République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Khider – BISKRA

Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie

Département d'informatique

N d'ordre :Rtic14/M2/2021

Mémoire

Présenté pour le diplôme de master académique en

Informatique

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

Les dossiers médicaux sur Blockchain.

Par : **Rahmani Rokia**

Soutenu le ../../2021 devant le jury composé de :

Mr. Belaiche Hamza , Président , Examinateur

Année universitaire 2020-2021

Dédicaces

Ce travail est dédié à :

Au meilleur des pères.

A ma très chère maman Qu'ils trouvent en moi la source de leur fierté A qui je dois tout.

A mes frères : Yougharta ,Yakob, Youcef, Ilias.

A ma tante Hadjer et son mari AbdelBaki .

A mon fiancé ,et à tous ceux que j'aime et chéris.

Remerciements

Tout d'abord, je voudrais montrer ma gratitude et mes louanges à Dieu tout-puissant pour m'avoir donné la force, les connaissances, la capacité et l'opportunité de relever ce défi et de persévérer et le compléter de manière satisfaisante.

je tiens à exprimer ma sincère gratitude à mon ecadreur Monsieur Beliache Hamza pour ses précieux conseils.

Je tiens également à remercier les membres du jury pour leurs efforts d'évaluation de ce travail.

Et enfin, je souhaite exprimer ma plus profonde gratitude à mes camarades de classe et à l'équipe académique du département pour leur aide apportée tout au long de ma carrière académique.

Résumé

Blockchain est une base de données partagée qui permet de créer la confiance entre individus sans tiers. L'architecture est ici décentralisée, en En d'autres termes, les données sont réparties entre les utilisateurs et, par conséquent, les informations ne peuvent jamais être effacé. Ainsi, parmi les secteurs porteurs de cette technologie (on entend Blockchain), on précise le secteur de la santé, car il est vraiment très sensible puisqu'il recommande de partager les informations des patients et leurs données de santé. Dans ce contexte, le l'objectif de ce projet est de proposer une approche Blockchain dans le domaine médical, qui vise à gérer les données de santé à l'aide de dossiers médicaux électroniques.

Mot clés : Blockchain,Confiance,Santé

Table des matières

Table des figures

Introduction générale

Des données médicales précises et complètes sont un atout précieux pour les patients. La protection de la vie privée et le stockage sécurisé des données médicales sont des questions cruciales lors des services médicaux. Le stockage sécurisé et la pleine utilisation des dossiers médicaux personnels ont toujours été une préoccupation pour la population en général. L'émergence de la technologie blockchain apporte une nouvelle idée pour résoudre ce problème. En tant que chaîne de hachage avec les caractéristiques de décentralisation, de vérifiabilité et d'immuabilité, la technologie blockchain peut être utilisée pour stocker en toute sécurité des données médicales personnelles. Dans cet article, nous concevons un schéma de stockage pour gérer les données médicales personnelles basé sur la blockchain. En outre, un cadre de service pour le partage de dossiers médicaux est décrit. De plus, les caractéristiques de la blockchain médicale sont présentées et analysées à travers une comparaison avec les systèmes traditionnels. Le schéma de stockage et de partage proposé ne dépend d'aucun tiers et aucune partie n'a le pouvoir absolu d'affecter le traitement.

Ce rapport se définit sur trois chapitres :

Le chapitre 1 introduit le concept du Blockchain, les cryptomonnaies, les caractéristiques de la blockchain, et déférente définitions sur déférente concept de base.

Le deuxième chapitre présent les bases sur les techniques utilisé par la blockchain,l' architecture, ainsi le système Blockchain.

Le troisième chapitre présente l'analyse conceptuelle de la solution proposée.

Dans le dernier chapitre, nous allons détailler la réalisation de la solution proposée. On a terminé ce mémoire par une conclusion générale.

Chapitre 1

La technologie Blockchain

1.1 Iintroduction

En 2019 pas une semaine ne s'écoule sans que l'on entende parler de la blockchain dans les méditas ou même au bistrot ! Il est vrai que le mot « blockchain » est sur toutes les lèvres mais pourtant peu de personnes comprennent véritablement l'enjeu de cette technologie comment elle peut être utilisée pour réaliser des transactions financières, faire des ICO (Initial coins offering), transférer des informations de manière fiable, vérifiée et sécurisée. Les crypto-monnaies en particulier Bitcoin et ethereum sont des exemples les plus populaires qui sont liés intrinsèquement a la technologie blockchain. Il est aussi le plus controversé, car il contribue à permettre à un marché mondial de plusieurs milliards de dollarsdes transactions anonymes sans aucun contrôle gouvernemental.

1.2 Historique

La blockchain a été introduite avec l'invention du bitcoin en 2008, puis avec sa pratique mise en œuvre en 2009. Pour ce chapitre, il suffit de présenter très brièvement le bitcoin car il existe un chapitre complet sur le bitcoin plus tard mais il est également indispensable de se référer au bitcoin car sans lui, l'histoire de la blockchain n'est pas complète. Le concept de monnaie électronique ou de monnaie numérique n'est pas nouveau. Depuis les années 1980, les protocoles d'e-cash ont existaient qui sont basés sur un modèle proposé par David Chaum. [11]

1.3 définition de blockchain

Le terme Blockchain provient de la manière dont le réseau stocke les données relatives aux transactions, c'est-à-dire des blocs (block en anglais), reliés pour former une chaîne (chain en anglais) . La « chaîne de blocs » s'étend ainsi au fur et à mesure de l'augmentation du nombre de transactions. Les blocs recueillent et confirment les heures et les séquences des transactions, ainsi consignées dans la Blockchain, dans un réseau distinct, régi par des règles convenues entre ses membres.

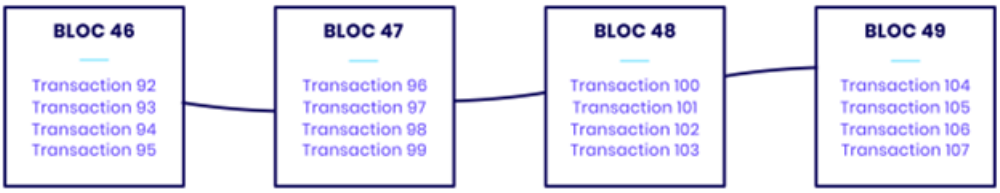

FIGURE 1.1 – Chaîne de blocs[8]

Chaque bloc contient un hash (empreinte numérique ou identifiant unique), les lots horodatés des transactions récentes valides et le hash du bloc précédent. Le hash du bloc précédent relie les blocs ensemble et évite qu'un bloc ne soit modifié ou inséré entre deux blocs existants. Ainsi, chaque bloc consécutif renforce la vérification du précédent, et, par conséquent, l'ensemble de la Blockchain. La Blockchain contient donc des témoins d'intégrité qui lui confèrent sa caractéristique essentielle d'immuabilité. Pour être très précis, même si la Blockchain contient des données de transaction, elle ne vient en aucun cas remplacer les bases de données, les technologies de messagerie, les traitements transactionnels ou les processus métier. Elle contient tout simplement des preuves de transactions vérifiées. Pour autant, même si une Blockchain sert pour l'essentiel de base de données d'enregistrement de transactions, ses avantages vont bien au-delà de ceux d'une base de données traditionnelle.[8]

1.4 Fonctionnent 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 la blockchain, toutes les transactions sont regroupées sous la forme de blocs. Chaque bloc doit ensuite être validé par les nœuds du réseau en utilisant une méthode algorithmique. Une fois que le bloc est validé, il est ajouté à la chaîne de blocs et devient donc visible de tous les utilisateurs. Voici un schéma qui vous permettra d'illustrer cette définition. [3]

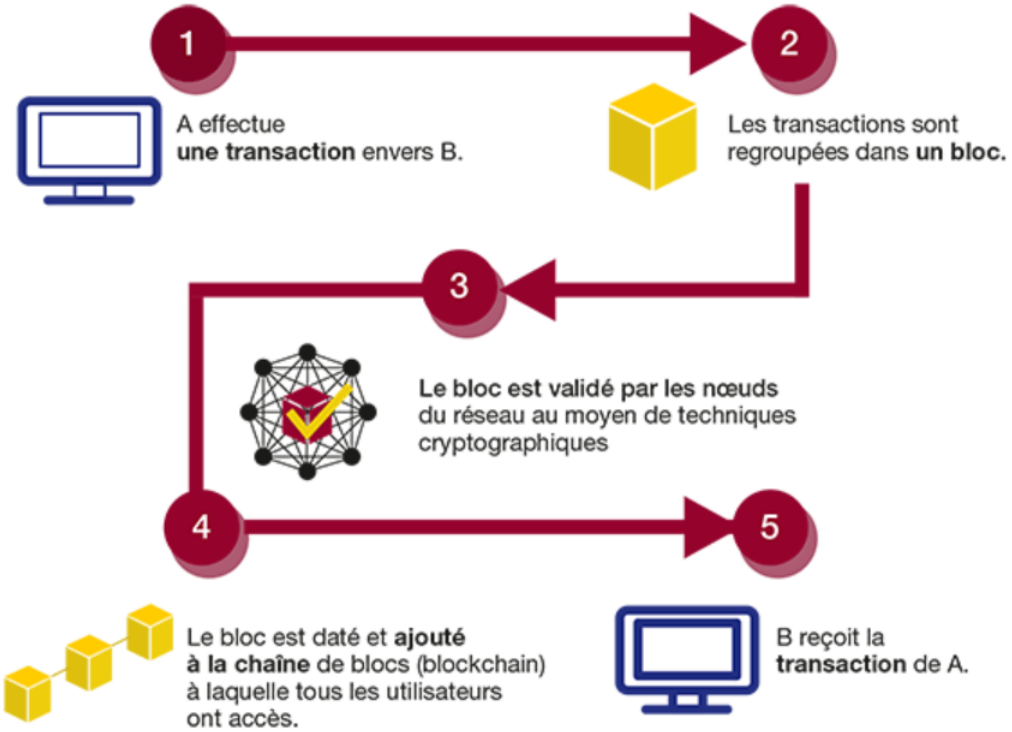

FIGURE 1.2 – Fonctionnemet d' une Blockchain

1.5 Mécanismes de consensus

Dans les paiements traditionnels, les tiers, traditionnellement les banques, sont digne de confiance pour le maintien des transactions et des soldes de comptes. Dans en revanche, la blockchain est un consensus distribué et sans confiance système. Les tiers ne sont pas nécessaires pour les transactions. Tout le monde peut vérifier les informations écrites, car tout le monde en a une copie de la blockchain. Il est important que tout le monde ait le même copie. Pour parvenir à ce consensus cohérent à l'échelle du système, un consensus mécanisme, soit une preuve de travail ou une preuve de participation est nécessaire.[25]

