plus petite quantité de jetons, peut voter dans un processus électoral qui choisit les producteurs de blocs pour le réseau.

1.5.4 preuve d'autorité (Proof of Authority) :

Le modèle de consensus de preuve d'autorité (également appelé preuve d'identité) repose sur la confiance partielle accordée aux nœuds de publication grâce à leur lien connu avec des identités du monde réel. Les nœuds de publication doivent avoir leurs identités prouvées et vérifiables au sein du réseau de la blockchain (par exemple, des documents d'identification qui ont été vérifiés, notariés et inclus sur la blockchain) [14].

1.5.5 Preuve du temps écoulé (Proof of Elapsed Tim) :

Dans le modèle de consensus de preuve de temps écoulé (Poet), chaque nœud de publication demande un temps d'attente à une source de temps matériel sécurisée à l'intérieur de son système informatique. La source de temps matérielle sécurisée générera un temps d'attente aléatoire et le renverra au logiciel du nœud de publication. Les nœuds de publication prennent le temps aléatoire qui leur est donné et deviennent inactifs pendant cette durée. Une fois qu'un nœud de publication se réveille de l'état inactif, il crée et publie un bloc sur le réseau de la blockchain, alertant les autres nœuds du nouveau bloc ; tout nœud de publication qui est toujours inactif arrêtera d'attendre, et tout le processus recommence [14].

1.6 Les types de blockchains

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

Comme illustré dans **le Tableau 1** il existe principalement trois types de blockchains : publiques (non permissionnaires), consortium (publiques permissionnaires) et privées. Ils présentent des caractéristiques différentes concernant qui peut accéder, écrire et lire les données sur la blockchain.

Table 1 Aperçu des Types de Blockchains [15] :

Propriété	**Blockchain publique**	**Blockchain de consortium**	**Blockchain privée**

Détermination par consensus	Tous les mineurs	Ensemble sélectionné de nœuds	Une organisation
Permission de lecture	Public	Public ou restreint	Public ou restreint
Immutabilité	Quasiment impossible	Pourrait être falsifié	Pourrait être falsifié
Efficacité	Basse	Élevée	Élevée
Centralisé	Non	Partiel	Oui
Processus de consensus	Non permissions	Permissionné	Permissionné

1.6.1 **Les Blockchains privées :**

Les blockchains privées nécessitent à la fois une permission pour lire les données stockées et une permission pour y écrire. Elles se développent très rapidement, car leur gouvernance est aisée et la confidentialité des données y est relativement garantie, puisqu'un nombre limité d'acteurs peuvent y accéder. Ce nombre limité d'acteurs permet également de déterminer facilement les responsabilités en cas de problème. Ce sont typiquement les blockchains correspondant à un usage spécifique, comme la blockchain Ever Ledger[16]**.**

1.6.2 **Les Blockchains publiques :**

Les blockchains publiques sont accessibles à tous, ce qui soulève des questions de gouvernance et de responsabilité. Elles représentent les premières itérations de blockchains

de crypto-monnaies, telles que Bitcoin et Ethereum. La confidentialité de leurs données est assurée par l'utilisation de pseudonymes. Cependant, toutes les transactions associées à un pseudonyme demeurent visibles par tous et peuvent être explorées à l'aide d'outils de recherche, tels que blockchain.info [15]**. La table 1.2** ci-dessous donne une description des caractéristiques des blockchains selon leurs types.

Table1.2 - ci-dessous résume certaines des différences majeures[15]**.**

	Type de Blockchain		
	Publique	**Privée**	**À consortium**
Sans permission ?	Oui	Non	Non
Qui peut la consulter	Tout le monde	Seulement les utilisateurs invités	Cela varie
Qui peut y écrire ?	Tout le monde	Des participants approuvés	Des participants approuvés
Propriété	Personne	Entité unique	Plusieurs entités
Participants connus	Non	Oui	Oui
Vitesse de transaction	Lente	Rapide	Rapide

1.6.3 Les Blockchains consortium

La blockchain à consortium se situe sur la limite entre chaînes publiques et privées, combinant des éléments des deux côtés. La différence la plus notable par rapport à chaque système peut être observée au niveau du consensus. 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[17]**.**

1.7 Domaines d'application

La blockchain a joué un rôle essentiel en offrant une alternative rentable et efficace aux paiements en espèces, ainsi qu'en permettant le bon fonctionnement du système de paiement. Elle trouve également des applications dans divers domaines tels que l'identité numérique, le commerce électronique, les assurances, la gestion des biens, les paiements électroniques et le crowdfunding. La blockchain facilite le flux de données et permet de vérifier chaque transaction sur un réseau, rendant possibles des actions impossibles dans les institutions financières conventionnelles en quelques secondes seulement.

Ce point se concentre principalement sur les applications blockchain émergentes pour les systèmes cyber-physiques, à savoir les dossiers médicaux, les transports, le commerce électronique, la finance et la cybersécurité[18]**.** Le **tableau 1.2** énumère les différents systèmes couverts par l'étude, ainsi que leurs domaines d'application respectifs.

Tableau 1 Domaines d'application [18].

Systèmes	**Applications**	**Avantages**
Transport	Electronique automobile, systèmes ferroviaires, réseaux routiers, aviation et gestion de l'espace aérien.	• Facilitation de la gestion complexe de la conformité des flux et des équipements • Simplification des procédures de paiement • Traçabilité des flux • Logistique inverse
E-commerce	Surveillance et suivi de la chaîne d'approvisionnement pour garantir l'ouverture du marché, Refonte du système de paiement, Plateforme de commerce électronique sécurisée, Témoignages de produits pour la vraie vie.	• Méthodes de paiement alternatives • Meilleur traitement des commandes • Sécurité renforcée des paiements • Des transactions plus rapides

Soins de santé	Électronique automobile, systèmes ferroviaires, réseaux routiers, aviation et gestion de l'espace aérien.	• Gestion des données médicales • Optimisation des essais cliniques • Traçabilité des médicaments et lutte contre la contrefaçon
Finances	Prévention de la fraude, Inclusion financière, Prévention du blanchiment d'argent, Trade Finance, Smart Assets et Smart Contracts.	• Uberisation des services bancaires • Facilitation des transferts de fonds • Des transactions plus sûres et plus efficaces
Cybersécurité	Infrastructure de signature sans clé, anonymat des utilisateurs, validation des transactions dans les systèmes cyber-physiques, authentification des données.	• Sécurité permanente des données • La décentralisation sur une blockchain pourrait remplacer les autorités de certification • Authentification avancée

1.7.1 **Applications dans le domaine des transports**

Le suivi et la traçabilité des données sont essentiels pour assurer la transparence et la gestion efficace des chaînes d'approvisionnement. Les données de suivi permettent de connaître en temps réel la localisation et l'historique des produits. Ces données peuvent être regroupées en trois catégories : les données de réglage, les conditions de transport et les transactions commerciales. La collecte, le nettoyage et l'archivage de ces données permettent de prendre des décisions tactiques et stratégiques informées[18].

1.7.2 Applications de la blockchain dans le domaine de la Banques

Certains prévoient que la blockchain pourrait potentiellement mettre fin aux banques traditionnelles en éliminant le besoin d'un tiers de confiance. Des services financiers pourraient être automatisés où fonctionner sur une blockchain, remettant en question le rôle des banques dans la société et l'économie. La nature décentralisée de la blockchain permet à quiconque, moyennant un capital confiance, de créer des services bancaires basés sur le bitcoin. Les coûts d'intermédiation faibles des services basés sur le bitcoin pourraient également contribuer à l'ubérisation des banques. Cependant, en raison des barrières réglementaires, le développement du bitcoin pourrait se concentrer dans des pays où la monnaie est instable. De plus, des tendances telles que les crises financières et les scandales ont alimenté une certaine hostilité idéologique envers les institutions financières traditionnelles, notamment parmi la communauté de la blockchain **[6].**

1.7.3 Applications de la blockchain dans le domaine de la cybersécurité

Une tendance relativement nouvelle en matière de cybersécurité est le développement de mécanismes et de systèmes de protection basés sur la technologie blockchain.

La blockchain garantit l'intégrité des transactions en l'absence d'un hub central fiable. Les actifs corporels et incorporels des utilisateurs du système font l'objet de transactions spécifiées comme des activités spécifiques prises dans une liste prédéterminée. Les blocs contenant les informations relatives aux transactions sont reliés entre eux par hachage pour constituer une chaîne. Pour qu'il soit plus difficile pour un attaquant de miner la blockchain, une méthode spécifique connue sous le nom d'algorithme de consensus est employée pour distribuer des copies identiques des blocs à tous les membres du système[18]**.**

1.7.4 Applications de la blockchain dans le domaine de la Chaîne d'approvisionnement (Supply Chain) :

Les blockchains permettent la traçabilité et la transparence dans la chaîne d'approvisionnement, en enregistrant chaque étape de la production, de la distribution et de la vente des produits. Cela peut aider à lutter contre la contrefaçon, à améliorer la gestion des stocks et à assurer la qualité des produits.

1.7.5 Applications de la blockchain dans le domaine de la Santé (Healthcare)

Les établissements de santé doivent faire face à des problèmes de sécurité et de confidentialité lorsqu'ils partagent des données sur plusieurs plates-formes. L'amélioration de la collaboration de données entre fournisseurs signifie l'amélioration de nombreux aspects du domaine de la santé, tels que la précision des diagnostics et l'efficacité des traitements. La blockchain peut créer cet environnement sécurisé pour permettre aux établissements de santé, aux payeurs et aux autres acteurs de ce domaine de partager l'accès à leur réseau avec des garanties d'intégrité des données [12].

Grâce à son mécanisme de stabilisation et de sauvegarde de l'ensemble des données avec lesquelles les utilisateurs peuvent interagir par le biais de divers types de transactions, la technologie blockchain offre d'énormes possibilités pour les applications biomédicales, génomiques, de télémédecine, de télésurveillance, de santé en ligne, de neurosciences et de soins de santé personnalisés en général **(voir la figure 10).**

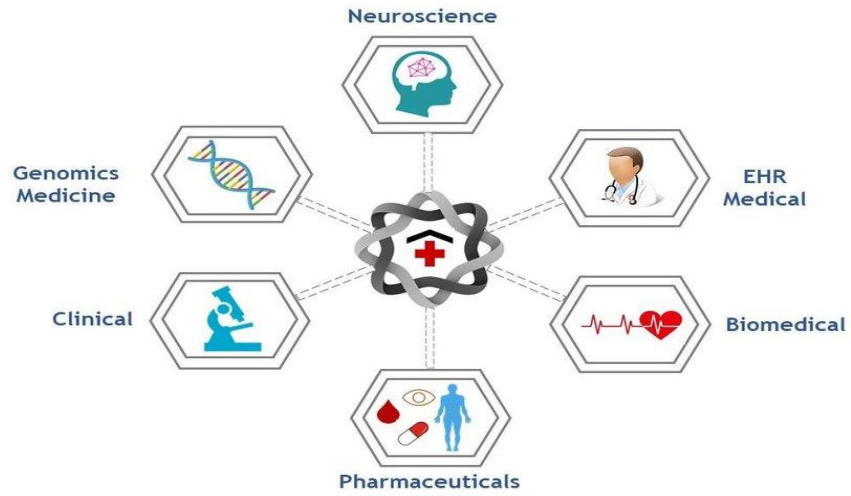

Figure 10 - Blockchain dans le secteur de la santé [19].

Les blockchains peuvent être utilisées pour sécuriser et partager les données médicales entre les fournisseurs de soins de santé, tout en préservant la confidentialité des patients. Elles peuvent également être utilisées pour suivre les données des patients, gérer les dossiers médicaux électroniques de manière sécurisée et garantir l'authenticité des médicaments. Nous allons dans le chapitre suivant aborder en détail les applications de la blockchain dans le domaine médical.

1.8 Les Contrats Intelligents ("Smart Contracts")

Les contrats intelligents font référence à une série de codes informatiques et de protocoles qui peuvent appliquer automatiquement un accord lorsque les conditions spécifiées sont remplies. Le contrat peut être présenté soit sous forme de code autonome, soit sous forme d'accord écrit traditionnel entre les parties dans le but de mettre en œuvre des dispositions spécifiques, telles que le transfert de frais. Les contrats intelligents aident à réduire les frais de transaction en éliminant le besoin de tiers de confiance par rapport aux contrats traditionnels. [20] a été le premier à introduire les contrats intelligents en 1997 en tant qu'ensemble de promesses, spécifiées sous forme numérique, comprenant des protocoles selon lesquels les parties exécutent ces promesses [21]**.**

Fonctionnant sur le principe des instructions conditionnelles "if-then", les contrats intelligents offrent trois avantages principaux : une vitesse accrue, une meilleure efficacité, et la certitude de l'exécution conforme aux termes convenus. Ils sont capables de surmonter les problèmes d'aléa moral et de réduire les coûts associés à la vérification, l'exécution, l'arbitrage et la fraude**[6].**

1.9 Conclusion

Dans ce chapitre, nous avons étudié le mécanisme et le concept sur lequel repose la blockchain, qui est une nouvelle technologie révolutionnaire qui a captivé l'attention des chercheurs et des innovateurs dans le monde de la technologie. Cette innovation informatique permet ainsi d'organiser les échanges de données sur un réseau distribué, assurant une sécurisation des données par chiffrement, et faisant participer les nœuds du réseau pour la création de nouveaux blocs de la chaîne.

La recherche sur l'utilisation de la blockchain dans le domaine de la santé est désormais établie en tant que domaine académique, et le nombre et la qualité des publications augmentent rapidement. Cette tendance est également perceptible dans le secteur industriel mondial de la santé, où le marché de la technologie blockchain devrait dépasser les 500 millions de dollars d'ici 2022. En raison de l'importance primordiale de maintenir la confiance tout en satisfaisant une demande croissante d'échange de données au sein de l'écosystème de la santé, les institutions de santé ont un besoin critique de nouvelles solutions préservant la confiance et améliorées.

Le prochain chapitre se concentrera sur l'examen plus approfondi des applications spécifiques de la technologie blockchain dans le domaine de la santé. Il pourrait explorer des cas d'utilisation plus détaillés, examiner les défis et les opportunités associés à l'adoption de la blockchain dans le secteur de la santé, et proposer des recommandations pour la mise en œuvre réussie de solutions basées sur la blockchain dans divers contextes de soins de santé.

Chapitre 2
Application de la blockhain dans domaine médical

2.1 Introduction

Au cours du chapitre précédent, nous avons examiné en détail les principes fondamentaux de la blockchain ainsi que les bases cryptographiques nécessaires à sa compréhension. En tant que technologie polyvalente, la blockchain trouve des applications potentielles dans divers secteurs tels que la finance, l'assurance, l'immobilier, la santé, entre autres. Dans ce chapitre, nous nous concentrerons spécifiquement sur les applications de la blockchain dans le domaine de la santé. Nous débuterons par une revue de la recherche scientifique actuelle dans ce domaine, afin de comprendre les avancées et les tendances émergentes. Ensuite, nous dresserons un tableau synthétique des différentes applications possibles de la blockchain dans le secteur de la santé, mettant en lumière ses implications et ses avantages potentiels.

2.2 Blockchain de soins de santé.

2.2.1 Etat actuel de la recherche scientifique sur l'impact de la technologie blockchain dans le secteur de la santé

La technologie blockchain, grâce à son mécanisme de stabilisation et de sauvegarde des données, ouvre de vastes perspectives dans divers domaines médicaux tels que la biomédecine, la génomique, la télémédecine, la télésurveillance, la santé en ligne, les neurosciences et les soins de santé personnalisés.

Il est largement reconnu que le domaine de la santé est l'un des secteurs qui devrait être le plus influencé par l'adoption de la technologie blockchain, comme le soulignent de nombreux experts. Plusieurs études ont été menées et publiées sur ce sujet, témoignant de l'intérêt croissant pour cette technologie dans le domaine de la santé. Cependant, en raison de la diversité des aspects de la santé, il est difficile de prédire quel sous-domaine bénéficiera le plus de l'utilisation de la blockchain.

Le tableau 3 présente les différentes applications de la blockchain dans le domaine des soins de santé. **Tableau 3- Applications de la blockchain dans le secteur de la santé**[18]**.**

Domaine d'application	**Applications**	**Contribution**
MI Store	Partage des informations sur les soins de santé à des fins administratives ou économiques	Développer un système de stockage des données d'assurance médicale basé sur la blockchain.
Med Rec	Dossier Médical Électronique	Donnez aux patients l'accès à tous leurs dossiers médicaux, rendez les soins vérifiables et partager leurs données.
Med lock	Informations sur les soins de santé qui sont partagées à des fins de recherche et de thérapie	Il est difficile pour les professionnels de la pharmacie de mettre au point des remèdes précis à partir de données recueillies selon des règles différentes, car les systèmes de DME actuels ne disposent pas d'une stratégie standard de gestion et de partage des données. Prenez des mesures dès maintenant pour résoudre ce problème
Analytique Methods in de soins de santé	Collecte, stockage et partage des données de santé	L'analytique dans les soins de santé à l'aide de la blockchain et de l'intelligence artificielle (IA).
Blockchain and Internet of	Intégration de grandes	La validation des transactions

Things (IoT) powered	quantités de données dans le processus d'exploitation minière	nécessite un mécanisme de consensus, ce qui réduit le coût de calcul des blocs miniers
Med Share	Modèle de stockage partagé en nuage pour les données	Réduire le délai de traitement et d'anonymisation des données en réduisant la latence.
Block Hie	Interopérabilité des données personnelles de santé et des dossiers médicaux électroniques	Stockage et vérification de la confidentialité et de la sécurité hors chaîne et sur chaîne
GAA-FQ	Contrôle d'accès granulaire aux dossiers médicaux électroniques (DME)	Autoriser des niveaux de granularité d'autorisation variés tout en gardant la structure de données de la blockchain sous-jacente compatible.

La technologie blockchain est prometteuse dans le secteur de la santé, notamment dans la numérisation des dossiers médicaux électroniques (EHR). Elle peut être utilisée pour garantir l'authenticité, la confidentialité et l'accès aux données médicales, ainsi que pour faciliter le partage sécurisé des informations entre les parties concernées. Nous pouvons citer le prototype "Med Rec"[22] qui utilise les avantages spécifiques de la blockchain pour gérer les EHR de manière décentralisée, offrant ainsi aux patients un accès complet et immuable à leurs informations de santé. Med Share [23] est un autre exemple qui se présente comme une solution sécurisée pour le partage de données médicales entre des parties non fiables, offrant un contrôle d'audit personnalisé et un minimum de risques pour la confidentialité et la sécurité des données.

2.2.2 Gestion des données médicales

De nos jours, il est difficile de visualiser de manière claire toutes les données liées à un patient et accumulées au cours de son parcours de soins. Ces informations proviennent habituellement de sources très variées, comme les médecins de ville, l'hôpital, les assurances, les pharmaciens ou les laboratoires d'analyses médicales. Les logiciels utilisés par ces parties prenantes pour collecter et gérer les dossiers médicaux sont différents et ne sont pas interopérables. Ainsi, il est parfois difficile de partager les informations. Par ailleurs, même si ces informations peuvent toutes être récupérées et assemblées, il n'est pas toujours évident de savoir dans quel ordre elles ont été produites et si elles sont exhaustives. Ce problème est fréquemment rencontré lors de l'admission d'un patient à l'hôpital. Les professionnels de santé n'ont en effet pas toujours accès à son historique et n'ont pas une visibilité complète sur les traitements qu'il prend, sur l'historique de sa maladie ou sur ses antécédents familiaux. L'idéal serait donc d'avoir une liste qui répertorie tous les lieux où se trouvent les données médicales d'un même patient afin de pouvoir rapidement les récupérer. Cette liste serait accessible, avec l'accord du patient, à tout professionnel de santé qui en ferait la demande. Ainsi, plutôt que de n'avoir accès qu'à la base de données de l'établissement où l'on se trouve, on pourrait avoir accès à toutes les sources d'informations dispersées dans toutes les bases de données du réseau. La technologie blockchain apporte justement cette solution sous la forme d'un registre distribué et sécurisé qui permet au patient non seulement d'avoir une visibilité sur ses données, mais aussi d'en contrôler les accès et d'en être le propriétaire[19].

2.2.3 Apports de la blockchain dans le domaine de la santé

Aujourd'hui, les besoins dans le secteur de la santé sont de disposer d'infrastructures de qualité soutenues par des technologies avancées et nouvelles. Dans ce contexte, la blockchain jouerait un rôle crucial dans la transformation de ce secteur. De plus, le paysage du système de santé évolue vers une approche centrée sur le patient, en se concentrant sur deux aspects principaux : des services accessibles et des ressources de soins de santé appropriées en tout temps. La blockchain renforce les organisations de santé pour fournir des soins adéquats aux patients et des installations de santé de haute qualité. L'échange d'informations médicales est un autre processus long et répétitif qui entraîne des coûts élevés pour l'industrie de la santé, ce problème peut être résolu grâce à cette technologie.

2.2.4 Un Modèle de Blockchain pour les Soins de Santé

Toute blockchain destinée aux soins de santé devrait être publique et devrait également inclure des solutions technologiques pour trois éléments clés : **la scalabilité**, **la sécurité d'accès et la confidentialité des données.**

- **Sécurité d'accès et confidentialité des données**

L'utilisateur aurait un accès total à ses données et un contrôle sur la manière dont ses données seraient partagées. L'utilisateur attribuerait un ensemble d'autorisations d'accès et désignerait qui peut interroger et écrire des données dans son Dossier médical. Une application de tableau de bord mobile permettrait à l'utilisateur de voir qui a la permission d'accéder à son dossier médical. L'utilisateur serait également capable de consulter un journal d'audit de qui a accédé à sa blockchain, y compris quand et quelles données ont été consultées. Le même tableau de bord permettrait à l'utilisateur de donner et de révoquer les autorisations d'accès à toute personne ayant un identifiant unique.

Les autorisations de contrôle d'accès seraient flexibles et créeraient plus que des autorisations "tout ou rien". L'utilisateur mettrait en place des transactions spécifiques et détaillées concernant qui a accès, la période allouée pour l'accès et les types particuliers de données pouvant être consultés. À tout moment, l'utilisateur pourrait modifier l'ensemble des autorisations. Les politiques de contrôle d'accès seraient également stockées de manière sécurisée sur une blockchain et seul l'utilisateur serait autorisé à les modifier. Cela fournit un environnement de transparence et permet à l'utilisateur de prendre toutes les décisions concernant les données collectées et la manière dont les données peuvent être partagées.

Après qu'un prestataire de soins de santé ait obtenu l'accès aux informations de santé d'un utilisateur, il interroge la blockchain pour les données de l'utilisateur et utilise la signature numérique pour authentifier les données. Le prestataire de soins de santé pourrait utiliser une application personnalisée de premier ordre pour analyser les données de santé.

L'authentification de l'identité suivrait les meilleures pratiques établies par les institutions financières et les régulateurs. Idéalement, les systèmes d'identification biométrique seraient utilisés car ils offrent une sécurité accrue par rapport aux méthodes d'authentification par mot de passe et par jeton (carte à puce).

Avec ce modèle, l'utilisateur a un contrôle absolu sur ses données et le pouvoir d'accorder l'accès à des prestataires de soins de santé spécifiques et/ou à des entités de soins de santé pour la communication et la collaboration dans le traitement et la prévention des maladies. La nature décentralisée de la blockchain combinée aux transactions signées numériquement garantissent qu'un adversaire ne peut pas se faire passer pour l'utilisateur ou corrompre le réseau, car cela impliquerait que l'adversaire ait falsifié une signature numérique ou pris le contrôle de la majorité des ressources du réseau. De même, un adversaire ne pourrait rien apprendre du registre public partagé car seuls des pointeurs hachés et des informations chiffrées seraient contenues dans les transactions[24]**.**

❖ La scalabilité

La scalabilité est la capacité d'un système à maintenir ses performances et sa fonctionnalité tout en gérant une croissance continue du nombre d'utilisateurs, de données ou de transactions, sans compromettre la qualité du service

La scalabilité d'une blockchain distribuée contenant des dossiers médicaux, des documents ou des images présente des défis en termes de stockage et de débit de données. Si cette blockchain est modélisée sur celle du Bitcoin, chaque membre du réseau aurait une copie de chaque dossier médical de chaque individu, ce qui serait peu pratique en termes de stockage des données. La duplication de tous les dossiers médicaux pour chaque membre du réseau consommerait beaucoup de bande passante, gaspillerait des ressources réseau et poserait des problèmes de débit de données. Pour que la blockchain puisse être utile dans le domaine des soins de santé, elle devrait agir comme un gestionnaire de contrôle d'accès pour les dossiers médicaux et les données. Les informations contenues dans plusieurs propositions de blockchain de santé seraient un index, une liste de tous les dossiers médicaux et données de santé de l'utilisateur, similaire à un catalogue de bibliothèques. Les transactions dans les blocs contiendraient l'identifiant unique de l'utilisateur, un lien chiffré vers le dossier médical et un horodatage pour la transaction, facilitant ainsi l'accès aux données. Toutes les données médicales seraient stockées hors blockchain dans un référentiel de données appelé **"data Lake"** (Un data Lake est un emplacement de stockage centralisé qui contient des big data sous un format brut et granulaire provenant d'un grand nombre de sources voir la **figure 11**)[25]**,** offrant une grande scalabilité et prenant en charge une variété d'analyses. Les informations stockées dans le data Lake seraient chiffrées et signées

numériquement pour garantir la confidentialité et l'authenticité. Lorsqu'un prestataire de soins de santé crée un dossier médical, une signature numérique est créée pour vérifier l'authenticité du document ou de l'image. Les données de santé sont ensuite chiffrées et envoyées au data Lake pour stockage. Chaque fois que des informations sont sauvegardées dans le data Lake, un pointeur vers le dossier de santé est enregistré dans la blockchain avec l'identifiant unique de l'utilisateur. Le patient est alors informé que des données de santé ont été ajoutées à sa blockchain. De même, un patient pourrait ajouter des données de santé avec des signatures numériques et un chiffrement à partir d'applications mobiles ou de capteurs portables [26]**.**

Figure 11- Blockchain dans le secteur de la santé[26]**.**

2.2.5 Avantages techniques d'une blockchain dans le domaine de la santé

La technologie blockchain présente de nombreux avantages pour l'informatique de santé. Reposant sur des logiciels open-source, des matériels grand public et des API ouvertes, elle favorise une interopérabilité plus rapide entre les systèmes et peut gérer efficacement de gros volumes de données et d'utilisateurs. La blockchain offre une tolérance aux pannes et une récupération après sinistre intégrées, tandis que les technologies de chiffrement sont reconnues comme des normes de l'industrie. Elle permettrait également aux patients, aux prestataires de soins de santé et aux chercheurs d'accéder à une source de données partagée pour obtenir des données de santé opportunes, précises et complètes. Les structures de données blockchain combinée aux "data laks" peuvent prendre en charge une grande variété de sources de données de santé, tandis que les architectures distribuées basées sur du matériel grand public offrent une haute scalabilité rentable. En outre, la blockchain fonctionne avec des algorithmes standard pour la cryptographie et le chiffrement des données, largement reconnus comme sécurisés dans de nombreuses industries et organisations gouvernementales [26]**.**

2.2.6 Avantages de la blockchain en matière de soins de santé :

La blockchain de soins de santé offre de nombreux avantages aux chercheurs médicaux, aux prestataires de soins de santé, aux aidants et aux individus. En regroupant toutes les données de santé dans un seul emplacement, en suivant les données personnalisées en temps réel et en permettant de définir les autorisations d'accès aux données de manière précise, elle favorise la recherche et la médecine personnalisée.

Les chercheurs en santé ont besoin de données complètes pour comprendre les maladies, accélérer la découverte médicale et développer des traitements personnalisés. La blockchain collecte des données diversifiées tout au long de la vie des patients, offrant ainsi un ensemble idéal pour les études longitudinales. Elle élargit également l'accès aux données de santé pour des populations sous-représentées dans la recherche médicale, facilitant ainsi l'engagement de ces populations et produisant des résultats plus représentatifs.

Les données de capteurs portables et d'applications mobiles, combinées à d'autres sources de données médicales, permettent une classification précise des patients et améliorent leur implication dans leurs propres soins de santé.

La disponibilité en temps réel des données facilite la coordination des soins cliniques, la détection précoce des épidémies et la surveillance continue des patients à haut risque. En favorisant le développement d'applications intelligentes pour les prestataires de soins de santé, la blockchain permet une discussion constructive entre le médecin et le patient sur les options de traitement[26].

2.3 Sécurité des soins de santé

2.3.1 Les 4 critères fondamentaux de la sécurité de l'information

Ces critères concernent des caractéristiques que le propriétaire ou le gestionnaire de l'information veut voir réalisées afin de s'assurer que la sécurité est au rendez-vous :

1. **Confidentialité** est cette caractéristique d'une information de n'être accessible qu'à ceux qui sont autorisés.
2. **L'intégrité** est la caractéristique d'une information de n'être modifiée que par des personnes autorisées et selon un procédé défini.

3. **La disponibilité** est la caractéristique d'une information d'être accessible et utilisable par son destinataire autorisé à l'endroit et à l'heure prévue.
4. **La traçabilité** est la caractéristique qui conserve les traces de l'état et des mouvements de l'information. Sans elle, on n'a aucune chance d'avoir l'assurance que les trois autres critères sont respectés[27]**.**

❖ **Le secret médical et les données à caractère personnelles et médicales :**

- **Secret médical** : Le secret médical est un principe éthique et juridique qui oblige les professionnels de la santé à ne pas divulguer les informations confidentielles obtenues dans le cadre de la relation médecin-patient, sauf autorisation expresse du patient ou dans des cas spécifiquement prévus par la loi. Il vise à protéger la vie privée et la confidentialité des informations médicales des patients.
- **Données à caractère personnel** : Les données à caractère personnel sont des informations qui permettent d'identifier directement ou indirectement une personne physique, telles que le nom, l'adresse, le numéro de téléphone, etc. Ces données sont soumises à des lois strictes de protection de la vie privée.
- **Données à caractère médical** : Les données à caractère médical sont un sous-ensemble des données à caractère personnel et incluent des informations spécifiques sur la santé d'une personne, telles que les antécédents médicaux, les diagnostics, les traitements, etc. Ces données sont également protégées par des réglementations strictes pour garantir la confidentialité et la sécurité des informations médicales des individus.

2.3.2 Sécurité et confidentialité des données à caractère médical :

Le premier et le plus important défi pour les applications contenant des données sensibles, concerne la sécurité et la confidentialité des données. Avec la mise en œuvre d'applications basées sur la technologie de la blockchain, la nécessité pour un tiers d'effectuer une transaction est éliminée. Étant donné que le mécanisme de blockchain permet à l'ensemble de la communauté, plutôt qu'à un seul tiers de confiance, de vérifier les enregistrements dans une architecture de blockchain, les données sont exposées à des risques potentiels en matière de sécurité et de confidentialité. Étant donné que tous les nœuds peuvent accéder aux données transmises par un nœud, la confidentialité des données ne sera pas active[12]**.**

La sécurité des données médicales est cruciale pour protéger la vie privée des patients et garantir l'intégrité des informations de santé.

❖ **La blockchain offre plusieurs solutions pour renforcer cette sécurité**

- ***L'immuabilité des données*** : La blockchain enregistre les données de manière immuable, ce qui signifie qu'une fois qu'elles sont enregistrées, elles ne peuvent pas être modifiées sans consensus du réseau. Cela empêche toute altération non autorisée des dossiers médicaux.
- ***La confidentialité des données*** : Les données médicales stockées sur la blockchain peuvent être chiffrées de manière sécurisée, garantissant que seuls les utilisateurs autorisés y ont accès. Chaque patient peut avoir un contrôle total sur qui peut voir ses informations.
- ***La traçabilité des accès*** : La blockchain permet de suivre chaque accès aux données médicales. Les patients peuvent voir qui a consulté leurs informations, quand, et dans quel but, ce qui renforce la transparence (la capacité à surveiller, à comprendre et à auditer les activités qui se déroulent sur les réseaux, les systèmes et les applications. et la responsabilité (la capacité à responsabiliser les utilisateurs et les personnes pour leurs actions).
- ***L'interopérabilité :*** La blockchain peut favoriser l'interopérabilité entre les différents systèmes de santé. Les informations médicales peuvent être partagées plus facilement et en toute sécurité entre les professionnels de santé, améliorant ainsi la qualité des soins.
- ***La gestion des consentements*** : Les patients peuvent gérer de manière autonome les autorisations d'accès à leurs données médicales via des contrats intelligents. Cela permet un contrôle granulaire sur la manière dont leurs informations sont utilisées.
- ***La sauvegarde des données*** : En répartissant les données sur un réseau décentralisé, la blockchain garantit qu'il n'y a pas de point de défaillance unique. Les données sont ainsi mieux protégées contre les cyberattaques.
- ***La recherche médicale*** : Les chercheurs peuvent accéder à des ensembles de données anonymisées stockées sur la blockchain pour des études médicales, tout en préservant la confidentialité des patients.

- ***La lutte contre la contrefaçon de médicaments*** : La blockchain peut être utilisée pour tracer la chaîne d'approvisionnement des médicaments, garantissant ainsi l'authenticité des produits pharmaceutiques.

2.3.3 Exigences de base pour le partage et la protection des données médicales

Un schéma idéal de partage et de protection des données médicales devrait satisfaire aux exigences de base suivantes, à savoir la sécurité et la protection de la vie privée, l'accès aux données, le contrôle du patient (engagement de l'utilisateur) et une norme unifiée :

1. **Sécurité et protection de la vie privée** : Les données médicales ne peuvent pas être utilisées illégalement par qui que ce soit. Le schéma devrait être en mesure de résister aux attaques malveillantes, et tout comportement illégal pourrait être tracé.
2. **Accès aux données** : une fois autorisés, les patients peuvent consulter toutes leurs données médicales et les médecins peuvent accéder aux informations médicales antérieures sous réserve de l'autorisation des patients.
3. **Contrôle du patient** : le patient pourrait gérer ses antécédents médicaux, c'est-à-dire que personne ne pourrait obtenir les données historiques sans l'accord du patient.
4. **Norme unifiée** : dans le modèle, tous les participants devraient utiliser une norme de données et un schéma de gestion unifiés, ce qui est utile pour mettre en œuvre le partage de données et améliorer la stabilité du système [28]**.**

2.4 Conclusion

La technologie blockchain représente une avancée majeure et prometteuse dans le domaine de la santé. En offrant une solution décentralisée et sécurisée pour la gestion des données médicales, elle répond à plusieurs des défis actuels du secteur, notamment en termes de sécurité, de confidentialité, d'interopérabilité et de contrôle des accès. Les applications potentielles de la blockchain en santé sont nombreuses et variées, allant de la gestion des dossiers médicaux électroniques à la télémédecine, en passant par la recherche médicale et la lutte contre la contrefaçon de médicaments.