1.5.1 Preuve de travail (PoW)

Dans le système de preuve de travail, les mineurs se font concurrence pour résoudre un «Puzzle de calcul», qui est moyennement difficile à résoudre mais le résultat doit être facile à vérifier. Ce puzzle implique la détermination d'un nonce, que lorsque les données du bloc sont hachées, le hachage est plus petit supérieur à un seuil défini. Habituellement, la force brute est utilisée pour résoudre le puzzle. Ce processus s'appelle l'exploitation minière. Comme la puissance de calcul du réseau augmente, les blocs sont créés plus rapidement. Réagir à ce changement, le seuil défini, appelé difficulté, est périodiquement adapté pour réguler le taux de génération de bloc. Le premier mineur à trouver une solution en fait la publicité auprès du réseau et est récompensée. L'exploitation minière sert deux objectifs : vérifier la légitimité des transactions et créer de nouvelles pièces en récompensant les mineurs. L'inconvénient de PoW qu'il faut beaucoup d'énergie, par ex. Les transactions Bitcoin d'ici 2020 seront consomment autant d'électricité que le Danemark aujourd'hui . [26]

1.5.2 preuve d'enjeu (PoS)

Dans le système de preuve d'enjeu, les mineurs ne sont pas en concurrence, le jeu de validateurs est conservé. Quiconque possède les pièces de la blockchain,peut rejoindre cet ensemble en verrouillant toutes ses pièces, appelées le pieu, dans un dépôt. Les validateurs participent alors à la création du bloc processus, où deux grands types d'algorithmes de consensus sont utilisés. Dans le PoS basé sur la chaîne, le validateur, qui a le droit de créer le bloc, est périodiquement sélectionné de manière pseudo-aléatoire. Dans Byzantine-fault- PoS de style tolérant les validateurs peuvent proposer des blocs, le droit de faire ainsi leur est assigné au hasard, plus loin les validateurs sont d'accord ou en désaccord sur les blocs proposés en votant. Le créateur de bloc reçoit des frais de transaction au lieu de bloquer les récompenses. Par conséquent, toutes les pièces sont créés au début et leur nombre ne change jamais. Comme décrit dans [7] [22] , les avantages du PoS sont que moins d'énergie est nécessaire pour un consensus et une protection accrue contre les attaques.

1.5.3 Preuve d'autorité (PoA)

Dans le système de preuve d'autorité, seuls les nœuds autorisés exclusivement ont le droit de créer de nouveaux blocs. Le système ne repose pas sur résoudre des «énigmes informatiques» et est principalement utilisé pour le consortium blockchains [28].

1.6 Les types de la blockchain

1.6.1 Blockchain publique

Dans la blockchain publique, tous les nœuds du réseau d'échange sont contrôlés par le réseau peer-to-peer. Il n'y a aucune barrière d'entrée, aucune permission à demander pour effectuer une transaction et tous les acteurs sont donc en situation égalitaire dans leur participation au réseau. C'est le cas de la monnaie virtuelle bitcoin, bien sûr, et de l'Ethereum.

1.6.2 Blockchain privée

La blockchain privée tourne sur un réseau privé sur lequel le gérant peut modifier le protocole quand il le souhaite. Personne ne peut y participer sans y être autorisé. "Cette blockchain n'est pas très intéressante, juge David Teruzzi, expert en bitcoin. Elle est certes scalable à l'infini, contrairement à la blockchain publique, mais son intérêt est limité puisqu'elle ne fait pas le lien entre différents acteurs." Les blockchains privées sont en fait beaucoup utilisées par des acteurs comme les banques, par exemple, pour expérimenter en interne sur la blockchain et accroître leur connaissance de la technologie. "Cela les aide à mieux appréhender la blockchain pour l'utiliser dans le futur dans un scénario plus complexe", explique Luca Comparini, responsable blockchain chez IBM France. Mais pas seulement. "Les blockchains privées peuvent aussi permettre de raccorder différents systèmes d'information qui ne se parlent pas bien au sein d'une même entreprise."

1.6.3 Consortium

Le consortium est une blockchain qui regroupe plusieurs acteurs mais qui n'est pas publique et ouverte à tous. "C'est une blockchain hybride, résume David Teruzzi. Les droits d'écriture et de modification sont modifiables et certains nœuds peuvent être rendus publics tandis que d'autres restent privés." Les participants possèdent certains droits et les décisions prises sur la blockchain le sont par la majorité d'entre eux.

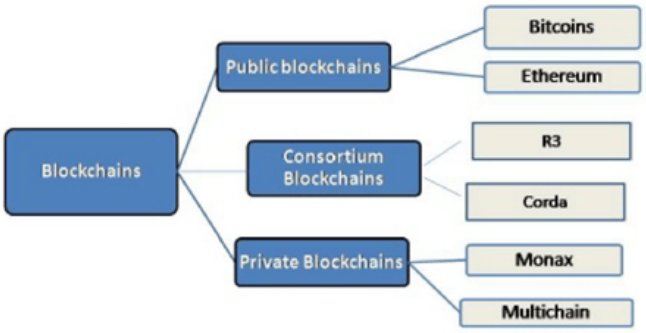

FIGURE 1.3 – Les types de la Blockchain

1.7 Role des blockchain

Un blockchain est un système pair à pair sans autorité centrale qui gère les flux des données . L' une des principales façon d'éliminer le contrôle central tout en maintenant l'intégrité des données est d'avoir un large réseau distribué d'utilisateurs indépendants. Cela signifie que les ordinateurs qui composent le réseau se trouvent dans plus qu'un seul emplacement.Ces ordinateurs souvent appelées des nœuds plein.[16]

1.8 Blockchain aujordhui

1.8.1 Cryptomonnaie

Crypto :

fait la reference à la partie « cryptographique » qui est necessaire pour sécuriser l'algorithme utiliser au seine de la cryptomonnaie.

monnaie :

fait reference au système de paiement universel permettant les échanges . On peut aussi utiliser le nom de « crypto-actif » qui selon moi est plus approprié car toute cryptomonnaie n'as pas forcément pour objectif d'être une monnaie.Il estt plus juste de la voir comme un actif. Vous verrez que la majeur partie des communications dans les médias sont faites avec le terme « cryptommonnaie », ou sont diminutif « crypto ». [5]

1.8.2 Histoire des cryptomonnaie :

•2008 :Publication du fonctionnement de Bitcoin

Le timing est parfait . La création de Bitcoin en 2008 intervient juste après la crise financière des « Subprimes »,causée par la fiallite de la banque Lehman Brothers qui plonge alors l'économie dans le chaos.Il y a à ce moment –là un réel besoin d'apporter un système plus transparent et de redonner du pouvoir aux particuliers qui sont prisonniers des banques.

•2013 :Bitcoin atteint les 1000 Dollar

Incroyable mais vrai, en seulement 4 ans depuis sa création ,le Bitcoin franchit la barre des 1000. Bitcoin est alors à ce moment là encore très méconnu et réservé aux initiés. Cette performance exceptionnelle a permis à certains investisseurs de devenir millionnaires. On note aussi que plusieurs cryptomonnaies se lancent au fur et à mesure .

•2015 :lancement d'Ethereum

C'est en 2015 que se lance le projet Ethereum ,avec à sa tête vitalik buterin qui est une figure incontournable du marché des cryptomonnaies. Ethereum a apporté une innovation très puissante au sein des cryptomonnaies : les contrats intellegents(smart contrats) sur lesquels nous reviendros plus tard.

•2017 :Bitcoin atteint les 20 000 Dollar

L'euphorie s'accentue encore plus en 2017, de nombreuses crypto monnaies voient le jour et beaucoup de personnes investissent à la hâte car les rendements sont délirants. A cette période ,il est assez simple de multiplier par trois son portefeuille en quelques jours , en investissant sur les nouveaux projets qui se lancent. Imaginez donc l'état d'excitation général. 'est la première fois qu' un marché propose de tels rendements ,aussi facilement et en si peu de temps.

1.8.3 Bitcoin

•Historique L'historique de Bitcoin a été mouvementé depuis le lancement des premiers bitcoins en 2009 et la première véritable transaction effectuée en mai 2010 (2 pizzas contre 10,000 BTC, ce qui équivaudrait aujourd'hui, au cours actuel, à 2 millions d'euros la pizza !). Début 2011, le bitcoin touche la parité avec le dollar et atteint plusieurs millions de dollars de capitalisation : les premiers articles sur le Bitcoin commencent alors à apparaître dans des journaux majeurs aux Etats-Unis. Après deux phases de bulles, aux printemps 2011 et 2013, le cours du bitcoin a retrouvé plus de stabilité depuis 2014. L'intérêt porté à la blockchain elle-même, au-delà de son application monétaire qu'est le bitcoin, est venu relativement tardivement, à partir des années 2013- 2014. Il n'y a bien sûr pas de date précise étant donné que la blockchain existe depuis la création de Bitcoin. Les pionniers s'y sont intéressés avant 2013-2014, mais ce n'est véritablement qu'en 2015 que la blockchain a commencé à susciter une grande attention.