Les études et les prototypes tels que MedRec et MeDShare démontrent déjà les bénéfices concrets de l'utilisation de la blockchain, comme la sécurisation des données, l'amélioration de

l'accès aux informations par les patients et les professionnels de santé, et l'optimisation des processus administratifs. En centralisant les données de santé de manière sécurisée et en permettant une gestion fine des autorisations d'accès, la blockchain favorise une approche plus centrée sur le patient, permettant une meilleure coordination des soins et une personnalisation accrue des traitements.

Néanmoins, l'adoption de la blockchain dans le secteur de la santé n'est pas sans défis. La scalabilité, la standardisation des données, et la protection de la vie privée sont des enjeux majeurs qui nécessitent des solutions technologiques robustes et une collaboration étroite entre les différents acteurs du secteur.

En conclusion, bien que la technologie blockchain soit encore en phase de développement et d'expérimentation, ses potentialités pour transformer le secteur de la santé sont immenses. En offrant une infrastructure transparente, sécurisée et efficace pour la gestion des données médicales, la blockchain peut contribuer de manière significative à améliorer la qualité des soins, à réduire les coûts et à favoriser l'innovation dans le domaine médical.

Chapitre 3
Conception de notre protocole de contrôle d'accès décentralisé

3.1 Introduction

Les données des patients constituent un atout précieux pour leur bonne prise en charge. Malgré les préoccupations en matière de confidentialité, 90 % des Américains estiment important d'avoir un accès en ligne à leurs dossiers médicaux [29]. Cependant, les médecins et les patients disposent chacun d'un ensemble différent d'informations recueillies au fil des ans. Un emplacement central où toutes les informations sur le patient peuvent être compilées et accessibles aussi bien aux médecins qu'aux patients est fortement demandé **[30].**

Dans le chapitre qui suit, nous allons présenter la problématique que nous avons traitée au cours de notre PFE, et nous allons par la suite donner la solution que nous avons conçue.

Notre architecture vise à permettre aux patients de gérer tous seuls leurs propres données de manière sécurisée. Elle se compose de trois couches :

La couche de stockage : Cette couche fournit un service de stockage évolutif, sécurisé, décentralisé hautement disponible et protégée contre les attaques de confidentialité et d'intégrité. Les données sont stockées dans le cloud décentralisé de type **IPFS**. Le réseau IPFS est un réseau de stockage distribué et participatif, ce qui réduit le problème des silos de données qui affectent les serveurs centraux. L'intégrité de toutes les données est vérifiée à l'aide de fonctions de hachage, vous pouvez donc avoir confiance que vous obtenez toujours les données que vous recherchez. Les fichiers et les données peuvent être stockés sur plusieurs nœuds, ce qui permet de maintenir le contenu accessible même en cas de pannes critiques.

La couche de Gestion des Accès : Elle est composée d'un protocole de contrôle d'accès implémenté en surcouche d'une blockchain privée.

Couche d'Utilisation des Données Les entités qui utilisent les données de santé des patients sont incluses dans cette couche.

3.2 Problématique traitée au cours de notre projet

La problématique que nous avons traitée dans notre projet de fin d'étude est la suivante : Comment permettre au patient d'être seul propriétaire de ces données médicales, mais en même temps de les stocker en ligne en toute confidentialité. (celà implique l'utilisation de la cryptographie et du chiffrement). Par seul propriétaire, nous voulons dire qu'il est le seul à avoir accès à ses données, et la seule habilité à en donner l'accès au personnel médical en cas de besoin. Personne, pas même le fournisseur de service de stockage en ligne n'a accès aux dossier médical en clair ou aux clés de chiffrement dudit dossier.

La problématique centrale de notre travail réside dans la protection des informations sensibles des patients (nous avons traité en particulier le côté confidentialité des données). Cette problématique constitue un défi majeur lors de la conception d'applications blockchain pour les soins de santé, comme en témoignent les recherches scientifiques dans ce domaine.

Les systèmes actuels de gestion des prestations de santé sont confrontés à des limitations significatives, en raison notamment de leur nature centralisée et des coûts élevés associés à leur maintenance et à leur mise à jour.

3.3 Travaux antérieurs :

Les travaux existants les plus étroitement liés aux nôtres se situent dans le domaine des systèmes de données de santé basés sur le cloud. Nous résumons ceux que nous avons considérés comme les plus pertinents comme suit. Les études citées dans la référence [31]**.** Ont conçu un cadre au niveau national pour les systèmes médicaux électroniques basés sur des modèles de cloud. Par exemple, les auteurs de la référence [32]**.** Ont proposé un modèle basé sur le cloud pour construire un système d'information au niveau national qui offrait un moyen rentable de traiter les informations des patients dans les zones rurales. Les gens sont encouragés à fournir leurs informations de santé personnelles qui seront stockées dans le cloud de santé et consultées par les professionnels de la santé et les décideurs politiques pour fournir davantage de services médicaux, tels que le diagnostic et le contrôle à distance des maladies, etc. Le cloud utilisé était un cloud centralisé. Dans [33]**.** Un cadre couvrant le processus de la collecte des données à leur livraison est fourni. En utilisant des capteurs attachés aux équipements médicaux, les données peuvent être collectées et stockées dans un cloud directement, ces données peuvent être consultées par des professionnels médicaux autorisés [34]**.** Ont introduit un système centré sur le patient construit sur le cloud avec une couche de collecte de données,

une couche de gestion de données et une couche de service de données. Le chiffrement basé sur la technique cryptographique ABE (attribut base encryptions) est l'un des schémas de chiffrement les plus populaires utilisés dans le cloud [35] et [36]**.** Ont proposé un modèle de contrôle d'accès centré sur le patient et préservant la confidentialité basée sur l'ABE[37]. Ont décrit un nouveau cadre avec un modèle de contrôle d'accès basé sur les rôles, conscient de la confidentialité et basé sur le cloud, qui peut être utilisé pour la contrôlabilité, la traçabilité des données et l'accès autorisé aux ressources de données de santé[30]**.**

3.4 Notre contribution :

Lors de l'étude des différents travaux antérieurs, nous avons constaté que la majorité des systèmes proposés se concentrait sur donner le contrôle total au patient en matière de gestion de ses données. Mais le stockage la plupart du temps était centralisé chez un fournisseur. Ceci n'est pas conforme à la vision que nous avons de la propriété des données médicales. Si les données sont stockées chez un fournisseur de cloud, nous ne pouvons pas prétendre que ces données appartiennent à 100% au patient, puisqu'il dépend du fournisseur d'accès pour lui fournir le service. L'architecture que nous proposons est basée sur un système de stockage cloud décentralisé de type IPFS [38]**.**

Les systèmes que nous avons étudiés ne proposaient pas de mécanisme d'accès d'urgence aux dossiers du patient dans le cas où celui-ci n'est plus en mesure d'accéder à ses données, par exemple, s'il est trop malade ou inconscient. Et dans les rares cas qu'ils le proposaient, ils ne donnaient pas d'implémentation précise.

L'architecture que nous proposons offrira au patient la possibilité de désigner deux personnes de confiance, qui pourront dans un tel cas, reconstruire les clés de chiffrement du patient. Et ainsi pourront fournir les autorisations d'accès aux personnel médical. Nous utilisons le protocole de partage de secret développé par "Adi Shamir". Ce protocole sera décrit brièvement dans la suite du document.

3.4.1 Partage de clé secrète de Shamir

Le partage de clé secrète de Shamir (*Shamir Secret Sharing*) est un algorithme de **Cryptographie** [39] créé par **Adi Shamir**[40]. C'est une forme de **secret réparti**[41], où un secret est divisé en parties, donnant à chaque participant sa propre clé partagée, où certaines des parties ou l'ensemble d'entre elles sont nécessaires afin de reconstruire une phrase de passe qui donne accès au secret.

Dans certains cas, il n'y a pas forcément besoin de tous les participants pour reconstituer le minimum nécessaire qui forme la phrase de passe d'accès au secret, c'est pourquoi est parfois utilisé un schéma de seuil où un nombre k des parties est suffisant pour reconstruire le secret d'origine**[42].**

- **Explication avancée**

Le partage de clés secrètes de Shamir est utilisé pour sécuriser l'accès à un secret (un fichier, un texte...) de manière distribuée, le plus souvent pour sécuriser d'autres clés de chiffrement. Le secret est divisé en plusieurs morceaux, appelées *parties*. Ces morceaux, en *éclats de verre*, sont utilisés pour reconstituer le secret original : *la phrase de passe*.

Pour déverrouiller l'accès au secret via le partage de clés secrètes de Shamir, nous avons besoin d'un nombre minimum de parties réunies. C'est ce qu'on appelle **le seuil**, qui est utilisé pour indiquer le nombre minimum de parties nécessaires pour reconstituer la phrase de passe et verrouiller l'accès au secret. Prenons un exemple : Nous allons faire une équation linéaire passant par le point (0, S). Il existe de nombreuses équations linéaires passant ce point, comme illustré dans la figure 12 ci-dessous. Le schéma de partage de secret de Shamir est basé sur un principe simple que nous avons étudié étant enfants : il existe une multitude de droites qui peuvent passer par un point donné (figure 13). Cependant, si l'on fournit les coordonnées de deux points, nous ne pourrons trouver qu'une seule droite qui passe par ces deux points (voir figure14)

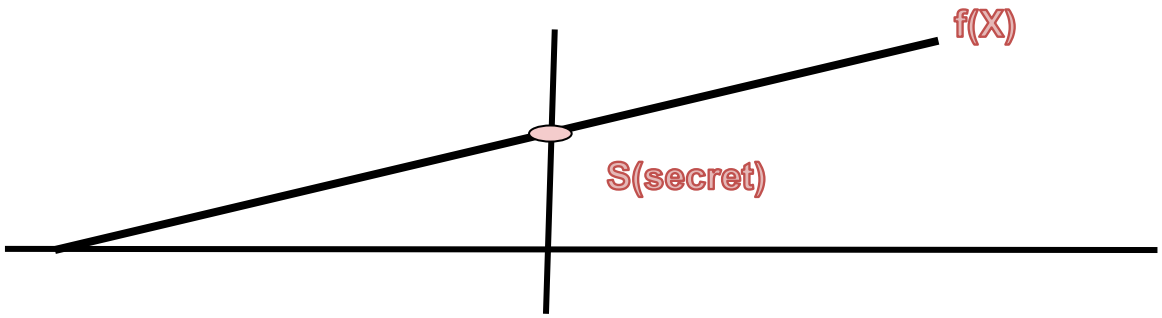

Figure 12- Le secret S et la droite qui lui correspond.

Dans la figure 10 ci-dessus, le secret S est sur l'axe des ordonnées. et c'est toujours le cas quand nous utilisons l'algorithme de Shamir.

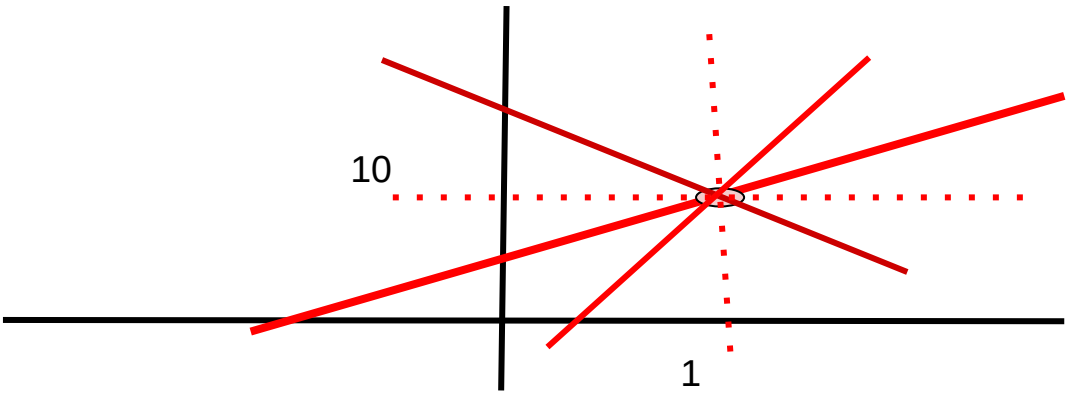

Figure 13- une multitude courbe peuvent passer par un seul point.

- **Exemple d'utilisation :** La société **XYZ** doit sécuriser le mot de passe de son coffre-fort. Elle pourrait utiliser un moyen standard, comme **l'AES**, mais que faire si la détentrice ou le détenteur de la clé n'est pas disponible ou meurt ? Que se passe-t-il si la clé est compromise par un pirate malveillant ou si le détenteur de la clé décide de trahir la société, et utilise son pouvoir sur le coffre à son avantage ? »
- C'est là qu'intervient le partage de clé secrète de Shamir. Il peut être utilisé pour chiffrer le mot de passe du coffre-fort et générer un certain nombre de parties, une configuration dans laquelle un certain nombre de parties peut être attribué à chaque dirigeant de la société XYZ. Ce n'est que s'ils mettent leurs parties en commun qu'ils peuvent reconstituer la phrase de passe secrète pour déverrouiller le coffre-fort. Le seuil peut être fixé de façon appropriée en fonction du nombre de personnes impliquées, de sorte que le coffre-fort soit toujours accessible par les personnes autorisées. Si une partie ou deux tombaient entre de mauvaises mains, cela ne permettrait pas de déverrouiller par mot de passe à moins que les autres dirigeants ne coopèrent avec leurs parties distribuées auparavant.
- **Définition mathématique :** Formellement, notre objectif est de diviser certaines données **D** (par exemple, la combinaison du coffre) en **N** pièces $\boldsymbol{D_n}$, $\boldsymbol{D_n} \ldots \boldsymbol{D_n}$ de telle sorte que :
    - La connaissance de **K** ou plus "$\boldsymbol{D_i}$" ***pièces*** rend **D** facilement calculable ;
    - La connaissance de **K-1** ou moins "$\boldsymbol{D_i}$" ***pièces*** rend **D** complètement indéterminée (en ce sens que toutes ses valeurs possibles sont également probables).

3.4.2 Système de partage de secret de Shamir

L'idée essentielle d'Adi Shamir[40] est que 2 points sont suffisants pour définir une ligne, 3 points suffisent à définir une parabole, 4 points pour définir une courbe cubique [43], etc. Autrement dit, il faut ***K*** points pour définir un polynôme de degré **K-1.** La figure 12 ci-dessous représente une ligne qui correspond à un polynôme de premier ordre. Cela veut dire que le seuil ici est égal à 2 (K). Il suffit de connaître les coordonnées de deux points, afin de pouvoir reconstituer le polynôme correspondant F(x). Après cela, il suffit de calculer F(0) pour connaître le secret (dans l'algorithme de Shamir, le secret est toujours un point sur l'axe des y). Dans la figure 12 ci-dessous, le secret est égal à 7.

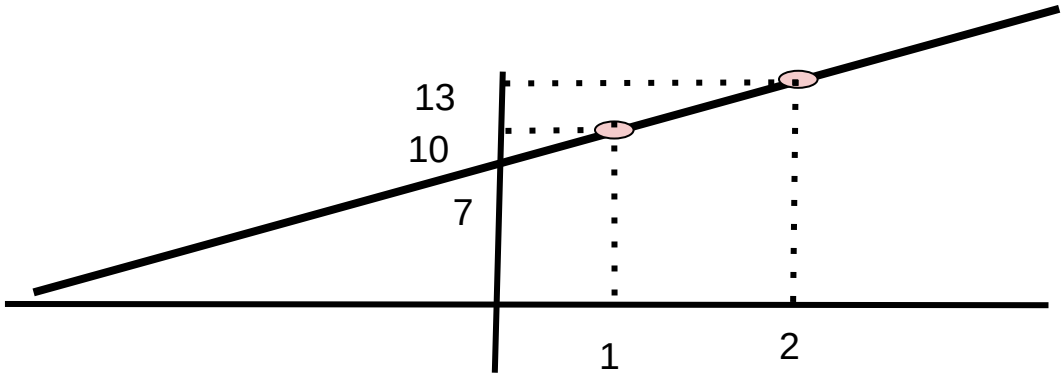

Figure 14- reconstruction du secret partagé avec un seuil égal à 2

- **Méthode de génération de secret :**
  - Supposons que nous voulons utiliser un schéma de seuil **(K,n)** pour partager notre secret **"S",** que l'on suppose être un élément dans un corps fini F. Nous allons choisir au hasard $(K-1)$ coefficients $a_1, a_2, \ldots, a_{k-1}$ dans F, et poser $a_0 = S$. Ensuite, nous allons construire le polynôme $F(x) = a_0 + a_1 x_1 + a_2 x_2 + \cdots a_{k-1} x_{k1}$
  - Soient n'importe quels **"n" points** calculés à partir de ce polynôme. Par exemple, si nous voulons partager notre secret en n parties, nous allons calculer pour (i=1,..n)les valeurs $(i, f(i))$**.** Chaque participant se voit attribuer un point (un couple d'antécédent et de l'image correspondante à la fonction polynomiale[44]. Étant donné un sous-ensemble de '**k**' ces couples, nous pouvons trouver les coefficients du polynôme à l'aide de l'interpolation polynomiale, le secret étant le terme constant **a0**[42]**.** Pour

plus de précisions sur la méthode de calcul ou les propriétés de sécurité de l'algorithme, le lecteur peut consulter l'article original dans la référence suivante [45].