•Definiton Bitcoin peut être défini de différentes manières ; c'est un protocole, une monnaie numérique et une plateforme. C'est un combinaison de réseau peer-to-peer, de protocoles et de logiciels qui facilitent la création et l'utilisation de la monnaie numérique nommée bitcoin. Notez que Bitcoin avec un B majuscule est utilisé pour désigner le Bitcoin protocole, alors que le bitcoin avec un b minuscule est utilisé pour désigner le bitcoin, la monnaie. Nœuds dans ce les réseaux peer-to-peer se parlent en utilisant le protocole Bitcoin. La décentralisation de la monnaie a été rendue possible pour la première fois avec l'invention du bitcoin. De plus,

le problème de la double dépense a été résolu de manière élégante et ingénieuse en bitcoin. Un problème de double dépense survient lorsque, par exemple, un utilisateur envoie des pièces à deux utilisateurs différents au en même temps et ils sont vérifiés indépendamment comme des transactions valides. .[26]

1.8.4 smart contrat

Smart contrat :Un contrat intelligent est un code exécutable qui s'exécute sur la blockchain pour faciliter, exécuter et appliquer les termes d'un accord. L'objectif principal d'un contrat intelligent est d'exécuter automatiquement les termes d'un accord une fois que les conditions spécifiées sont remplies. Ainsi, les contrats intelligents promettent des frais de transaction faibles par rapport aux systèmes traditionnels qui nécessitent un tiers de confiance pour appliquer et exécuter les termes d'un accord. L'idée des contrats intelligents est venue de Szabo en 1994 [23]. Cependant, l'idée n'a pas vu le jour jusqu'à l'émergence de la technologie blockchain. Un contrat intelligent peut être considéré comme un système qui libère des actifs numériques à tout ou partie des parties impliquées une fois que des règles arbitraires prédéfinies ont été respectées [1]. Par exemple, Alice envoie X unités monétaires à Bob, si elle reçoit Y unités monétaires de Carl. De nombreuses définitions différentes d'un contrat intelligent ont été discutées dans la littérature. Dans [5], l'auteur a classé toutes les définitions en deux catégories, à savoir le code de contrat intelligent et le contrat juridique intelligent. Le code de contrat intelligent signifie «un code stocké, vérifié et exécuté sur une blockchain» [24]. La capacité de ce contrat intelligent dépend entièrement du langage de programmation utilisé pour exprimer le contrat et des caractéristiques de la blockchain. Un contrat juridique intelligent signifie un code pour compléter ou remplacer des contrats juridiques. La capacité de ce contrat intelligent ne dépend pas de la technologie, mais plutôt des institutions juridiques, politiques et commerciales. Cette étude se concentrera sur la première définition, qui est le code de contrat intelligent.

Caractéristiques de la blockchain

La blockchain a cinq caractéristiques :

•**décentralisation :** : Étant donné que le système blockchain adopte le mode réseau P2P, il n'y a pas centre de contrôle obligatoire. Chaque nœud du réseau a le même statut dans le

système. Les données les blocs générés sont conservés par tous les nœuds du système. Tous les nœuds ont enregistré et des données de transaction stockées, augmentant la robustesse de la base de données.

•**Ouverture :**Le système blockchain utilise des algorithmes mathématiques fiables pour réguler le comportement des transactions. L'échange de données entre les nœuds du système ne nécessite pas de confiance mutuelle. Les règles de fonctionnement sont ouvertes et transparentes. En plus des informations privées du nœud étant cryptées dans le système, les autres données sont ouvertes à tous. Tout le monde peut interroger la blockchain informations de données via la valeur de hachage de l'en-tête de bloc et les informations enregistrées est sauvegardé de manière redondante sur plusieurs nœuds. La mise à jour des informations nécessite la mutuelle l'authentification de plusieurs nœuds, ce qui signifie qu'un nœud ne peut pas tromper les autres nœuds, de sorte que le les informations de l'ensemble du système sont très transparentes.

•**d'exécution automatique :** La blockchain peut être transformée en contrats intelligents en écrivant code, qui stipule les obligations à exécuter par chaque partie dans le contrat et leconditions d'exécution du contrat. Le système blockchain juge automatiquement le conditions d'exécution du contrat. Lorsque toutes les conditions de détermination sont satisfaites, le système blockchain appliquera automatiquement les termes du contrat. D'une part, cela a augmenté l'efficacité de l'exécution des contrats et, plus important encore, il a effectivement assuré la mise en œuvre du contrat sans la supervision d'un tiers puissant . [33]

•**Traçabilité :** protection contre la falsification des données, sécurité et crédibilité. La traçabilité signifie que les enregistrements ajouté à la blockchain sera stocké en permanence, et les informations du commerçant sont liées à chaque enregistrement de transaction dans la blockchain. Le chemin de transfert complet de l'objet de la transaction peut être entièrement enregistré et retracé, ce qui facilite la supervision de la transaction . La technologie blockchain utilise des principes cryptographiques asymétriques pour crypter les données, et le un algorithme puissant formé par l'algorithme de consensus est utilisé pour se défendre contre les attaques et garantir la modification non destructive et l'imprévisibilité des données de la blockchain. Prenons l'exemple de la blockchain Bitcoin ; la manipulation des données ne peut être mise en œuvre qu'après contrôlant 51

•**Anonymat :**L'échange de données entre nœuds dans un système blockchain suit un algorithme fixe,les deux parties n'ont donc pas besoin de divulguer leur identité. Au lieu de

cela, les règles de procédure dans la blockchain sont utilisés pour se faire confiance.

1.9 Les avantages et les inconvénients de la blockchain :

1.9.1 Les avantages

Une meilleure transparence

La technologie blockchain se veut être un système transparent.Le contrôle des informations repose sur les utilisateurs. Tous ont donc accès à un contrôle complet de leurs transactions.

Une sécurité renforcée

Grâce à la cryptographie, l'authenticité des informations est assurée. Rappelez-vous aussi qu'une fois le bloc validé celui-ci n'est plus modifiable. Pour qu'un éventuel changement ait lieu, la majorité des membres du réseau doivent être d'accord. Enfin, les informations étant distribuées sur plusieurs ordinateurs, les données sont bien plus sécurisées en cas de défaillance sur un réseau.

Des transactions plus rapides

Généralement il est nécessaire d'attendre plusieurs jours pour qu'un virement soit réellement effectué. avec la technologie blockchain, cela ne prend que quelques minutes

Des coûts de transactions faibles

Cette technologie est aussi bénéfique pour les utilisateurs en terme de coût de Ceux-ci sont largement réduits sans l'intervention d'une organisme tierce. La technologie blockchain est aujourd'hui de plus en plus utilisée grâce à un mécanisme sécurisé et la facilité des transactions.

Pour fournir un service plus rapide, de meilleure qualité et plus fiable aux utilisateurs, la blockchain fait donc son apparition dans les cryptomonnaies, les domaines de la santé, juridique,

gouvernemental, dans l'industrie automobile ou encore dans les banques et marchés d'actions.

1.9.2 Les inconvénients

Le principal inconvénient de la Blockchain est la haute énergie dépendance parce que le processus d'extraction consomme beaucoup d'énergie pour calculer le code de hachage du bloc suivant. Il est nécessaire pour être le premier à obtenir la rémunération de ces calculs. Dans ce cas, ce goulot d'étranglement de la Blockchain limite le débit élevé et les faibles latences. Le paramétrage des tailles de bloc et des intervalles ne sera pas assez pour les plus gros déploiements de charge de la Blockchain [31],[19]. Un autre inconvénient de la Blockchain est l'introduction car les institutions financières doivent abandonner leur réseaux et commencez à en créer un nouveau. L'intégration peut être un processus très difficile et la plupart des institutions ne veulent pas pour implémenter la Blockchain dans leurs systèmes existants [31], [19].

Tous ces inconvénients découlent d'une autre limitation majeure – les coûts élevés de la mise en œuvre de la Blockchain.

1.10 Conclusion

Les crypto-monnaies sont une nouvelle technologie et sont la raison de la modernisation de l'économie. Déjà maintenant, un grand nombre de personnes utilisent des crypto- pièces pour le paiement, participent à leur production et gagnent de l'argent grâce à la volatilité du marché. Aujourd'hui, les crypto-monnaies sont au stade de la formation. Des versions améliorées sont publiées chaque année. Mais il est déjà évident pour de nombreux experts que les crypto-monnaies sont l'argent du futur avec un grand potentiel de développement.

Chapitre 2

La sécurité de la Blockchain

2.1 Introduction

Dans le chapitre précédent, on a présenté le bagage théorique de la technologie blockchain. On a aussi présenté les différentes crypto-monnaie qui utilise par cette technogie. Cette technologie repose sur un système de pair-à-pair décentralisé : les données ne sont pas hébergées par un serveur unique mais distribuées entre les utilisateurs, sans intermédiaire. les blockchains (chaînes de blocs) sont sécurisées par différents mécanismes, notamment par des techniques cryptographiques avancées . La technologie Blockchain est la structure de base de la plupart des systèmes de crypto-monnaie et empêche ce type de monnaie numérique d'être dupliqué ou détruit. Cependant, la sécurité de la blockchain est loin d'être un sujet simple. Par conséquent, il est important de comprendre les concepts de base et les mécanismes qui assurent une protection efficace de ces systèmes innovants.