3.5 Le Rôle de la Technologie Blockchain dans la Facilitation de l'Échange de Données Médicales"

La blockchain sert à établir un système de contrôle d'accès basé sur une architecture décentralisée. Cela permettra aux individus de gérer leur DSE (dossier médical électronique) et d'en être les seuls propriétaires. En plus de télécharger le DSE, le patient peut également choisir de le partager en lecture ou en écriture avec son médecin. La blockchain améliore la commodité de l'échange des dossiers médicaux grâce à ses caractéristiques. Peu importe le lieu de la consultation médicale, le patient pourra accéder à son DSE tant qu'il dispose d'un réseau pour se connecter au système [46].

3.6 Description générale de notre modèle de contrôle d'accès aux données des patients

Notre modèle de contrôle d'accès aux données des patients est conçu pour définir les autorisations d'accès des professionnels de santé à différents types de données. Le patient a le pouvoir de consulter des données et de consentir à leur consultation et modification. Le patient n'a pas le droit de modifier lui-même ses données de santé (afin de garantir l'intégrité des données et leur utilisabilité en cas de besoin). Le patient a le droit de choisir deux personnes de confiance (des personnes de son entourage). Ces personnes de confiance vont pouvoir prendre le contrôle du dossier médical dans le cas où le patient n'est plus en mesure de le faire (maladie mentale, accident grave, etc.). Les professionnels de santé, quant à eux, peuvent consulter les données (lecture) et les modifier (lecture/écriture) en fonction des autorisations accordées par le patient. Notre objectif principal est de gérer de manière efficace le contrôle d'accès des utilisateurs.

L'administrateur du système est responsable de la gestion du système (usage classique d'un administrateur (ajout d'utilisateur etc.,). L'administrateur est également responsable de la récupération des clés de chiffrement du patient dans les cas d'urgence. Il pourra avec l'aide des personnes de confiance désignées par le patient, récupérer les clés de chiffrement. Il est à souligner, que l'administrateur, tout seul, ne peut récupérer ses clés de chiffrement sans

l’intervention de “au moins une des personnes autorisées par le patient”. De même, les personnes de confiance désignées par le patient, ne pourront pas reconstruire les clés de chiffrement du patient chacune de leur côté. Afin de reconstituer le secret, il faut au minimum la collaboration de deux personnes. Ceci va garantir la confidentialité du dossier médical et en même temps, sa disponibilité dans les cas d’urgence.

Notre plateforme web dispose d'une interface de connexion permettant à l'administrateur, au patient et au personnel de santé de s'authentifier. L'administrateur a la possibilité d'ajouter un membre du personnel de santé ou un patient. De plus, notre plateforme comprend une interface dédiée au "Personnel de santé", où chaque utilisateur dispose d'un numéro d'employé (identifiant) et d'un mot de passe.

Le personnel médical peut consulter le dossier du patient avec son autorisation, et il peut mettre à jour les données. En revanche, en l'absence d'autorisation, il est seulement autorisé à consulter les données sans possibilité de les modifier.

Enfin, notre application intègre une interface "Patient" permettant à ce dernier de consulter son profil et de donner l'autorisation au personnel de santé pour accéder à ses données.

3.7 Environnement système et architecture

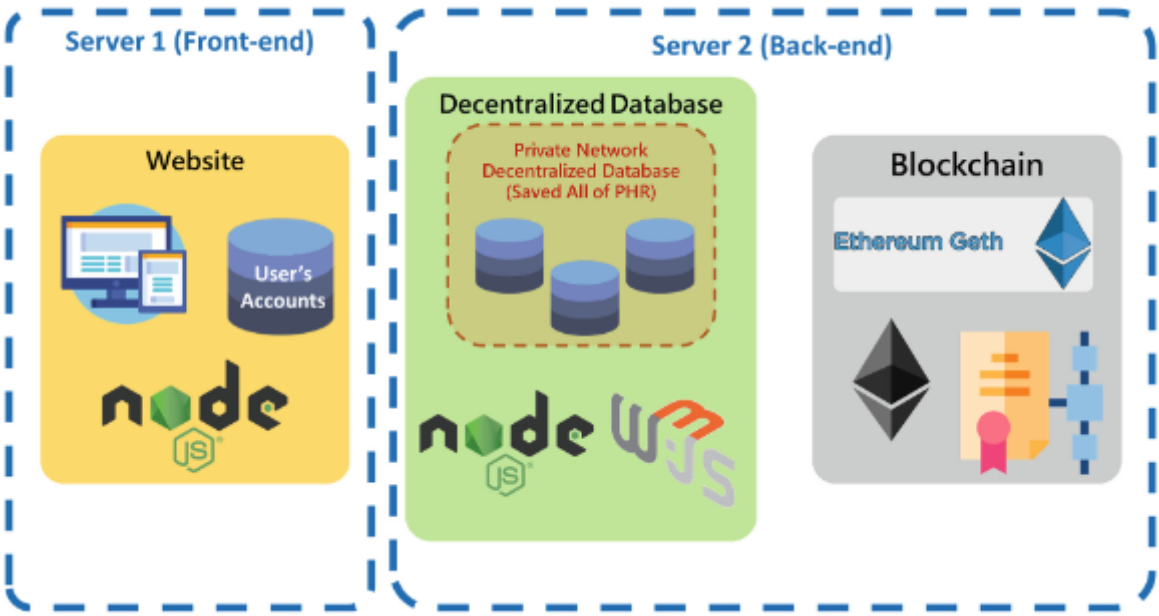

Figure15- l’architecture que nous avons proposée. Elle est constituée de trois modules

La figure 15 ci-dessus représente l'architecture que nous avons proposée. Elle est constituée de trois modules :

- Module du site Web de visualisation : Tous les utilisateurs téléchargent, visualisent et partagent des données en utilisant ce module.
- Module de base de données décentralisée : Stocke toutes les données médicales. Ne fournit que la fonction d'ajout d'enregistrements et de visualisation via le module du site Web de visualisation, sans fonction de modification ni de suppression.

Chaque fois que de nouvelles données sont ajoutées, elles sont transférées au module blockchain via Web3.js.

3.8 Méthodes d'analyse et de conception

Dans cette section, nous présentons plusieurs modèles de conception de notre application à travers des diagrammes UML, notamment le diagramme de cas d'utilisation et le diagramme de séquence. Ces diagrammes visent à fournir une représentation visuelle claire des fonctionnalités et des interactions au sein de notre application.

3.8.1 Les besoins attendus de protocole de contrôle d'accès

❖ **Identification des acteurs :**

- ***Administrateur*** : L'administrateur est responsable de la gestion globale de la plateforme. Il a le pouvoir d'ajouter des outils pour gérer les fonctionnalités de l'application. Il a également le pouvoir d'initier la procédure de récupération des clés de chiffrement du patient en cas d'urgence. La fonctionnalité de l'administrateur inclut :
  - **La Gestion du Personnel de Santé** : L'administrateur peut créer des contrats pour chaque membre du personnel médical lors de son ajout initial dans le système. Ces contrats établissent les conditions et les termes de l'engagement professionnel avec le système. Une fois créés, ces contrats ne peuvent pas être modifiés ou supprimés par la suite, assurant ainsi l'intégrité et la permanence des accords contractuels.
  - ***Gestion Patients*** : Les informations des patients sont saisies via un formulaire et utilisées pour générer le contrat.

- **Récupérer les clés de chiffrement en collaboration avec les personnes de confiance désignées par le patient.**

- ***Patient*** : Le patient est l'utilisateur final de l'application. Il a le contrôle sur ses propres données de santé et peut décider d'autoriser ou de refuser l'accès à ces données aux professionnels de santé. Les fonctionnalités du patient sont les suivantes :
  - ***Consultation du profil***
  - ***Gestion des autorisations d'accès***
  - ***Consultation des données de santé***
  - ***Définition de deux personnes de confiance pour les cas d'urgence.***
- ***Personnel médical*** : Le personnel médical Nous entendons par ce terme les médecins. Les fonctionnalités auxquelles ils ont accès sont les suivantes :
  - ***Consultation des données autorisées par les patients***
  - ***Modifications des données autorisées par les patients.***
  - ***Accès en Urgence : En situations d'urgence, les médecins peuvent obtenir des accès temporaires et prioritaires aux informations médicales essentielles.***

- **Remarque** :' Nous n'avons pas pris en considération les autres catégories de métiers dans la description de notre protocole de contrôle d'accès. Même si notre protocole peut être utilisé par les autres catégories puisque, le patient est en mesure de donner accès à une partie seulement de son dossier médical, et que cet accès peut être en lecture seule'.

❖ Diagramme de profil :

Le diagramme dans la figure 16 ci-dessous représente le diagramme de profile de notre protocole

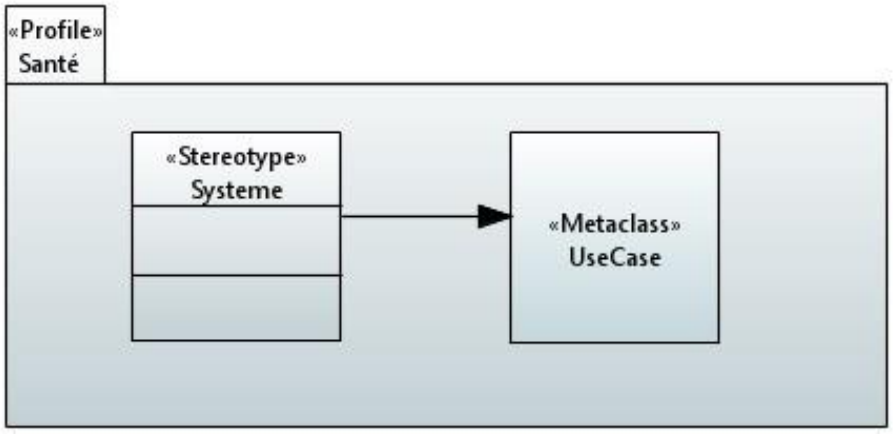

Figure 16-Diagramme de profile

❖ Le Diagramme de contexte statique :

Le diagramme dans la figure 17 ci-dessous représente le diagramme de contexte statique : de notre protocole

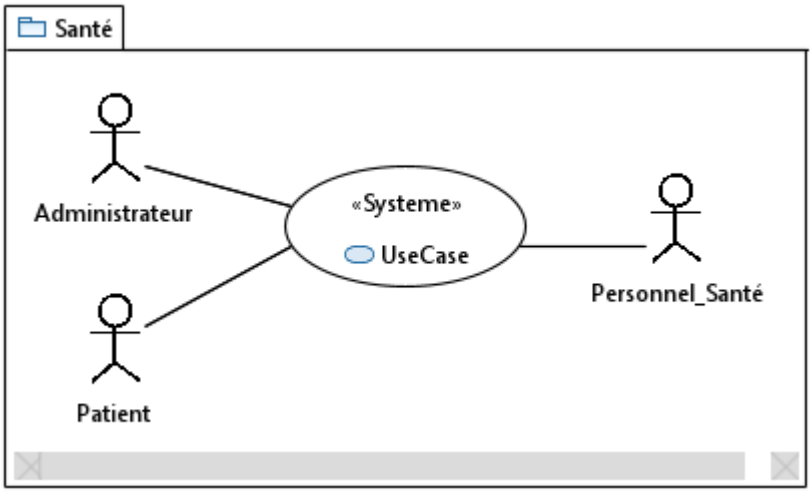

Figure 17-Diagramme e de contexte statique

Le Diagramme de cas d'utilisation :

Le diagramme dans la figure 18 ci-dessous représente le diagramme de cas d'utilisation :

Figure 18-Diagramme de cas d'utilisation :

3.9 La description textuelle de deux scénarios d'utilisation de notre protocole

Scénario1 :

Dans cette sous-section, deux scénarios d'utilisation de notre système sont présentés, mettant en scène John, un patient, et son médecin Bob. John peut décider d'accorder à Bob

l'accès à ses données de test sanguin par exemple, qu'il chiffre et envoie à Bob via notre système. Comme nous l'avons expliqué plus tôt, les données sont stockées de manière sécurisée dans un cloud décentralisé. Les données sont chiffrées à l'aide de l'Advanced encryptions standard dans sa version la plus sûre (AES-256), seul John connaît la clé de déchiffrement. Lors de l'inscription dans notre système, chaque patient se voit attribuer une clé de chiffrement symétrique. En plus, comme nous l'avons expliqué lors du premier chapitre, les adresses dans la blockchain sont en réalité des clés publiques de chiffrement asymétrique. Lors de L'inscription, John en obtenant une adresse ethereum se verra attribuer une paire de clé publique et privée. Les membres du personnel médical comme Bob dans notre application se verront également attribuer leur pair de clé publique privée qui correspond à leur adresses ethereum.

Si John désire au cours d'une consultation partager une partie de son dossier médical avec Bob, il va la déchiffrer avec sa clé AES-256, ensuite, il va la chiffrer avec la clé publique de Bob et transmettre le dossier chiffré au travers de la blockchain (dans un bloc de données). Bob va alors recevoir une notification dans l'application lui indiquant que John vient de partager avec lui des données.

Si John souhaite conserver certaines informations confidentielles, il peut les masquer pour empêcher tout accès non autorisé.

Ce scénario est compatible avec les deux cas de figures : partage avec autorisation de modification et partage en lecture seule. Cependant, dans le cas où Bob a obtenu le droit de modifier les données, il devra refaire le chiffrement en utilisant la clé publique de John. John déchiffrera par la suite les données et effectuera un dernier chiffrement avec sa clé de chiffrement symétrique (AES-256) et enverra les données mises à jour sur le serveur cloud

Scénario 2 :

Dans le cas où John est admis aux urgences et qu'il n'est plus en mesure de fournir son consentement pour la consultation de son dossier médical : Bob le médecin va faire la demande d'un accès d'urgence auprès de Alice (l'administratrice du système).

Les personnes de confiance sélectionnées par John lors de sa première inscription sont contactées par téléphone ou tout autre moyen rapide disponible. L'une d'entre elles (Rachelle) devra se présenter et fournir la partie du secret qu'on lui a communiqué auparavant. Elle combinera sa partie du secret avec celle de Alice (l'administrateur) afin de reconstruire la clé de chiffrement symétrique originale de John et pouvoir lui donner les soins nécessaires.

3.10 Diagramme de séquence

3.10.1 Diagramme de Séquence : Authentification

Le diagramme dans la figure 14 ci-dessous représente diagramme de séquence d'authentification illustre le processus d'interaction entre un utilisateur (administrateur ou patient ou professionnel de santé) et le système pour s'authentifier. (La figure 11 suivante représente Diagramme de Séquence : Authentification)

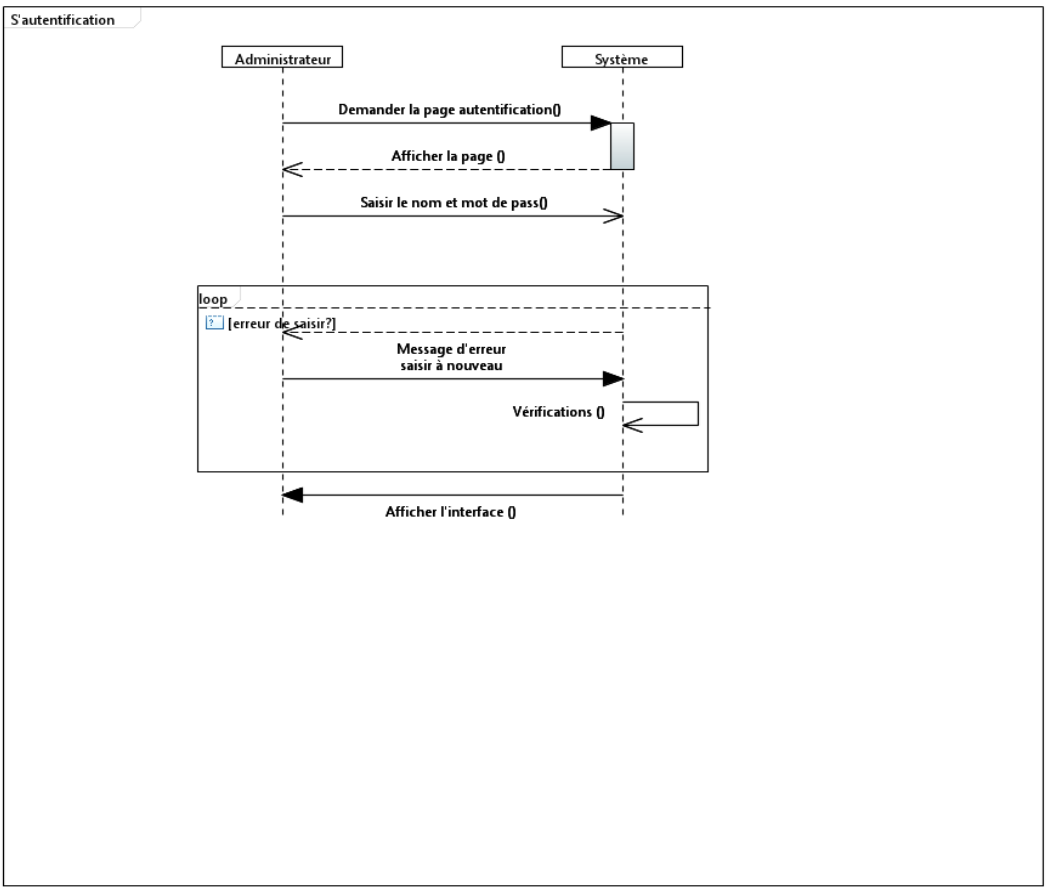

Figure 16-Diagramme de séquence administrateur pour s'authentifier.

3.10.2 **Diagramme de Séquence : Ajout d'un Patient par l'Administrateur**

Le diagramme dans la figure 19 ci-dessous représente illustre le processus par lequel un administrateur s'authentifie dans le système et ajoute un nouveau patient. (Diagramme de Séquence : Ajout d'un Patient par l'Administrateur).

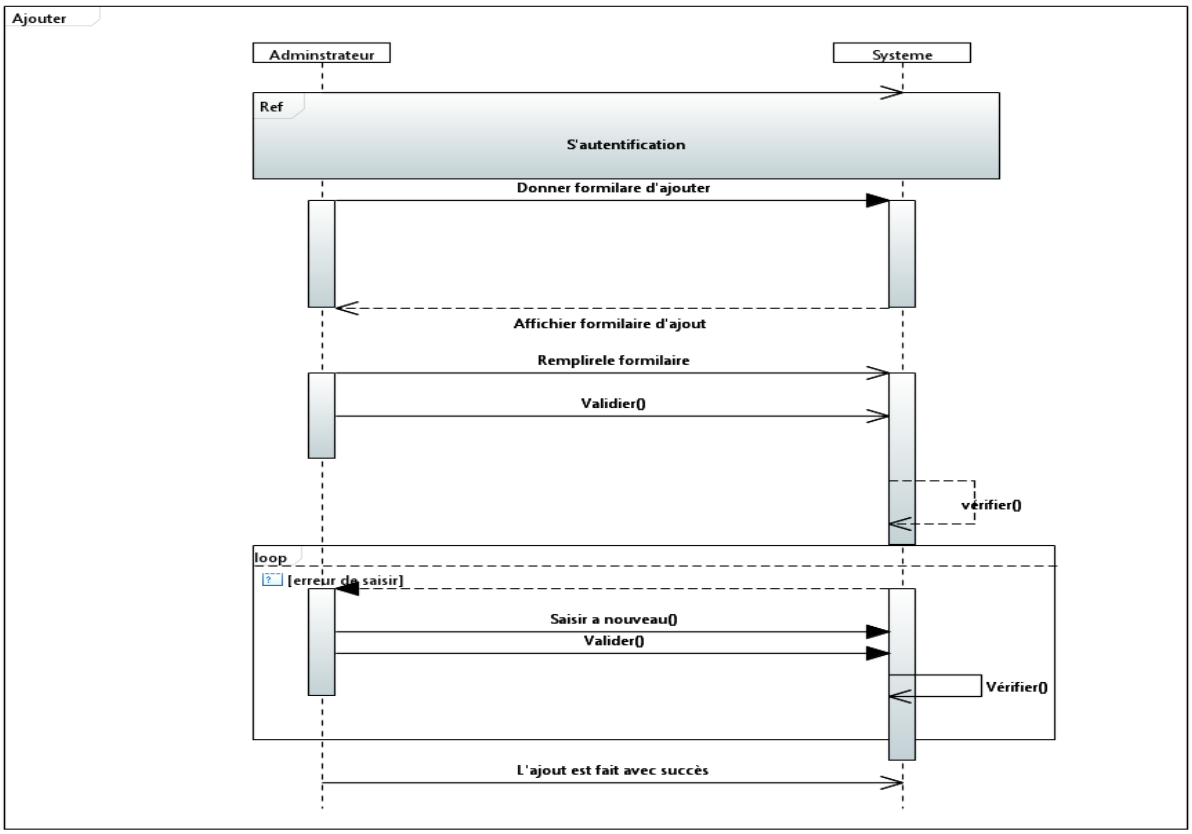

Figure 19-Diagramme de séquence administrateur pour gestion de patient .

3.10.3**Diagramme de Séquence : Consultation de la donnée par le Patient**

Le diagramme dans la figure 14 ci-dessous représente illustre le processus par lequel un patient consulte sa donnée via l'application**.**

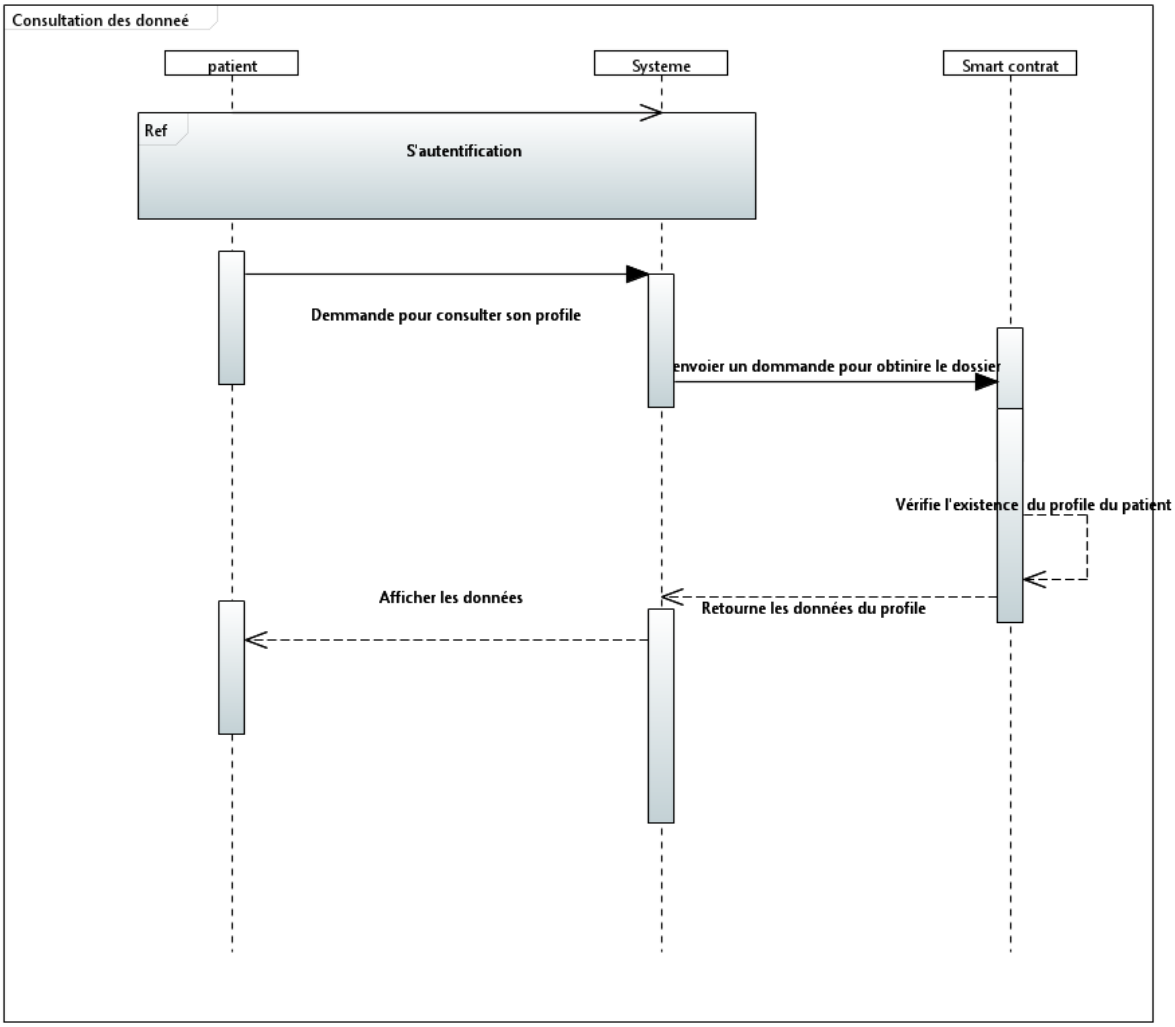

Figure 3.19-Diagramme de séquence pour Consultation des données par le Patient.

3.10.4 **Diagramme de Séquence : Gestion des Autorisations d'Accès:**

Le diagramme dans la figure 20 ci-dessous représente illustre le processus par lequel un patient consulte sa donnée via l'application**.** Illustre le processus par lequel un patient gère les autorisations d'accès pour les professionnels de santé. Ce processus permet de définir qui peut accéder aux données du patient et dans quelles conditions.

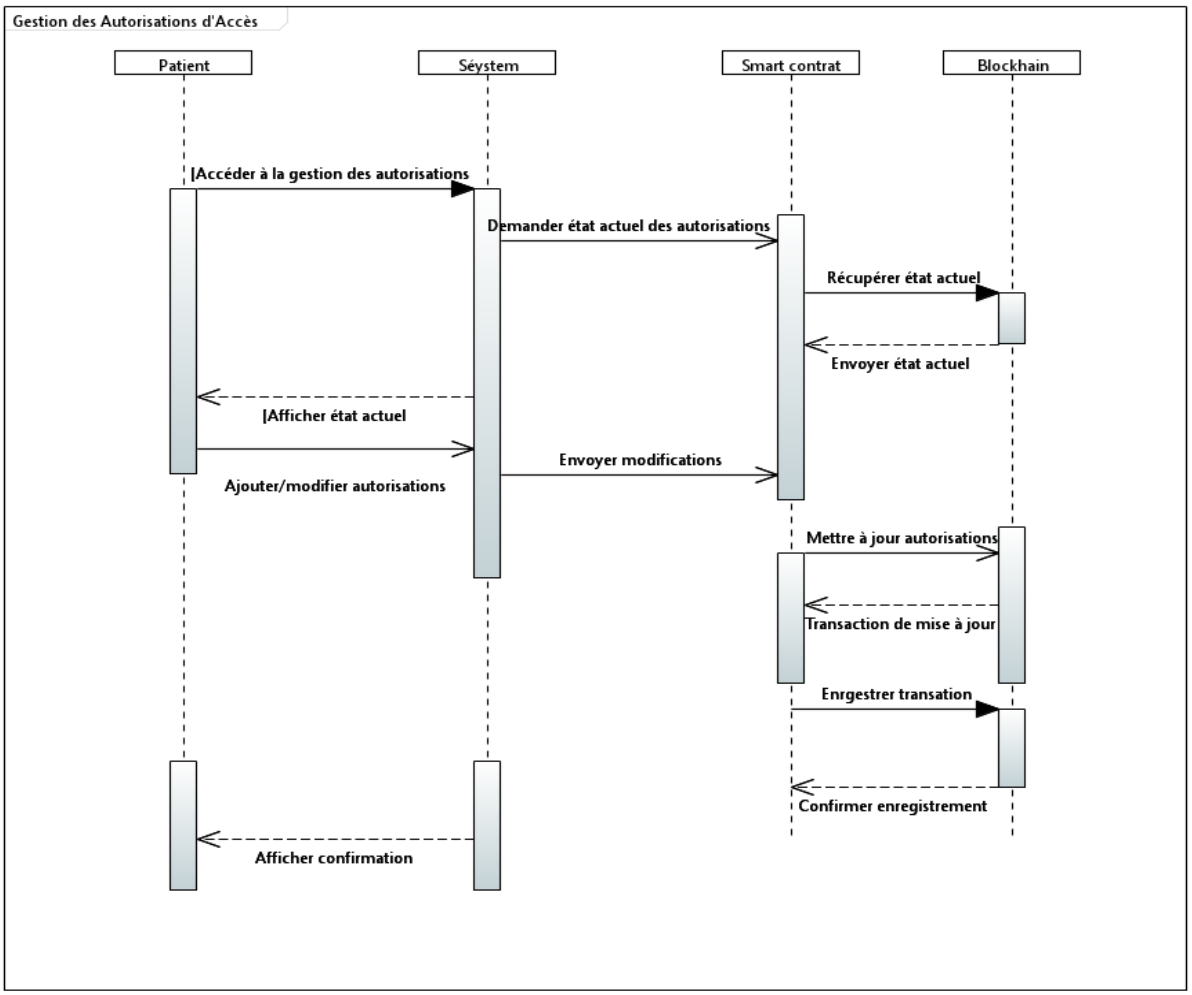

Figure 20-Diagramme de séquence pour la Gestion des Autorisations d'Accès

3.10.5 Diagramme de Séquence : Définition de Deux Personnes de Confiance pour les Cas d'Urgence via un Smart Contract

Le diagramme dans la figure 21 ci-dessous représente illustre le processus par lequel un patient consulte sa donnée via l'application illustre le processus par lequel un patient définit deux personnes de confiance via un smart contract pour accéder à ses données médicales en cas d'urgence. Ce processus utilise la technologie blockchain pour enregistrer et gérer les autorisations de manière sécurisée et décentralisée.

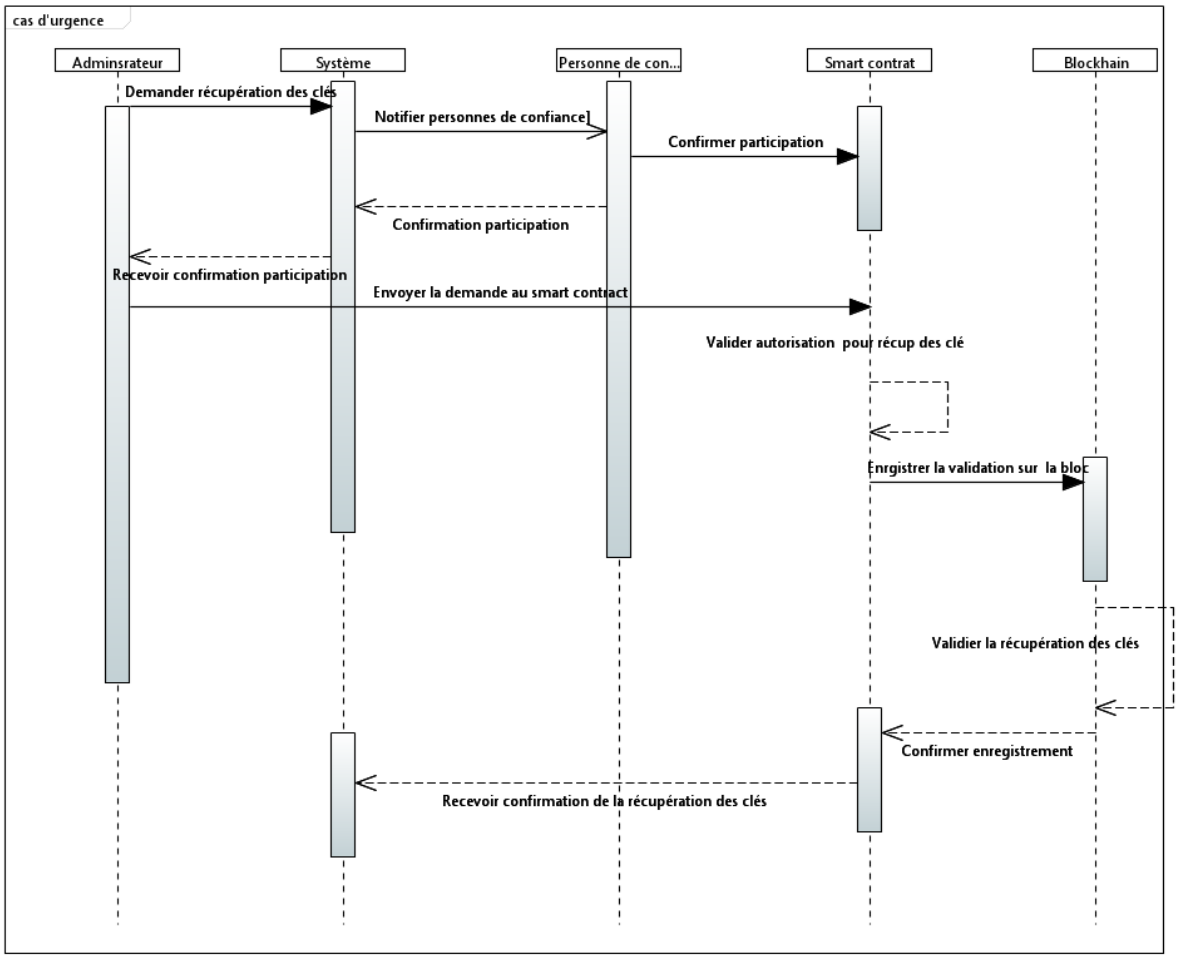

Figure 21-Diagramme de séquence pour la *Définition de Deux Personnes de Confiance pour les Cas d'Urgence*

3.10.6 Diagramme de Séquence : Consultation des données autorisées par les patients

Le diagramme dans la figure 22 ci-dessous représente illustre le processus par lequel un patient consulte sa donnée via l'application**.** Illustre le processus par lequel un **professionnel**

de santé consulte les données d'un patient pour lesquelles il a obtenu les autorisations nécessaires.