2.2 Le système Blockchain

2.2.1 Composition d'une Blockchain

Comme indiqué précédemment, une blockchain est une chaîne de blocs contenant chacun plusieurs transactions, et qui vont être inscrits au fur et à mesure dans la blockchain par des nœuds du réseau. L'implémentation peut différer d'une blockchain à l'autre, mais les principaux

éléments d'un bloc sont les suivants : •**un index**

•**un hash servant à identifier le bloc**

•**le hash du bloc précédent**

•**un timestamp**

•**un ensemble de transactions**

Le premier bloc d'une blockchain est appelé le "Genesis Block". .[4]

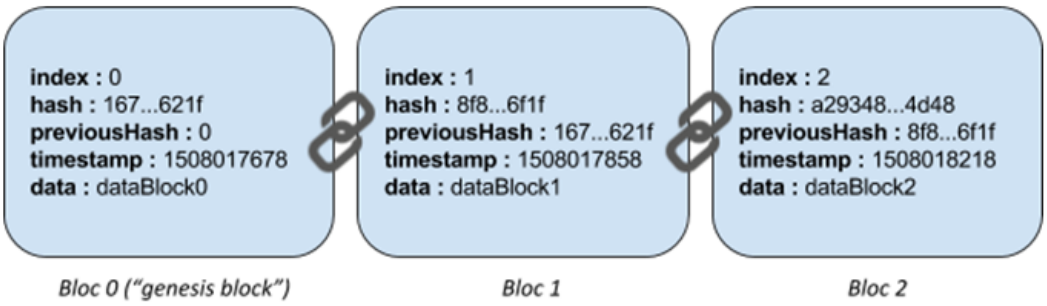

FIGURE 2.1 – Les types de la blockchain [4]

2.2.2 Les transactions

Lorsqu'un utilisateur soumet une transaction (transfert de bitcoins vers une personne par exemple), cette dernière est envoyée sur la blockchain et passe en attente de validation. C'est alors que les "mineurs" entrent en jeu. Ces utilisateurs apportent de la puissance de calcul au réseau afin de vérifier ces transactions. Typiquement, le logiciel des mineurs va consulter l'historique des transactions, et s'assurer qu'un utilisateur désirant effectuer une transaction possède bien ce qu'il prétend avoir. Intervient ensuite un consensus pour s'assurer qu'un mineur a bien fourni de la puissance de calcul pour calculer le hash du nouveau bloc. Il s'agit de la preuve de travail ("proof-of-work"). Une fois fait, le mineur diffuse le hash du nouveau bloc à l'ensemble du réseau. Si le résultat satisfait le consensus, le bloc est ajouté à la blockchain et le mineur est rémunéré avec des tokens de la blockchain, fraîchement créés [19].

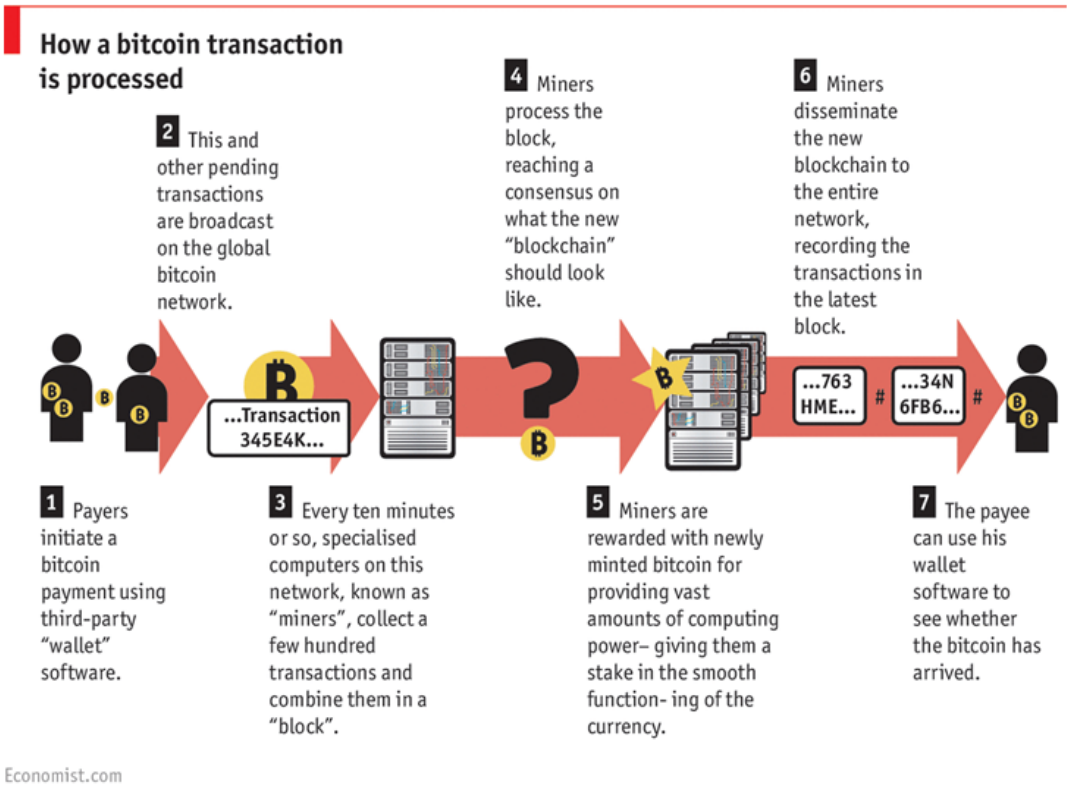

FIGURE 2.2 – Transaction Bitcoin

2.2.3 Essentiels Bitcoin

Dans son œuvre désormais célèbre, Satoshi Nakamoto a montré un solution aux problèmes que la mise en œuvre et la convivialité de la monnaie numérique confrontée, en particulier la double dépense problème [24]. Alors que la véritable identité de Nakamoto est un point de spéculations, ce que l'on sait, c'est que jusqu'en 2010, il est resté actif sur le projet Bitcoin, puis il a reculé et a donné le projet à la communauté pour un développement ultérieur [33] . Il a proposé un système avec serveur d'horodatage distribué P2P qui sert de générateur de la preuve informatique de la ordres chronologiques des transactions . Une pièce électronique est défini comme une chaîne de signatures numériques. Chaque transaction est défini comme un ensemble de hachage signé numériquement du précédent transaction et la clé publique du prochain propriétaire. La clé privée est utilisé pour signer la transaction et la clé publique est utilisée pour vérification de la transaction,la clé publique est conservée dans le portefeuille, qui peut être implémentée dans un logiciel, matériel, ou en ligne.

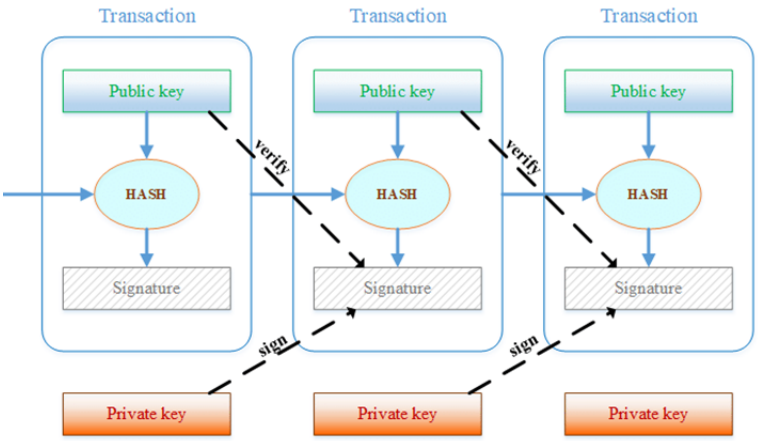

FIGURE 2.3 – Essentiels Bitcoin

2.3 L'échange pair à pair (p2p)

2.3.1 Signification P2P :

Le pair-à-pair, peer-to-peer ou P2P (les trois termes désignent la même chose), Un réseau pair à pair est un réseau d'ordinateurs qui communique directement d'un ordinateur à l'autre. La blockchain permet à deux ordinateurs d'échanger de la valeur sans devoir faire appel à un tiers de confiance. L'internet permet aux ordinateurs de communiquer des informations en peer-to-peer (c'est-à-dire sans intermédiaire. [29].

2.3.2 Rôle du P2P dans la blockchain

Le P2P est une technologie basée sur un principe très simple, c'est le concept de décentralisation. L'architecture peer-to-peer de la blockchain permet à toutes les crypto-monnaies d'être transférées dans le monde entier, sans avoir besoin d'intermédiaire ou d'intermédiaire ou de serveur central. Avec le réseau peer-to-peer distribué, toute personne souhaitant participer au processus de vérification et de validation des blocs peut configurer un nœud Bitcoin.

La blockchain est un suivi décentralisé d'un ou plusieurs actifs numériques sur un réseau peer-to-peer. Lorsque nous disons un réseau peer-to-peer, cela signifie un réseau peer-to-peer décentralisé où tous les ordinateurs sont connectés d'une manière ou d'une autre, et où chacun conserve une copie complète du registre et le compare à d'autres appareils pour garantir le

les données sont exactes. Ceci est différent d'une banque, où les transactions sont stockées de manière privée et ne sont gérées que par la banque.[31]

2.3.3 La diffusion des blocs sur un réseau pair à pair

Chaque bloc est validé par certains utilisateurs baptisés « mineurs » , et sont transmis aux « noeuds » du réseau, c'est-à-dire aux détenteurs du registre, ce registre étant la chaîne de blocs elle-même. Cette dernière est actualisée en permanence.