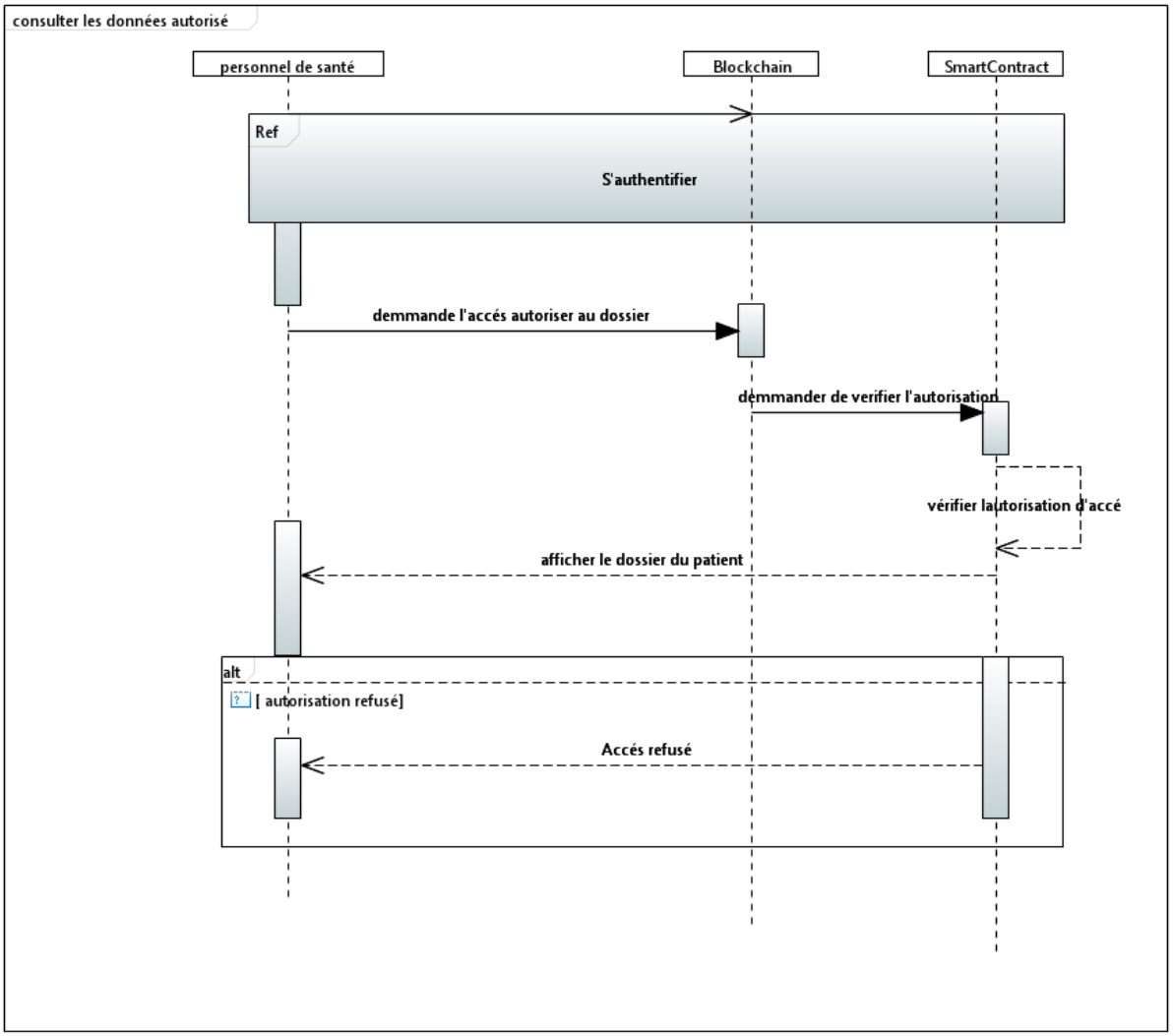

Figure 22-Diagramme de séquence pour la Consultation des données autorisées par les patients.

3.11 Diagramme de classe

Le diagramme dans la figure 23 ci-dessous le diagramme de classe.

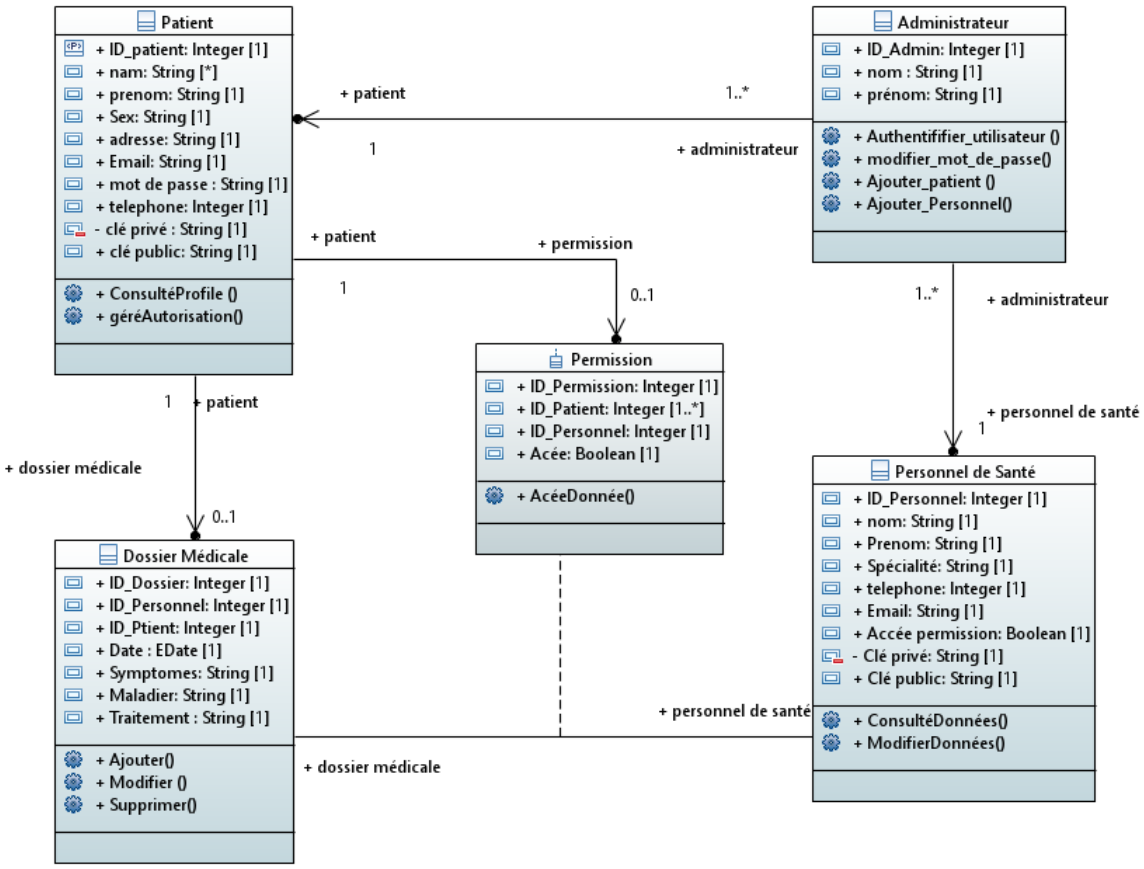

Figure 23 – Diagramme de classe.

3.12Implémentation

Dans cette section, nous donnons une description de l'implémentation de notre protocole.

Notre système de contrôle d'accès utilise trois fonctions cryptographiques : un algorithme de chiffrement symétrique (voir la section (algorithmes symétriques dans chapitre

1)), un algorithme de chiffrement asymétrique (voir section chapitre 1) et enfin l'algorithme de Shamir pour le partage de secret qui nous servira à partager la clé de chiffrement symétrique pour l'avoir la récupération plutard en cas d'urgence.

Le Protocole de contrôle d'accès que nous avons proposé consiste en les fonctionnalités suivantes :

1. L'inscription des utilisateurs (patient ou personnel de santé).
2. Le contrôle des accès aux données à l'aide de la Blockchain : Le patient peut autoriser un membre du personnel de santé à accéder uniquement en lecture ou en lecture et écriture.
3. La récupération des clés de chiffrement à l'aide de l'algorithme de Shamir.

Dans ce qui suit, nous allons donner une description détaillée de chaque étape.

3.12.1 Inscription d'un Utilisateur de Type Patient :

Lors de l'inscription, le patient (John) va fournir les informations nécessaires à son identification. Il fournira également l'identité et le contact de deux personnes de confiance : par exemple Alice, son épouse, et Rachelle, sa sœur.

1. Après l'inscription, John va se voir attribuer une paire de clés ($\mathbf{S_K}$, $\mathbf{P_K}$,).

2. générée par G( ) (voir section chiffrement symétriques). John se verra également attribuer une clé secrète K pour l'algorithme de chiffrement symétriques.

Remarque : De nombreuses méthodes permettent de générer des clés de chiffrement pour des algorithmes symétriques et asymétriques. Nous n'allons pas aborder cette partie dans la description du protocole.

3. Accorder l'accès s'effectue de la façon suivante :

4. John télécharge les données (c) demandées depuis le cloud.

5. Il utilise sa clé de chiffrement symétrique pour les déchiffrement : m← D (c , k).

6. Ensuite il va chiffrer les données qui sont à présent en clair à l'aide la clé publique de Bob.

3.12.2 La procédure de chiffrement à l'aide de la clé publique de Bob suit les étapes suivantes

Génération des 3 parties qui nous serviront à reconstituer la clé K : Comme expliqué plus haut lors de la description de l'algorithme de Shamir, nous allons créer un schéma de partage de type (2, 3) où 2 représente le nombre minimal de pièces du puzzle à avoir pour reconstituer le secret. Et 3 présente le nombre de parties que l'on va créer à partir de notre secret :

John va choisir (2-1) =1 coefficients et poser ao=k (ou k est de la clé de chiffrement symétrique de John)." ensuite John construit le polynôme f(x)=k+$a_1 x$.

John a presque fini. Comme expliqué plus haut lors de la présentation de l'algorithme, chacune des personnes de confiance sélectionnées par John se verra attribuer l'un des points par lesquels passe la courbe correspondant au polynôme F(X)=k+a1x). En d'autres termes, chacun se verra attribuer un couple d'antécédent et de l'image correspondant de la fonction polynomiale.

L'administrateur du système se verra également attribuer un troisième couple. Une cela effectuer, le secret est partagé entre Alice, Rachelle et l'administrateur.

Enfin John va chiffrer l'ensemble de ses données médicales à l'aide de la fonction de chiffrement symétrique et les transmettre au stockage dans un cloud décentralisé de type et IPFS par exemple.

3.12.3 Inscription d'un utilisateur de type personnel médical :

Lors de cette inscription, après avoir fourni les données nécessaires, le membre du staff médical va générer à l'aide de G( ) une paire de clés secrète/publique (PK,SK).

3.12.4 Procédure d'autorisation d'accès en lecture et en écriture

Dans cette sous section, nous allons présenter la partie du Protocole dans laquelle John accorde un droit d'accès à Bob son médecin, pour la lecture et l'écriture, nous n'allons pas aborder la partie lecture seule, parce qu'elle est incluse dans celle-ci.

John arrive chez Bob pour effectuer une consultation. Cette consultation peut s'effectuer dans un hôpital, un cabinet médical, ou tout endroit connecté à internet. Bob demande l'accès à

une partie des dossiers de John. Par exemple, ses analyses de test sanguin. John reçoit la notification, il lui accorde l'accès.

- Accorder l'accès s'effectue de la façon suivante :
- John télécharge les données (c) demandées depuis le cloud.
- Il utilise sa clé de chiffrement symétrique pour les déchiffrement : m←D(c ,k).
- Ensuite il va chiffrer les données qui sont à présent en clair à l'aide la clé publique de Bob.
- La procédure de chiffrement à l'aide de la clé publique de Bob suit les étapes suivantes :
- John va générer aléatoirement une valeur "x" d'une taille de plus de 128 bits. (Encore une fois de nombreux générateurs aléatoires sont communs et peuvent être utilisés).
- John calcule y←F(pk bob, x) où F est un fonction TDF, par exemple la fonction RSA. Et p_{kbob} est la clé publique de Bob.
- John calcule : K← H(x) où H est une fonction de hachage cryptographique (par exemple SHA-256 ou SHA-3).
- John calcule C2 ← ES(Ks,m) où ES est un algorithme de chiffrement symétrique par exemple AES- 256.
- Enfin John envoie sur la blockchain la paire (y,c).
- La pair (y,c) est visible pour tous les nœuds de la blockchain mais seul Bob est en mesure de la déchiffrer.
- Bob va alors recevoir la paire(y, c).
- Il va calculer X← (S_k,YF^{-1}) "F^{-1}" et l'inverse de la fonction à porte dérobée. (voir section chiffrement asymétrique)
- Bob calculerK←H(x).

- Bob calculer m← Ds ($\boldsymbol{K_S}$,c), où Ds est à la fonction de déchiffrement de l'algorithme symétrique.
- Maintenant, Bob Voit le données “m” en clair et il peut consulter librement Les données :
- Dans le cas où Bob n'a accès qu’en lecture, le protocole s'arrête ici.
- Dans le cas où Bob à accès en écriture, il peut modifier les données à l’aide des mêmes étapes qu'à suivi John pour le chiffrement asymétrique avant de les transmettre à Bob (bien sûr, il va utiliser la clé publique de John). Et ensuite il transmettra à l’aide de la blockChain, le dossier ainsi chiffré.
- À la réception, John va déchiffrer les données avec les mêmes étapes, suivi par Bob lors de la transmission initiale. Et ensuite, il fera appel une dernière fois à sa clé de chiffrement secrète K pour le chiffrer une dernière fois avant de le remettre dans le cloud.

3.12.5 **Description du protocole de récupération de clé secrète :**

Dans les cas d’urgence, quand John est trop malade pour autoriser les accès ou encore s’il perd sa clé secrète (dans ce cas sans procédure de récupération, personne ne pourra lui retrouver sa clé)

- L’administrateur du système peut initier une procédure de récupération: (Rappelons que l’administrateur et lui-même en possession d’un couple (antécédent, image) par lequel passe la droite constituée par le polynôme généré par John lors de son inscription initiale.
- Supposons que Bob à fait la requête d’une procédure de récupération suite à l’admission aux urgences de John . L’administrateur reçoit la requête et contactes par des moyens rapides Rachelle et Alice (les personnes de confiance désignées par John.)
- La première à répondre, va coupler sa pièce du puzzle avec celle de l’administrateur afin de récupérer la clé de chiffrement et permettre d’effectuer les soins nécessaires à John.

3.13 Discussion de notre proposition de solution

Nous allons dans cette avant dernière section du chapitre discuter notre proposition de protocole d'accès décentralisé aux données médicales.

Comme nous l'avons mentionné dans la section 2.3.3, les Exigences de base pour le partage et la protection des données médicales sont les suivantes : la sécurité et la protection de la vie privée, l'accès aux données sous réserve d'autorisation du patient doit être garantie. Les données doivent être contrôlées pas le patient et enfin, le protocole doit suivre une norme unifiée.

Le protocole que nous avons conçu répond aux trois premiers critères et peut répondre au dernier. En ce qui concerne l'utilisation d'une norme unifiée, cela n'aura aucun impact sur notre protocole.

3.13.1 Sécurité et protection de la vie privée : Notre protocole utilise un chiffrement extrêmement

Fort. AES-256 est la version la plus forte du standard et elle est à ce jour inviolable. Sa sécurité repose sur le caractère secret de la clé de chiffrement. Il existe de nombreuses méthodes reconnues et utilisées dans la gestion des clés secrètes. Nous n'allons pas traiter l'aspect de gestion de ces clés secrète parce qu'il est hors de propos en ce qui concerne notre thème. En Résumé, AES-256 garanti un très haut degré de confidentialité et le respect du caractère secret des données médicales.

- **Accès aux données :** Les patients sont les seuls maitres de leurs données. Nous avons mis l'accent sur cet aspect lors de la conception de notre solution. Personne ne peut accéder aux données du patient sans l'autorisation expresse de celui-ci. Une fois autorisé, l'accès est garanti.
- **Contrôle des données :** Grace au model que nous avons proposé, les patients sont en mesure de contrôler les données qu'ils vont divulguer à leur médecin, ceci leur permettra de masquer certaines informations qui ne sont pas pertinente à l'instant T.

Enfin, lors de notre recherche bibliographique, nous avons pu constater que la plupart des systèmes de contrôle d'accès décentralisés proposés, ne présentaient pas de système de récupération d'urgence de clé secrète de chiffrement. Et ceux qui en mentionnaient le fait qu'il

en fallait un ne détaillaient comment nous pourrions procéder. A notre connaissance, nous sommes les premiers à présenter un système de contrôle d'accès décentralisé pour des données médicales, dans lequel le patient est au centre du système, le seul propriétaire et gestionnaire de ses données, mais en même temps en cas d'urgence, les secours seront en mesure de lui apporter les soins nécessaires. Ceci est notre contribution principale et ceci est également très important dans le cadre d'un système qui veut garantir que le patient soit seul maitre de ses données, mais en même temps, vu le caractère particulier de certaines situations (cas d'urgence, ou perte de clé de chiffrement par le patient par exemple) cette fonctionnalité permettra de garder le système fonctionnel (car il est infaisable de retrouver la clé de chiffrement autrement), et en même temps totalement sécurisé et décentralisé.