Dans les blockchains dites ouvertes (permissionless), comme celle du bitcoin, n'importe quel utilisateur de l'internet peut ainsi devenir un noeud du réseau en téléchargeant le registre auprès d'un noeud existant. Chaque noeud est connecté à plusieurs autres, appelés pairs, eux-mêmes ayant leurs propres pairs, ce qui forme un réseau pair à pair.[14]

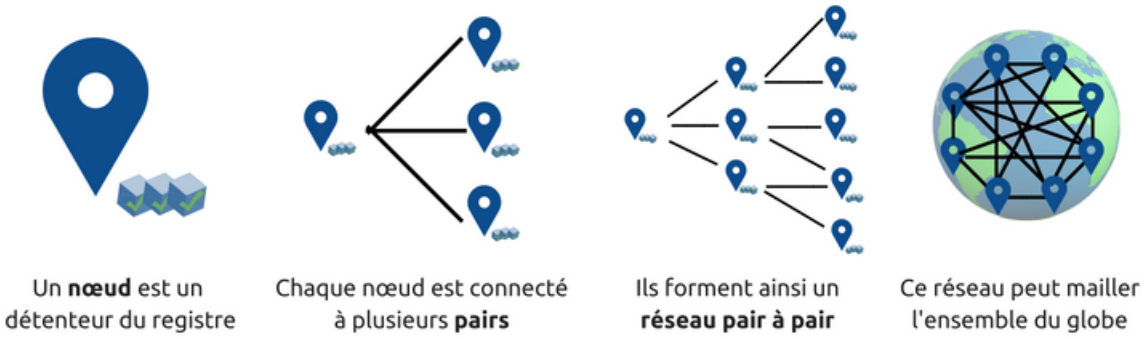

FIGURE 2.4 – La notion de réseau pair à pair [14]

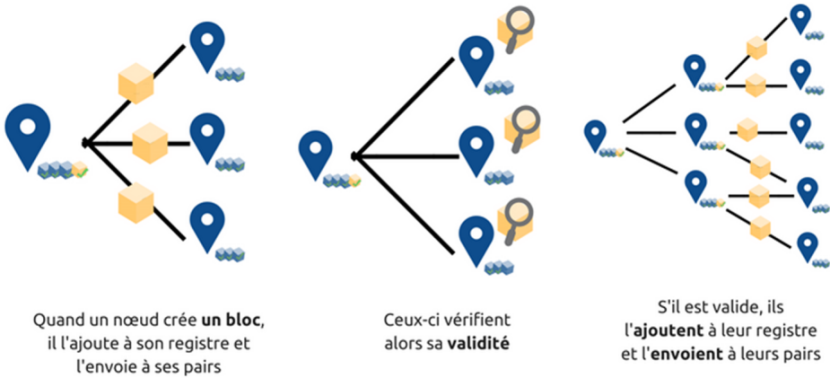

FIGURE 2.5 – Diffusion d'un bloc dans le réseau[14]

si un noeud essaie d'introduire dans le réseau un bloc invalide, celui-ci n'est pas validé par la plupart des noeuds (certains peuvent toutefois être corrompus) et n'est donc pas ajouté à

leur registre ni transmis à leurs pairs.

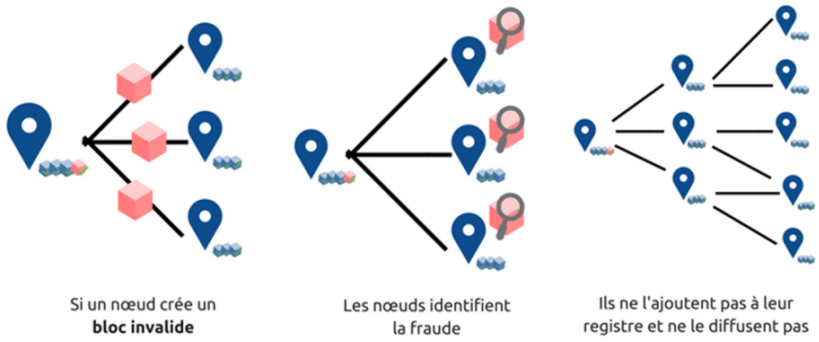

FIGURE 2.6 – Introduction d'un bloc invalide [14]

La validation des blocs permet donc de se prémunir du risque d'attaque malveillante. Aucune autorité centrale ne s'en occupe, puisque les utilisateurs s'en chargent en surveillant le système et en se contrôlant mutuellement. Cette sécurité, source de confiance, est l'un des aspects essentiels de la blockchain. Le fait que des centaines de copies du registre soient mises à jour simultanément et régulièrement vise à rendre les blockchains quasiment indestructibles.

2.3.4 Centralisé vs décentralisé

Le point de départ évident serait de parler du système de paiement mondial, car c'était l'idée originale derrière la première crypto-monnaie décentralisée du monde - Bitcoin. Chaque banque dans le monde fonctionne sur des serveurs centralisés. Cela signifie qu'ils ont accès à toutes vos activités financières.

Ils savent combien vous êtes payé, où vous dépensez votre argent, à qui vous envoyez votre argent et tout ce qui concerne votre compte bancaire. De plus, si quelqu'un pouvait obtenir votre mot de passe bancaire sur Internet, ou pire encore, pirater les serveurs centralisés de la banque, il aurait accès à toutes ces informations. Si les serveurs centralisés tombaient en panne (ce qui arrive tout le temps), vous pourriez vous voir refuser l'accès à vos fonds.

Lorsque nous comparons centralisé et décentralisé, un système de paiement décentralisé résout tous ces problèmes. Lorsque vous utilisez une crypto-monnaie pour envoyer ou recevoir des paiements, vous n'avez pas besoin de compter sur un tiers pour confirmer la transaction. C'est pourquoi Bitcoin et certaines autres crypto-monnaies sont appelés «monnaies numériques peer-to-peer».

Comme il n'y a pas d'exigence pour un tiers, les frais sont considérablement inférieurs et, dans certains cas, pratiquement gratuits. Cela rend les crypto-monnaies parfaites lors de l'envoi ou de la réception d'un paiement de quelqu'un dans un autre pays, car des sociétés comme Western Union facturent des montants très élevés.

Les systèmes décentralisés sont sans frontières, donc cela ne change rien si vous envoyez de l'argent à quelqu'un dans votre ville natale ou à quelqu'un à l'autre bout du monde. Cela prend le même temps et les frais sont les mêmes.

Vos fonds sont également beaucoup plus sûrs lorsque vous utilisez un système décentralisé. La seule personne qui a accès à votre argent est vous, car vous êtes la seule à avoir les clés privées pour accéder à vos fonds. Si vous suivez les bonnes mesures de sécurité, personne ne peut savoir quelles sont ces clés privées.

Dans l'ensemble, un système mondial de paiements décentralisé présente les avantages suivants.[2]

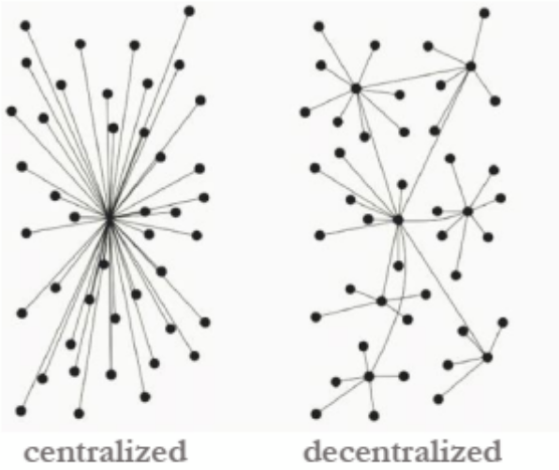

FIGURE 2.7 – Centralisée vs décentralisé [2]

2.3.5 Ledger distribué et BlockChain

Un registre distribué, également connu sous le nom de registre partagé, est une liste de données partagées et synchronisées qui sont réparties géographiquement sur plusieurs sites. Les données sont exactement répliquées et synchronisées sur tous les sites pour maintenir l'intégrité, la disponibilité et la résilience des données [1]. Contrairement au système centralisé, il n'y a pas d'administrateur central ni de point de contrôle unique. Si un emplacement échoue brusquement

ou cesse de fonctionner, l'emplacement restant dispose des données et de la capacité nécessaires pour gérer le grand livre ou tous les détails de la transaction en l'absence de l'emplacement défaillant. De cette façon, un registre distribué fournit des informations en temps réel et réduit les taux d'erreur ou d'échec des transactions. Cela réduit également les coûts d'infrastructure par rapport au système centralisé. Un registre distribué utilise un réseau peer-to-peer pour communiquer avec des nœuds répartis dans le monde entier. De plus, la technologie du grand livre distribué nous donne la possibilité de réaliser des économies d'échelle en permettant à la transaction de servir simultanément de rapport d'accord, de règlement et de réglementation. Au lieu de créer de nombreux services duplicatifs et redondants, un seul enregistrement principal principal peut servir de source, éliminant le besoin de rapprochement et augmentant la vitesse de traitement post-négociation . [17]

2.4 Cryptographie

2.4.1 Définition de la cryptographie :

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.

2.4.2 L'usage de la cryptographie

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

La confidentialité :

consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

L'intégrité :

vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.

L 'authentification :

consiste à assurer l'identité d'un utilisateur, c.-à-d de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

La non répudiation :

de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. [30]

2.4.3 Confidentialité et algorithmes de chiffrement :

La confidentialité est le premier problème posé à la cryptographie. Il se résout par la notion de chiffrement. Il existe deux grandes familles d'algorithmes cryptographiques à base de clef : Les algorithmes à clef secrète ou algorithmes symétriques, et les algorithmes à clef publique ou algorithmes asymétriques Chiffrement symétrique ou clef secrète : dans la cryptographie conventionnelle, les clefs de chiffrement et de déchiffrement sont identiques : c'est la clef secrète, qui doit être connue des tiers communiquant et d'eux seuls. Le procédé de chiffrement est dit symétrique. Les algorithmes symétriques sont de deux types : • Les algorithmes de chiffrement en continu, qui agissent sur le message en clair un bit à la fois ; • Les algorithmes de chiffrement

par bloc, qui opèrent sur le message en clair par groupes de bits appelés blocs. Les principaux algorithmes à clé privée sont : Blowfish DES/3DES IDEA.

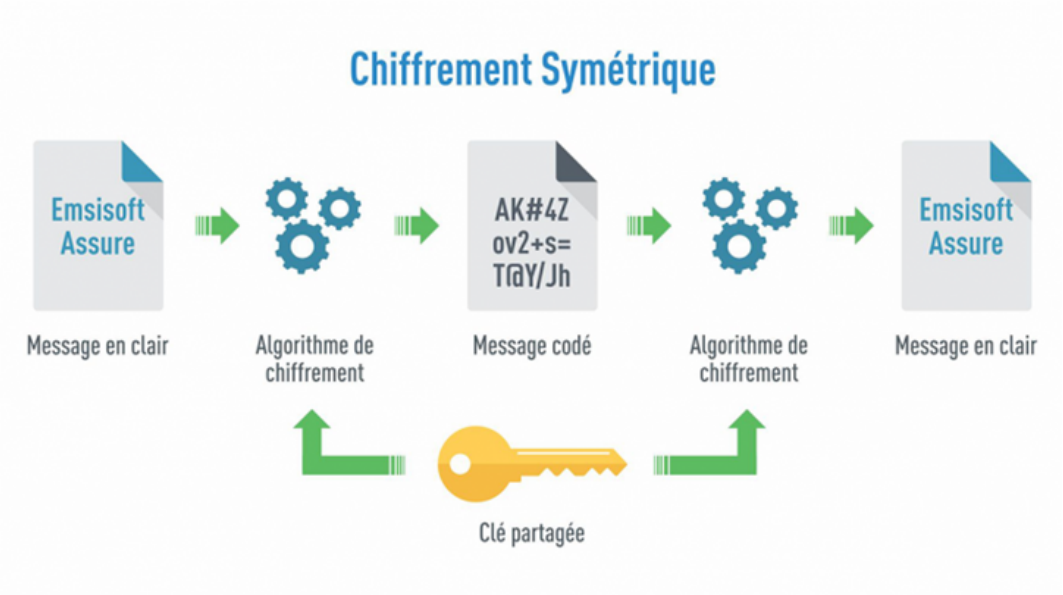

FIGURE 2.8 – Chiffrement symétrique

Chiffrement asymétrique ou à clef public : avec les algorithmes asymétriques, les clefs de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée. C'est pourquoi on parle de chiffrement à clef publique. Si la clef publique sert au chiffrement, tout le monde peut chiffrer un message, que seul le propriétaire de clef privé pourra déchiffrer. On assure ainsi la confidentialité. Certains algorithmes permettent d'utiliser la clef privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer, mais seul le possesseur de clef privée peut chiffrer. [34]

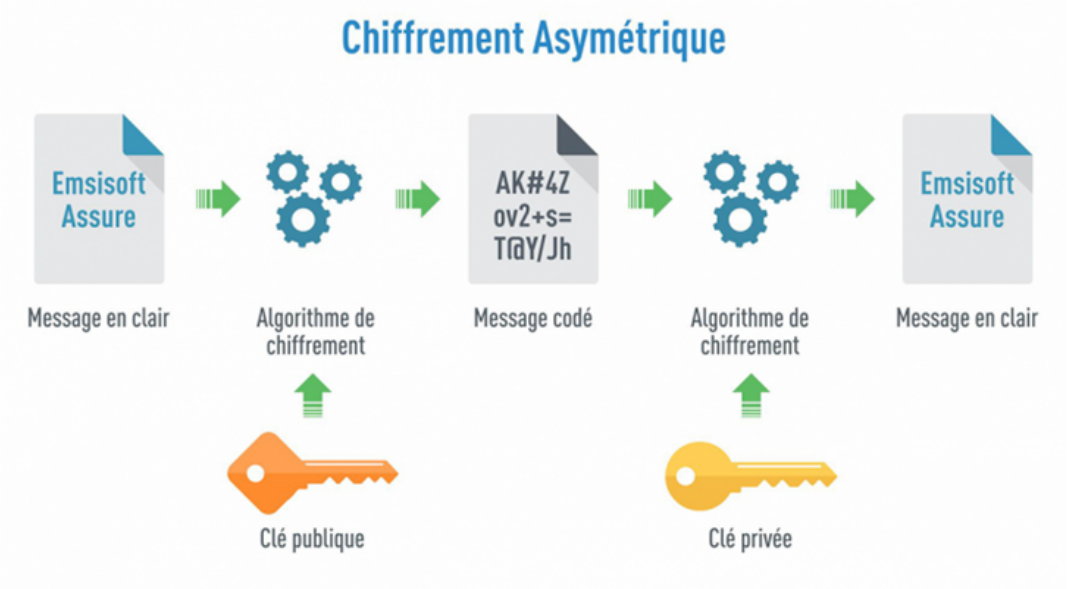

FIGURE 2.9 – Chiffrement asymétrique [34]

2.4.4 La signature numérique :

Les signatures numériques sont l'un des principaux aspects de la sécurité et de l'intégrité des données enregistrées sur une blockchain. Ils font partie intégrante de la plupart des protocoles de la blockchain, principalement utilisés pour sécuriser les transactions et les blocs de transactions, les transferts d'informations sensibles, la distribution de logiciels, la gestion des contrats et tout autre cas où il est important de détecter et de prévenir toute manipulation externe. Une signature numérique est un mécanisme de cryptographie utilisé pour vérifier l'authenticité et l'intégrité de données numériques. Nous pouvons considérer cela comme une version numérique des signatures manuscrites ordinaires, mais avec des niveaux plus élevés de complexité et de sécurité. Pour simplifier, nous pouvons décrire une signature numérique comme un code rattaché à un message ou un document. Après avoir été généré, le code sert de preuve quand au fait que le message n'ait été trafiqué d'aucune sorte entre l'expéditeur et le destinataire. Bien que le concept de sécurisation des communications en utilisant la cryptographie remonte assez loin dans l'histoire de l'humanité, les systèmes de signature numérique sont devenus réalité dans les années 1970 - grâce au développement de la Cryptographie à Clé Publique (PKC). Pour savoir comment les signatures numériques fonctionnent, nous devons d'abord comprendre les bases des fonctions de hachage et de la cryptographie à clé publique.[15]

2.4.5 Cryptographie à Clé Publique (PKC)

La cryptographie à clé publique, ou PKC en anglais, fait référence à un système de cryptographie qui utilise une paire de clés : une clé publique et une clé privée. Les deux clés sont corrélées mathématiquement et peuvent être utilisées à la fois pour du cryptage de données et des signatures numériques. En tant qu'outil de chiffrement, la PKC est plus sûre que les méthodes plus rudimentaires de cryptage symétrique. Alors que les systèmes plus anciens dépendent de la même clé pour chiffrer et déchiffrer les informations, PKC permet le chiffrement de données avec une clé publique et le décryptage de ces données avec la clé privée correspondante. En dehors de cela, le schéma PKC peut également être appliqué dans la génération de signatures numériques. En substance, le processus consiste à hacher un message (ou des données numériques) avec la clé privée du signataire. Puis, le destinataire du message peut vérifier si la signature est valide en utilisant la clé publique fournie par le signataire. Dans certaines situations, les signatures numériques peuvent inclure un chiffrement, mais ce n'est pas toujours le cas. Par exemple, la blockchain Bitcoin utilise la PKC et les signatures numériques, mais contrairement à ce que beaucoup de monde a tendance à croire, il n'existe pas de chiffrement dans le processus. Techniquement, Bitcoin déploie l'Algorithme de signature numérique Elliptic Curve Digital Signature Algorithm (ECDSA) pour authentifier les transactions.

2.4.6 Hachage de la Blockchain

Dans la chaîne de blocs, les hachages sont utilisés pour représenter l'état actuel du monde, ou pour être plus précis, l'état d'une blockchain. Ainsi, l'entrée représente tout ce qui s'est passé sur une chaîne de blocs, donc chaque transaction jusqu'à ce point, combinée avec les nouvelles données qui sont ajoutées. Cela signifie que la sortie est basée sur, et donc façonnée par, toutes les transactions précédentes qui ont eu lieu sur cette blockchain.

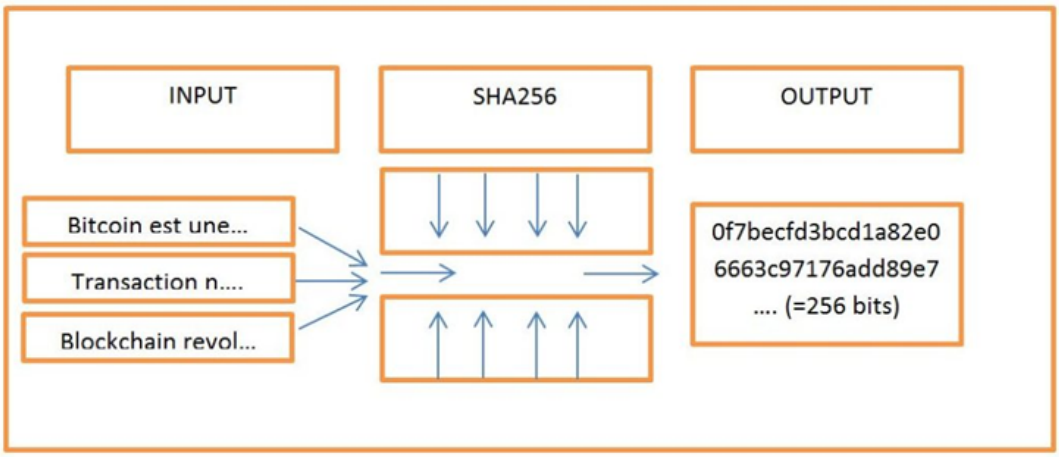

FIGURE 2.10 – Hachage de la Blockchain [10]

Comme nous l'avons mentionné, la moindre modification d'une partie quelconque de l'entrée entraîne une modification considérable de la sortie , c'est là que réside la sécurité irréfutable de la technologie de la blockchain. Changer n'importe quel enregistrement qui s'est déjà produit sur une blockchain changerait tous le hashage, les rendant faux et obsolètes. Cela devient impossible si l'on tient compte de la nature transparente de la blockchain, car ces changements devraient se faire en pleine vue de l'ensemble du réseau. Le premier bloc d'une blockchain, appelé bloc de genèse, contient ses transactions qui, une fois combinées et validées, produisent un hachage unique. Ce hachage et toutes les nouvelles transactions en cours de traitement sont ensuite utilisés comme entrée pour créer un tout nouveau hachage qui est utilisé dans le bloc suivant de la chaîne. Cela signifie que chaque bloc renvoie à son bloc précédent par le biais de son hachage, formant ainsi une chaîne vers le bloc de genèse, d'où le nom de blockchain.[10]