3.14Conclusion

Les services de santé sont soumis à des règles de confidentialité particulièrement strictes, ce qui les distingue des autres services. La blockchain, pour jouer un rôle efficace dans ce domaine, doit garantir en priorité la protection et l'anonymat des données des patients. Elle doit également garantir que le patient est seul maitre de ces données. Notre proposition de solution au problème de contrôle d'accès aux données médicales des patients dans les systèmes de e-santé vise à répondre à cette exigence cruciale. Dans le prochain chapitre, nous explorerons les détails de l'implémentation de notre proposition et discuterons des différentes facettes de notre approche. En intégrant des mécanismes de sécurité robustes et en assurant la transparence et la disponibilité des données, notre solution vise à renforcer la confiance des patients dans la gestion de leurs informations médicales tout en facilitant l'accès aux professionnels de santé autorisés.

Chapitre 4
Réalisation d’un prototype d'application

4.1 Introduction

Dans ce chapitre, nous nous consacrerons à la réalisation et à la mise en œuvre de notre preuve de concept de protocole de gestion d’accès des données personnelles et médicales à l'aide de la blockchain. Nous allons présenter les outils de développement adoptés : la Blockchain Ganache (pour les clés privées et les adresses), XAMPP, le langage de programmation PHP, le framework Bootstrap ainsi que l'environnement de développement Sublime Text. Enfin, nous présenterons les interfaces utilisateur. Le coeur de notre travail consiste en la conception et l’implémentation d’un système décentralisé de gestion d’accès aux données médicales. Lors de la conception de ce protoype d’application, nous n’avons pas implémenté la partie cloud décentralisé, Cette partie constitue une continuité potentielle pour des futures étudiants.

4.2 Outils de développement

Les outils de développement essentiels pour créer une D’App incluent la Blockchain Ganache, les langages de programmation Solidité et JavaScript, ainsi que l'environnement de développement Visual studio code, truffle et Meta Mask (une extension de navigateur Web Ethérée qui agit comme un portefeuille Ethereum et une interface pour les D’Apps basées sur Ethereum).

4.2.1 Généralités sur Ethereum

L'Ethereum est une plateforme de blockchain open-source et décentralisée qui permet la création d'applications décentralisées (d’Apps) et de contrats intelligents. Lancée en 2015, Ethereum est la deuxième crypto monnaie en termes de capitalisation boursière, juste derrière le Bitcoin. La monnaie native de Ethereum est l'Éther (ET), qui sert à faciliter les transactions et à rémunérer les validateurs et les développeurs pour leurs contributions au réseau [47].

4.2.2 **Solidity**

Solidity est un langage de programmation de haut niveau pour la création de contrats intelligents (ou smart contracts) sur la blockchain Ethereum. Les contrats intelligents sont des contrats à exécution automatique qui automatisent l'échange d'actifs entre des parties. La particularité est qu'aucun intermédiaire n'est requis pour assurer le respect de ce contrat.

Solidity a été spécialement conçu pour la création d'applications décentralisées, d'App (« applications distribuées »), qui sont exploitées sur des machines virtuelles Ethereum (EVM). Les contrats intelligents conviennent notamment pour la gestion des actifs numériques, la création de marchés boursiers décentralisés et la mise en œuvre de systèmes de vote [48].

Figure 24- Logo Solidity.

4.2.3 **Xampp**

XAMPP est une distribution de logiciels serveur, c'est à dire qu'il s'agit d'un regroupement de logiciels, installables en une fois, permettant de constituer un serveur local.

L'installation de XAMPP permet donc grâce à divers logiciels de travailler sur un site internet dynamique directement sur son ordinateur [49]**.**

4.3 4.2.4 Ganache

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

Ganache est disponible en deux versions : une interface utilisateur et une CLI. Ganache UI est une application de bureau prenant en charge la technologie Ethereum et File coin. Notre outil de ligne de commande plus robuste, ganache, est disponible pour le développement de Ethereum [50]**.**

Figure 25- : Logo Ganache.

4.3.1 JavaScript

JavaScript est un langage informatique utilisé sur les pages web. Ce langage a la particularité de s'activer sur le poste client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition à d'autres langages qui sont activés côté serveur.

Figure 26- Logo JavaScript.

4.3.2 Truffle

Truffle est un Framework de développement Ethereum (créé par Consensus, l'entreprise co-fondée par Vitalik Buterin). Il permet d'interfacer des smart contracts avec du code JavaScript et l'ensemble de l'écosystème NodeJS. Cela ouvre donc la voie à l'utilisation des outils d'industrialisation du monde JavaScript pour la chaîne de blocs Ethereum.

Truffle apporte les fonctionnalités suivantes :

- **Gestion des dépendances (au travers de NPM ou EthPM – le package manager Ethereum de smart contracts)**
- **Compilation des contrats**
- **Migrations**
- **Tests (2 modes possibles)[51].**

4.3.3 Node.js

Node.js est un environnement d'exécution JavaScript gratuit, open-source et multiplateforme qui permet aux développeurs de créer des serveurs, des applications web, des outils en ligne de commande et des scripts[52].

4.3.4 Langage PHP

PHP (acronyme récursif de PHP : HyperText Préprocesseur) est un langage de script open source à usage général largement utilisé, particulièrement adapté au développement Web et pouvant être intégré au HTML.

4.4 Environnement de développement

4.4.1 Visual Studio Code

Visual Studio Code est un éditeur de code source léger mais puissant qui s'exécute sur votre bureau et est disponible pour Windows, MacOs et Linux. Il est livré avec une prise en charge intégrée de JavaScript, Type Script et Node.js et dispose d'un riche écosystème d'extensions pour d'autres langages et environnements d'exécution (tels que C++, C#, Java, Python, PHP, Go, .NET)[53].Il intègre plusieurs outils facilitant

la saisie de code par les développeurs comme la coloration syntaxique ou encore le système d'auto-complétions IntelliSense. En outre, l'outil permet aux développeurs de corriger leur code et de gérer les différentes versions de leurs fichiers de travail puisqu'un module de débogage est aussi de la partie. La **figure 27** ci-dessous représente son interface.

Figure 27 - Logo Visual Studio Code.

4.4.2 MetaMask

MetaMask est une extension de navigateur qui permet aux utilisateurs d'interagir avec des applications décentralisées (DApps) construites sur la blockchain Ethereum. Elle agit comme un portefeuille numérique, permettant aux utilisateurs de gérer leurs comptes Ethereum et d'effectuer des transactions en utilisant des contrats intelligents.

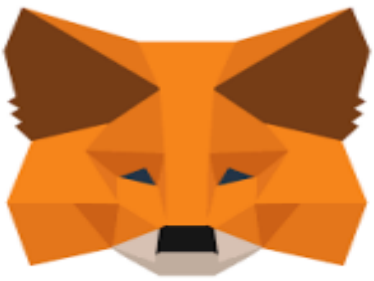

Figure 28-Logo MetaMask.

4.5 Outil de gestion de la bibliographie

4.5.1 Zotero

Zotero est un logiciel libre et open-source de gestion de références bibliographiques et de recherches. Conçu pour aider les chercheurs, étudiants et professionnels à organiser et gérer leurs sources d'information, Zotero permet de collecter, organiser, citer et partager les références bibliographiques de manière efficace[54].

4.6 Organigrammes de l'application

4.4.1 Interfaces d'authentification

L'interface illustrée dans la figure 29 ci-dessous montre le processus par lequel un patient médecin et au admin d'accéder à la page d'accueil

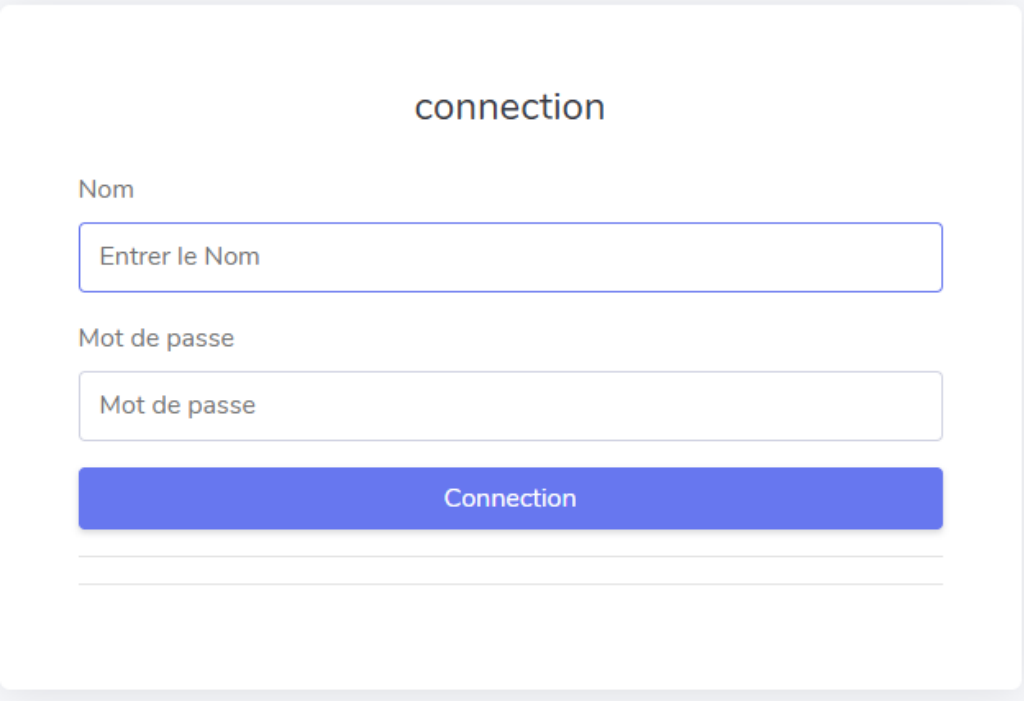

Figure 29-Interface principale de l'application.

4.6.1 L’interface de patient pour la permission

L'interface illustrée dans la figure 30 ci-dessous montre le processus par lequel un patient de donner la permission au médecin pour consulter leur dossier ou pour consulter et diagnostiquer grâce à cette interface.

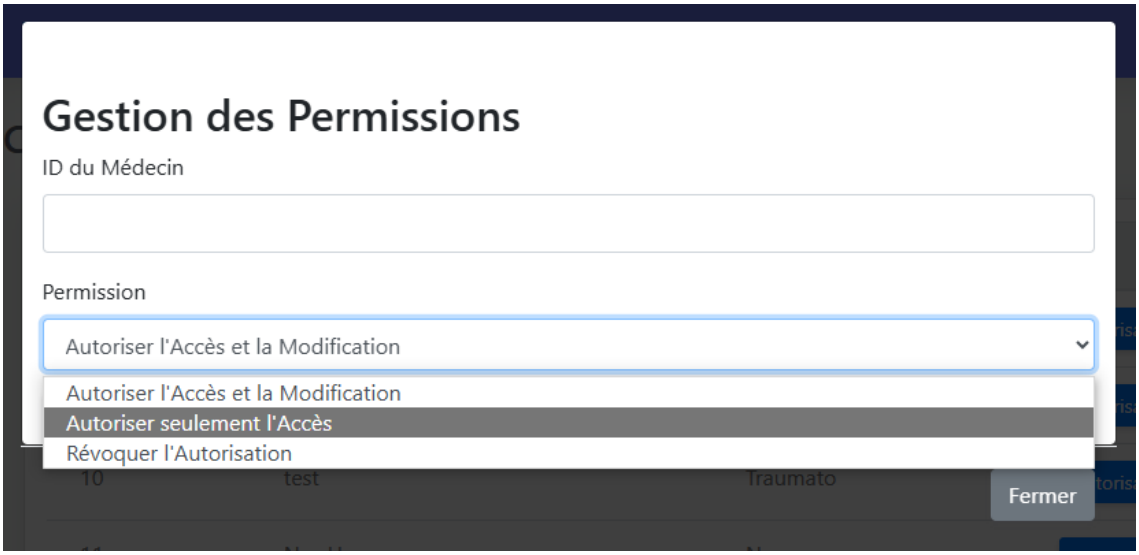

Figure 30 – l’interface de patient pour la permission

4.6.2 Interface de Délégation des Clés en Cas d'Urgence

4.6.3Interface de Délégation des Clés en Cas d'Urgence

L'interface illustrée dans la figure 31 ci-dessous montre le processus par lequel un patient de désigner trois personnes de confiance pour accéder à son compte en cas d'urgence. L'une de ces personnes est l'administrateur, et les deux autres peuvent être des proches, comme un membre de la famille ou un ami. Le patient fournit les clés publiques de ces trois personnes.

En cas d'urgence où le patient est inconscient, deux des trois personnes désignées peuvent utiliser leurs clés pour accéder aux informations médicales du patient et gérer son compte. Cette fonctionnalité garantit que des décisions médicales cruciales peuvent être prises rapidement

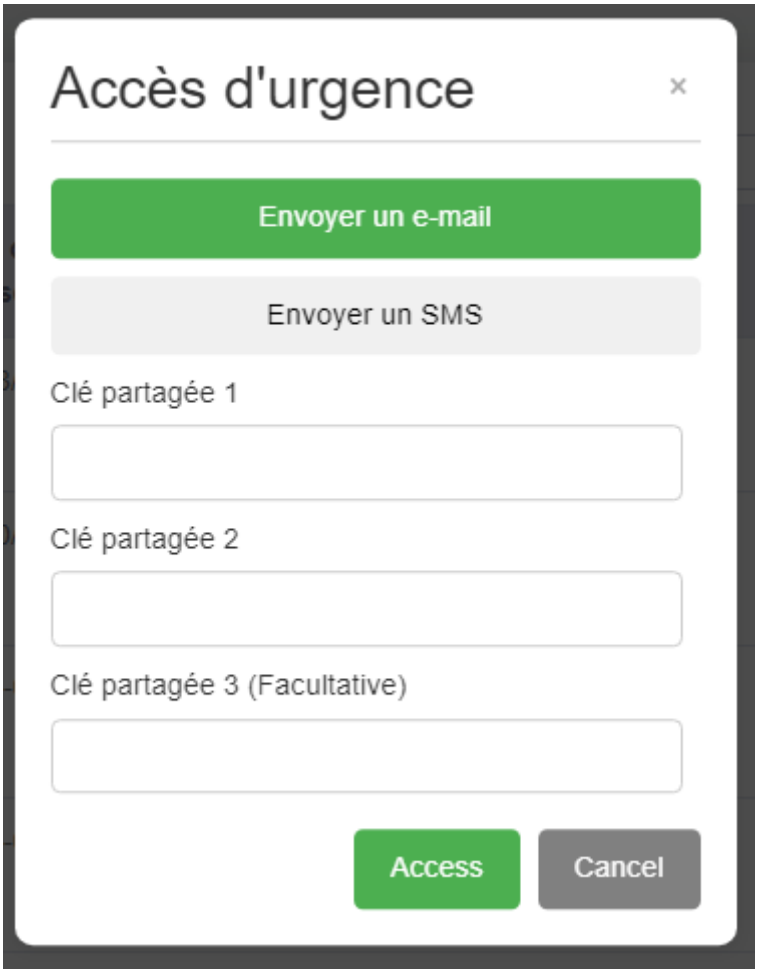

Figure 31-Interface de Délégation des Clés en Cas d'Urgence

4.6.4 L'interface d'ajout d'un patient par l'administrateur

L'interface illustrée dans la figure 32 ci-dessous montre le processus par lequel un administrateur enregistre un nouveau patient dans le système. (Interface d'Ajout d'un Patient par l'Administrateur).

Cette interface permet à l'administrateur d'enregistrer de nouveaux patients dans le système. L'admin remplit un formulaire avec les informations personnelles du patient, telles que le nom, la date de naissance, l'adresse, et les coordonnées de contact. Une fois ces informations saisies et validées, elles sont stockées dans la base de données.