2.5 Merkle Tree

Un type spécial de structure de stockage de données basé sur des fonctions de hachage est appelé arbre de Merkle : - Il est structuré comme un arbre binaire ; les feuilles contiennent les valeurs à stocker et chaque nœud interne est le hachage de ses deux enfants. - Il fournit des recherches efficaces et une protection contre la falsification, car la vérification d'une transaction est incluse dans l'arborescence. Peut être accompli en envoyant uniquement la transaction, le hachage contenu dans chaque nœud entre le nœud feuille de transaction et la racine, ainsi que les valeurs de hachage utilisées pour créer chaque hachage envoyé. -La recherche d'une

transaction dans une arborescence Merkle à trois niveaux inclut l'envoi de deux transactions (celle souhaitée et l'autre enfant de son parent) et de trois hachages (le parent de la transaction, la racine et l'autre enfant de la racine).[20]

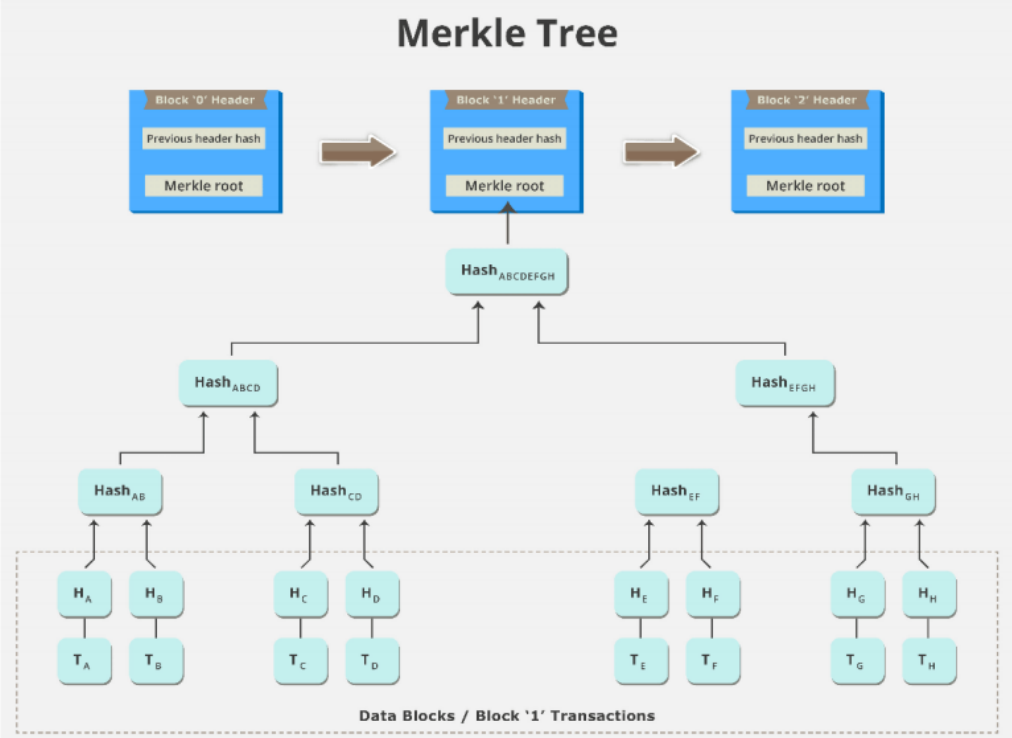

FIGURE 2.11 – Merkle Tree [20]

2.6 Les avantages de l'utilisation de la blockchain dans le monde médical

Certaines des fonctionnalités qui permettent aux blockchains de crypto-monnaie d'agir comme un enregistrement sécurisé des transactions financières sont également applicables au stockage de données médicales. Étant donné que la plupart des blockchains sont conçues comme des systèmes distribués qui enregistrent et protègent les fichiers grâce à la cryptographie, il est extrêmement difficile pour une personne de perturber ou de modifier les données sans l'approbation de tous les autres participants du réseau. L'immutabilité est donc l'une des caractéristiques permettant la création de bases de données incorruptibles pour les dossiers médicaux. De plus, l'architecture de pair-à-pair utilisée dans les chaînes de blocs permet de synchroniser toutes les copies de l'enregistrement d'un dossier médical au fur et à mesure de sa mise à jour, même si elles sont stockées sur différents ordinateurs. En réalité, chaque nœud du réseau détient une co-

pie de la blockchain complète et communique régulièrement pour garantir que les données sont à jour et authentiques. Ainsi, la décentralisation et la distribution des données sont également des aspects importants pour le monde médical. Il est à noter que les blockchains sont distribuées mais pas toujours décentralisées (en termes de gouvernance). La décentralisation n'est pas une opération binaire, donc en fonction de la manière dont les nœuds sont distribués et de l'architecture globale, les systèmes distribués peuvent présenter des degrés de décentralisation variables. Dans le contexte de la santé et du monde médical, les blockchains sont généralement conçues en tant que réseau privé, par opposition aux réseaux publics qui sont généralement utilisés comme registres pour les crypto-monnaies. Tandis que n'importe qui peut rejoindre et contribuer au développement d'une blockchain publique, les versions privées nécessitent une autorisation et sont gérées par un nombre de nœuds plus réduit.[18]

2.6.1 Une sécurité accrue

Comme indiqué précédemment, l'un des cas les plus importants d'utilisation des blockchains dans l'industrie médicale consiste à exploiter la technologie afin de créer une base de données sécurisée et unifiée entre homologues (et donc distribuée). Grâce à l'immutabilité des blockchains, la corruption des données ne devrait donc plus être un problème. La technologie blockchain peut de cette façon être utilisée pour enregistrer et suivre efficacement les données médicales de milliers de patients.

Contrairement aux bases de données traditionnelles qui reposent sur un serveur centralisé, l'utilisation d'un système distribué permet un échange de données avec des niveaux de sécurité accrus, tout en réduisant les coûts administratifs imposés par le système actuel. La nature décentralisée des blockchains les rend également moins vulnérables aux défaillances techniques et aux attaques externes qui compromettent souvent des informations précieuses. La sécurité fournie par les réseaux blockchain peut être particulièrement utile pour les hôpitaux, qui doivent souvent faire face aux intrusions de pirates informatiques et à des attaques par ransomware (ou rançongiciel).[18]

2.7 Conclusion

La blockchain peut se définir comme étant le moyen technologique pour redonner confiance à un système monétaire défaillant

Chapitre 3

Conception

3.1 Introduction

Avant de commencer à coder la partie applicative, nous nous intéressons à la phase de spécification pour bien définir, clarifier les grandes fonctionnalités de notre application.Ce chapitre consiste à donner une définition précise des besoins fonctionnels et non fonctionnels ainsi que les objectifs visés.

3.2 Sujet du projet (Objectif)

L'objectif principal est de produire la confidentialité pour victimisation des dossiers médicaux des patients « Blockchain La technologie". Le secret ou la confidentialité des informations sur les patients en est un parmi les piliers essentiels de la drogue. Protéger les données personnelles d'un patient n'est pas simplement une question de respect éthique, il est essentiel de créer des liens confiance entre le médecin et le patient.

3.3 Conception de l'architecture

3.3.1 Identification des diagrammes

nous allons identifier trois diagrammes :

3.3.2 Diagramme de cas utilisation :

Un diagramme de cas d'utilisation (UML) est un diagramme comportemental défini et créé à partir d'une analyse de cas d'utilisation. Son but est de représentent un aperçu graphique des fonctionnalités fournies par un système en termes d'acteurs et de dépendances éventuelles. le L'objectif principal d'un diagramme de cas d'utilisation est de montrer comment le système les fonctions sont exécutées pour quel acteur. Rôles des acteurs dans le système peut être décrit comme ci-dessous

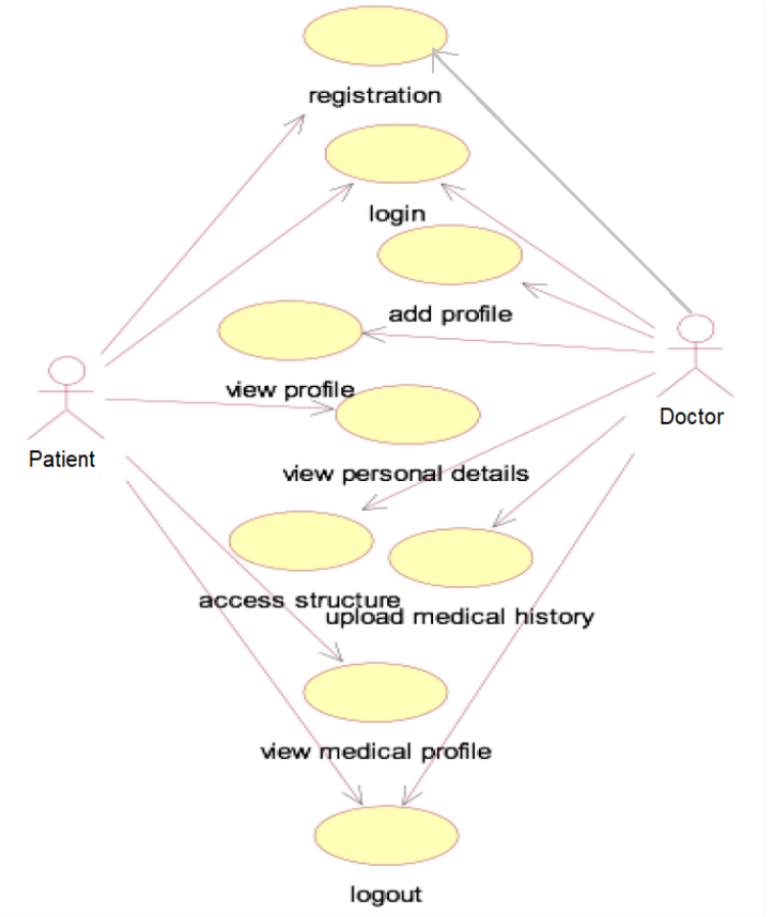

FIGURE 3.1 – diagramme de cas utilisation

3.3.3 Diagramme de séquence :

Les activités décrites dans la séquence début du diagramme après que toutes les entités ont été enregistrées et le les dossiers médicaux ont été envoyés au patient. La séquence des actions est la suivante :

1. Le patient génère une clé symétrique par rapport au dossier médical pour effectuer le cryptage. La clé publique

du patient est utilisé pour crypter la clé symétrique. Le dossier médical crypté et le les fichiers de clés symétriques sont téléchargés sur le serveur décentralisé stockage et le hachage du dossier médical crypté le fichier est stocké sur la chaîne.