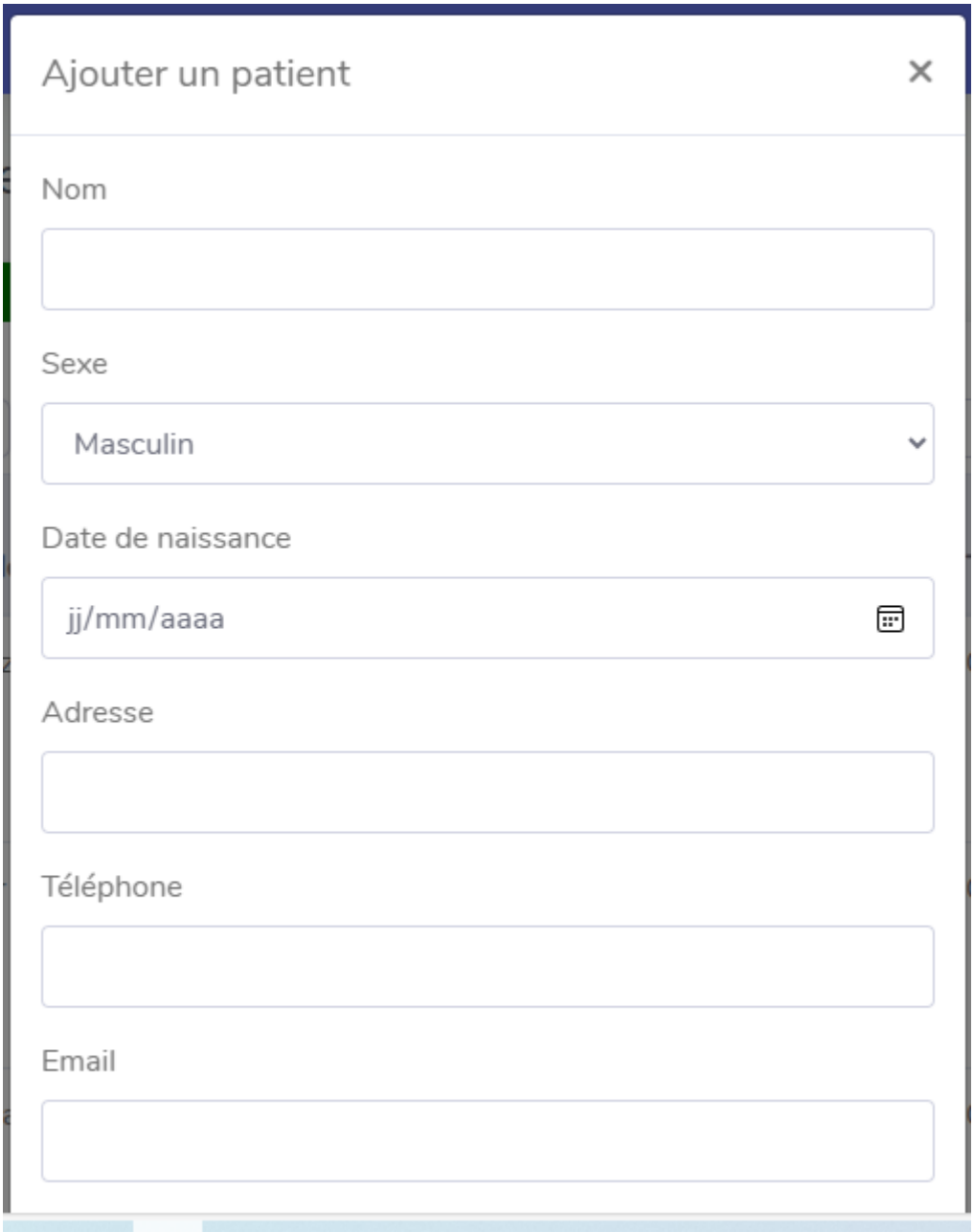

Figure 32 – l'interface d'ajout d'un patient par l'admin

4.7 SmartContrast

> xampp > htdocs > hospital > contracts > Migrations.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Migrations {
    address public owner;
    uint public last_completed_migration;

    constructor() {
        owner = msg.sender;
    }

    modifier restricted() {
        require(msg.sender == owner, "This function is restricted to the contract's owner");
        _;
    }

    function setCompleted(uint completed) public restricted {
        last_completed_migration = completed;
    }

    function upgrade(address new_address) public restricted {
        Migrations upgraded = Migrations(new_address);
        upgraded.setCompleted(last_completed_migration);
    }
}
```

Figure 33 – Interface montre une des smartContrat

4.8 Conclusion

Dans cette dernière partie, nous avons présenté la réalisation et l'implémentation de notre projet, en spécifiant nos choix d'outils, de langages et d'environnements de développement adoptés pour créer notre application.

Nous avons également abordé la problématique de la gestion du contrôle d'accès aux données médicales en utilisant la technologie blockchain. Pour répondre à cette problématique, nous avons proposé une solution visant à assurer la sécurité du partage des informations des patients entre les différents acteurs du système de santé. Cette solution repose sur l'utilisation de smart contracts et représente une avancée significative dans la protection des données médicales, répondant aux exigences de sécurité et de confidentialité indispensables dans ce

domaine. Le déploiement réussi de notre smart contract sur un réseau de test confirme l'efficacité et la faisabilité de notre approche pour une application à grande échelle.

Conclusion Générale

Pour conclure, la technologie blockchain reste un domaine très récent qui a néanmoins ouvert la porte à d'autres champs de recherche et d'exploitation des techniques cryptographiques qui se limitait auparavant à l'assurance de la sécurité des échanges sur le grand réseau web.

La digitalisation du secteur médical est une étape cruciale et essentielle pour optimiser la gestion, valoriser et améliorer la qualité, la sécurité ainsi que la prise en charge des patients, ce qui renforcera leur confiance dans le système de santé. Dans cette optique, notre travail a consisté à étudier la technologie Blockchain, les smart contracts et la plateforme Ethereum, puis à développer un système de contrôle d'accès visant à sécuriser les soins et à faciliter le partage de l'information entre les acteurs de ce système.

L'architecture de controle d'accès que nous avons conçu est complétement décentralisée : le réseau fonctionne en peer-to-peer et les données sont décentralisées. Nous avons conçu un smart contrat sur la plateforme Ethereum, garantissant la protection des données des patients et définissant les règles d'accès à ces informations selon certains critères.

L'architecture de controle d'accès que nous avons développé est basé sur un controle total par le patient. Ceci signifie que le patient est propriaitaire de ses données et que seul lui peut autoriser quelqu'un à consulter ou modifier les données. Cependant, Nous avons laissé la possibilité au patient de partager sa clé de chiffrement avec des personnes de confiance, afin que les accès dans des situations d'urgence soient permis. Le partage de ces clé est sans risque de divulgation de données confidentielles, puisque ces personnes de confiances doivent se réunir afin de reconstituer la clé de chiffrement. Ceci est notre principale contribution et constitue à notre connaissance la première implémentation concrète d'un tel schéma dans le domaine de la gestion des controles d'accès aux données médicales de façon décentralisé et

basé sur la blokchcain.

En conclusion, nous constatons que la recherche sur les applications de la blockchain en est encore à ses débuts. Cependant, nous estimons qu'elle pourrait apporter des bénéfices considérables à la société dans les années à venir.

Bibliographie

[1] « bitcoin-and-cryptocurrency-technologies ». Consulté le: 20 mars 2024. [En ligne]. Disponible sur: https://pdfdirectory.com/pdf/0765-bitcoin-and-cryptocurrency-technologies.pdf

[2] E. Academy, « Expliquez le concept de résistance aux pré-images dans les fonctions de hachage. - Académie EITCA », EITCA Academy. Consulté le: 6 mai 2024. [En ligne]. Disponible sur: https://fr.eitca.org/la-cyber-s%C3%A9curit%C3%A9/eitc-est-une-cryptographie-classique-avanc%C3%A9e/fonctions-de-hachage/introduction-aux-fonctions-de-hachage/r%C3%A9vision-de-l%27examen-introduction-aux-fonctions-de-hachage/expliquer-le-concept-de-r%C3%A9sistance-aux-pr%C3%A9-images-dans-les-fonctions-de-hachage/

[3] S. de Quénetain, « L'arbre de Merkle: la Colonne Vertébrale de la Blockchain », Blockchains Expert. Consulté le: 6 mai 2024. [En ligne]. Disponible sur: https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/

[4] S. de Quénetain, « L'arbre de Merkle: la Colonne Vertébrale de la Blockchain », Blockchains Expert. Consulté le: 6 mai 2024. [En ligne]. Disponible sur: https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/

[5] « Qu'est-ce qu'une chaîne de blocs (blockchain) ? » Consulté le: 30 avril 2024. [En ligne]. Disponible sur: https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

[6] « La-blockchain-decryptee-le-s-clefs-dune-revolution.pdf ». Consulté le: 30 avril 2024. [En ligne]. Disponible sur: https://www.fg2a.com/wp-content/uploads/2017/01/La-blockchain-decryptee-le-s-clefs-dune-revolution.pdf

[7] « Comment fonctionne la blockchain ? », CoinJournal. Consulté le: 6 mai 2024. [En ligne]. Disponible sur: https://coinjournal.net/fr/crypto-monnaies/apprendre/blockchain/

[8] johan.puisais, « La Blockchain : 900 mots pour tout comprendre », Formations et certifications Cloud, SIAM, Qualité - Valnaos. Consulté le: 7 mai 2024. [En ligne]. Disponible sur: https://www.valnaos.com/la-blockchain-900-mots-pour-tout-comprendre/

[9] gdar8, « Comment fonctionne la crypto monnaie ? - Bourse Apprentissage ». Consulté le: 7 mai 2024. [En ligne]. Disponible sur: https://www.bourse-apprentissage.com/comment-fonctionne-la-crypto-monnaie/

[10] « NIST FIPS 186-2 Digital Signature Standard (DSS), 2000-01 (with Change Notice from 2001-10).pdf ». Consulté le: 8 mai 2024. [En ligne]. Disponible sur: https://csrc.nist.rip/library/NIST%20FIPS%20186-2%20Digital%20Signature%20Standard%20(DSS),%202000-01%20(with%20Change%20Notice%20from%202001-10).pdf

[11] I. Yahia, « Système de blockchain hiérarchique et authentification légère pour un réseau

V2G sécurisé », PhD Thesis, Université du Québec à Trois-Rivières, 2022. Consulté le: 26 mai 2024. [En ligne]. Disponible sur: https://depot-e.uqtr.ca/id/eprint/10563/1/eprint10563.pdf
[12] O. Ayadi, « CHAPITRE III : État de l'art de la Blockchain », 2019.
[13] R. Bouvet, « La consommation d'énergie de la blockchain Ethereum va diminuer de 99% grâce au Proof-of-Stake et à ETH 2.0 », Clubic.com. Consulté le: 7 mai 2024. [En ligne]. Disponible sur: https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-372300-la-consommation-d-energie-de-la-blockchain-ethereum-va-diminuer-de-99-grace-au-proof-of-stake-et-a-eth-2-0.html
[14] D. Yaga, P. Mell, N. Roby, et K. Scarfone, « Blockchain Technology Overview », oct. 2018. doi: 10.6028/NIST.IR.8202.
[15] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, et A. Faxvaag, « Blockchain in healthcare and health sciences—A scoping review », *Int. J. Med. Inf.*, vol. 134, p. 104040, févr. 2020, doi: 10.1016/j.ijmedinf.2019.104040.
[16] P. Waelbroeck, « Les enjeux économiques de la blockchain », *Ann. Mines - Réal. Ind.*, vol. Août 2017, n° 3, p. 10-19, 2017, doi: 10.3917/rindu1.173.0010.
[17] « Blockchain Privées, Publiques et à Consortium — Quelles sont les différences ? », Binance Academy. Consulté le: 8 mai 2024. [En ligne]. Disponible sur: https://academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference
[18] « Blockchain-pour-les-systemes-cyber-physiques-Defis-et-applications ». Consulté le: 25 mars 2024. [En ligne]. Disponible sur: https://www.researchgate.net/profile/Maleh-Yassine/publication/377111048_Blockchain_pour_les_systemes_cyber-physiques_Defis_et_applications/links/6595beff2468df72d3f947e9/Blockchain-pour-les-systemes-cyber-physiques-Defis-et-applications.pdf
[19] M. E. Hasnia et Z. N. Elhouda, « Pour l'Obtention du Diplôme de Master en Informatique Option : Ingénierie des Systèmes d'Information Présenté par : ».
[20] « Formalizing and Securing Relationships on Public Networks | First Monday ». Consulté le: 25 mai 2024. [En ligne]. Disponible sur: https://firstmonday.org/ojs/index.php/fm/article/view/548
[21] M. Sookhak, M. R. Jabbarpour, N. S. Safa, et F. R. Yu, « Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues », *J. Netw. Comput. Appl.*, vol. 178, p. 102950, mars 2021, doi: 10.1016/j.jnca.2020.102950.
[22] A. Azaria, A. Ekblaw, T. Vieira, et A. Lippman, « MedRec: Using Blockchain for Medical Data Access and Permission Management », in *2016 2nd International Conference on Open and Big Data (OBD)*, août 2016, p. 25-30. doi: 10.1109/OBD.2016.11.
[23] « MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain | IEEE Journals & Magazine | IEEE Xplore ». Consulté le: 25 mai 2024. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/9547814
[24] « Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research ». Consulté le: 21 avril 2024. [En ligne]. Disponible sur: https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/11-74-

ablockchainforhealthcare.pdf
[25] « Data Lake : définition et guide définitif », Talend - A Leader in Data Integration & Data Integrity. Consulté le: 10 mai 2024. [En ligne]. Disponible sur: https://www.talend.com/fr/resources/guide-data-lake/
[26] L. A. Linn et M. B. Koo, « Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research ».
[27] jeanluc, « Les 4 critères fondamentaux de la sécurité de l'information – Info-Attitude ». Consulté le: 16 mai 2024. [En ligne]. Disponible sur: http://info-attitude.com/4-criteres-fondamentaux-securite-information/
[28] « A Blockchain-Based Medical Data Sharing and Protection Scheme | IEEE Journals & Magazine | IEEE Xplore ». Consulté le: 23 avril 2024. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/8813031
[29] « 2015 Edition | HealthIT.gov ». Consulté le: 5 mai 2024. [En ligne]. Disponible sur: https://www.healthit.gov/topic/certification-ehrs/2015-edition
[30] X. Yue, H. Wang, D. Jin, M. Li, et W. Jiang, « Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control », *J. Med. Syst.*, vol. 40, n° 10, p. 218, août 2016, doi: 10.1007/s10916-016-0574-6.
[31] E. Hendrick, B. Schooley, et C. Gao, « CloudHealth: Developing a reliable cloud platform for healthcare applications », in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, janv. 2013, p. 887-891. doi: 10.1109/CCNC.2013.6488579.
[32] « CRHIS | Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance ». Consulté le: 5 mai 2024. [En ligne]. Disponible sur: https://dl.acm.org/doi/abs/10.1145/2463728.2463805
[33] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, et G. S. Salvador, « A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions », in *2010 Second International Conference on eHealth, Telemedicine, and Social Medicine*, févr. 2010, p. 95-99. doi: 10.1109/eTELEMED.2010.19.
[34] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, et A. Alamri, « Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data », *IEEE Syst. J.*, vol. 11, n° 1, p. 88-95, mars 2017, doi: 10.1109/JSYST.2015.2460747.
[35] M. Barua, X. Liang, R. Lu, et X. Shen, « ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing », *Int. J. Secur. Netw.*, vol. 6, n° 2-3, p. 67-76, janv. 2011, doi: 10.1504/IJSN.2011.043666.
[36] S. Narayan, M. Gagné, et R. Safavi-Naini, « Privacy preserving EHR system using attribute-based infrastructure », in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, in CCSW '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 47-52. doi: 10.1145/1866835.1866845.
[37] L. Chen et D. B. Hoang, « Novel Data Protection Model in Healthcare Cloud », in *Proceedings of the 2011 IEEE International Conference on High Performance Computing and Communications*, in HPCC '11. USA: IEEE Computer Society, 2011, p. 550-555. doi: 10.1109/HPCC.2011.148.
[38] « An open system to manage data without a central server », IPFS. Consulté le: 25 mai 2024. [En ligne]. Disponible sur: https://ipfs.tech

[39] « Cryptographie - Wikiwand ». Consulté le: 26 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Cryptographie
[40] « Adi Shamir - Wikiwand ». Consulté le: 26 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Adi_Shamir
[41] « Secret réparti - Wikiwand ». Consulté le: 26 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Secret_r%C3%A9parti
[42] « Wikiwand - Partage de clé secrète de Shamir », Wikiwand. Consulté le: 25 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Partage_de_clé_secrète_de_Shamir
[43] « Courbe cubique - Wikiwand ». Consulté le: 27 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Courbe_cubique
[44] « Fonction polynomiale - Wikiwand ». Consulté le: 26 mai 2024. [En ligne]. Disponible sur: https://www.wikiwand.com/fr/Fonction_polynomiale
[45] A. Shamir, « How to share a secret », *Commun. ACM*, vol. 22, nº 11, p. 612-613, nov. 1979, doi: 10.1145/359168.359176.
[46] H. H. Kung, Y.-F. Cheng, H.-A. Lee, et C.-Y. Hsu, « Personal Health Record in FHIR Format Based on Blockchain Architecture », in *Frontier Computing*, J. C. Hung, N. Y. Yen, et J.-W. Chang, Éd., Singapore: Springer, 2020, p. 1776-1788. doi: 10.1007/978-981-15-3250-4_237.
[47] « Ethereum (ETH) : Qu'est-ce que c'est, comment ça fonctionne et comment en acheter ? », Coin Academy. Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://coinacademy.fr/ethereum-eth-fondamental/
[48] « Solidity : le langage de programmation pour les contrats intelligents », IONOS Digital Guide. Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://www.ionos.fr/digitalguide/sites-internet/developpement-web/solidity/
[49] « XAMPP — Documentation Design et Édition Numérique 2020-12-10--103343 ». Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://enseignement.leomartin.net/upem/2020-2021/documentations/xampp/index.html
[50] « Ganache | Présentation - Suite Truffes ». Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://archive.trufflesuite.com/docs/ganache/
[51] « Industrialisation de smart contracts avec Truffle », Ekino FR. Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://www.ekino.fr/publications/industrialisation-de-smart-contracts-avec-truffle/
[52] « Node.js — Run JavaScript Everywhere ». Consulté le: 25 mai 2024. [En ligne]. Disponible sur: https://nodejs.org/en
[53] « Documentation for Visual Studio Code ». Consulté le: 22 mai 2024. [En ligne]. Disponible sur: https://code.visualstudio.com/docs
[54] « Zotero | Your personal research assistant ». Consulté le: 31 mai 2024. [En ligne].