2. Le médecin interroge les dossiers médicaux disponibles. Cette communication a lieu hors chaîne. Une fois la le médecin décide de ce dont les dossiers médicaux ont besoin (sur la base les métadonnées enregistrées), le patient est averti par un demande de données. Le patient décide s'il accepte la demande ou la refuser, ce qui se fait en envoyant le réponse comme une transaction à leur PRSC personnel.

3. Dans le cas où un patient accepte la demande, le patient génère une clé de re-chiffrement et l'envoie au PRSC. À ce stade, ce contrat intelligent informe le médecin et les oracles qu'une demande pour les données a été accordée.

4. Les oracles récupéreront le fichier demandé à partir de blockchain. Le fichier est téléchargé sous forme de bundle, qui contient à la fois les données du dossier médical et la clé symétrique cryptée. La tâche des oracles est de calculer le hachage de la clé symétrique chiffrée et l'envoyer au contrat intelligent patient.

5. Sur la base de plusieurs réponses d'oracles, le PRSC détermine quel oracle a eu la bonne réponse. Ceci est décidé en comparant les hachages de clé et en déduisant quel oracle a fourni la réponse la plus rapide. Basé sur ces deux facteurs, ainsi que la réputation antérieure de les oracles, le système choisit l'oracle le plus réputé. À ce stade, un jeton est envoyé à la fois au médecin et à l'oracle sélectionné.

6. Le médecin demande le dossier médical au oracle sélectionné en soumettant le jeton. Après avoir reconnu l'exactitude du jeton, l'oracle recrypter la clé symétrique à l'aide du re-cryptage clé générée par le patient, elle devient donc cryptée par la clé publique du médecin

qui a initié la demande. Une fois le processus de re-chiffrement terminé, l'ensemble du dossier médical est envoyé au médecin.

7. Le médecin décrypte la clé symétrique recryptée en utilisant leur clé privée, révélant la clé symétrique en texte clair qui a été utilisée pour crypter le dossier médical. Ensuite, le médecin décrypte le dossier médical à l'aide du clé symétrique en texte clair, obtenant ainsi l'original des données de dossier médical lisibles.

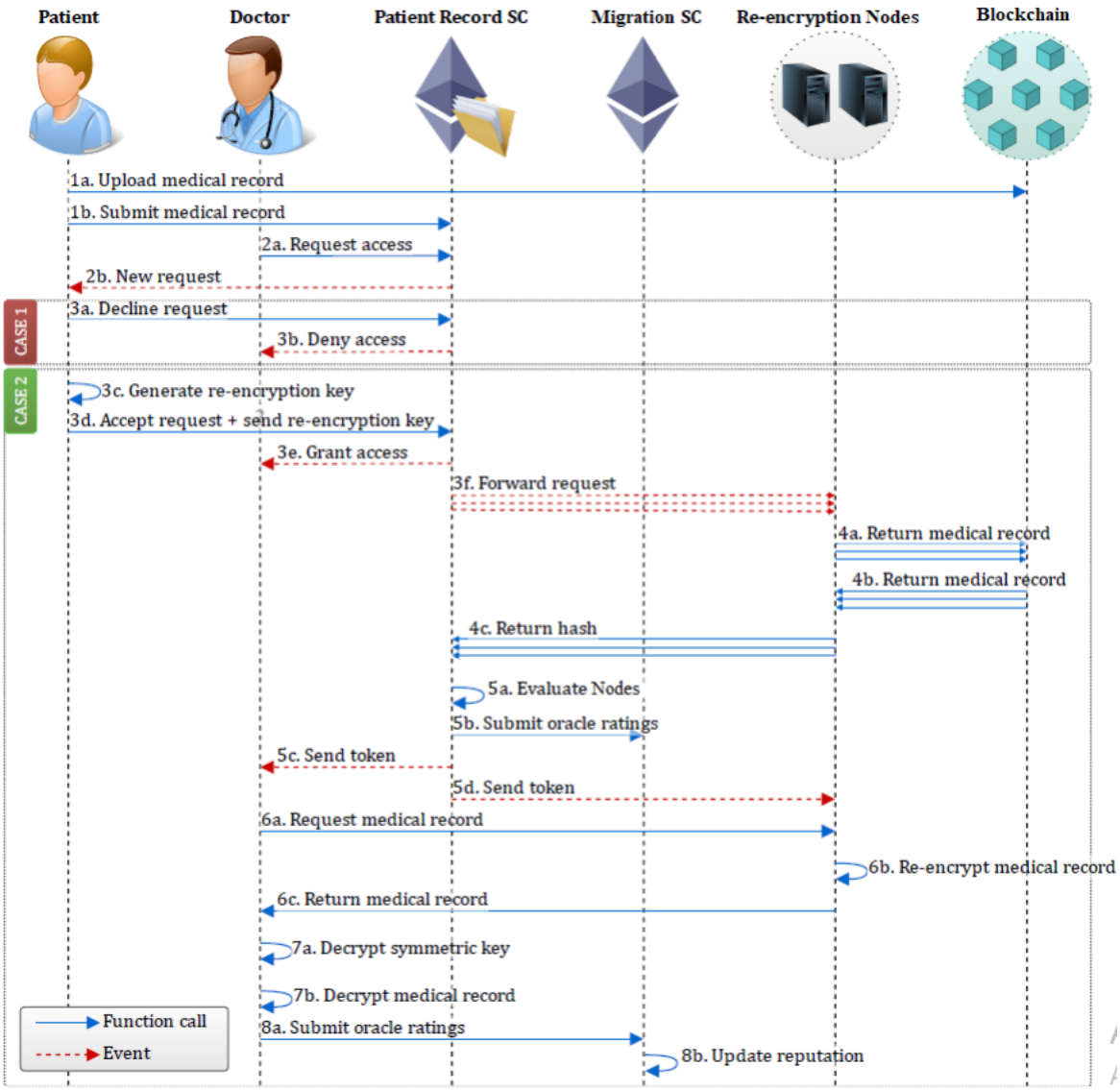

FIGURE 3.2 – Diagramme de séquence

3.3.4 architecture globale :

L'architecture MedBloc. Un « client P » est le service client des patients et un « client HP » est le service client des prestataires de soins de santé. Administrateurs réseau contrôler le serveur d'authentification, l'autorité de certification et l'ensemble du réseau Blockchain. Le réseau Blockchain est composé de plusieurs nœuds. Lignes pleines avec les flèches représentent le processus système (simplifié) lorsqu'un HP tente d'ajouter un nouveau dossier pour un patient. Les lignes pointillées avec des flèches représentent le processus du système lorsqu'une patiente tente de consulter ses dossiers.

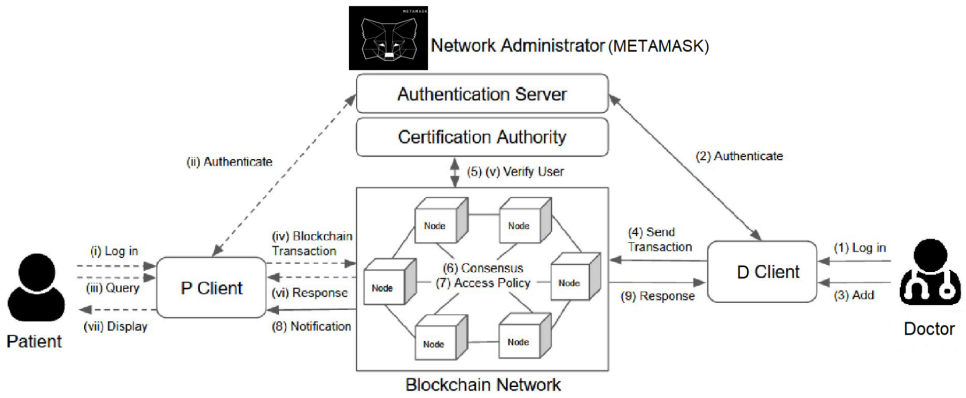

FIGURE 3.3 – Conception globale

3.4 Conclusion

Dans ce chapitre, nous avons identifié les diagrammes de cas d'utilisation, d'activités et de classes pour faciliter la réalisation de notre prototype. Dans le chapitre suivant nous montrerons les étapes, plus en détails, que nous avons suivies pour implémenter et réaliser notre solution.

Chapitre 4

Réalisation et implémentation

4.1 Introduction

Après avoir terminé la conception de notre système d'information, nous passons à la dernière phase de notre étude, qui est l'implémentation, dans ce chapitre nous allons pré senter les outils utilisés pour le développement de notre application "Blockchain et cryptomonnaie" et les interfaces les plus importantes de l'application.

4.2 Environnement de travail

L'environnement de travail est constitué par deux parties nommées environnement matériel et environnement logiciel.

4.2.1 Environnement matériel

Le développement de l'environnement matériel est caractérisé par :

- **Système d'exploitation :** Système d'exploitation Windows 10 64 bits.
- **Micro-Ordinator portable acer :** Pentium(R),Intel (R) CPU N4200 @ 1.10 GHz
- **Mémoire RAM :** 4 Go

4.2.2 Environnement logiciel

L'environnement logiciel consiste les composants suivants :

ganache

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

Ganache est disponible en deux versions : une interface utilisateur et une interface de ligne de commande. Ganache UI est une application de bureau prenant en charge les technologies Ethereum et Corda. L'outil en ligne de commande, ganache-cli (anciennement appelé TestRPC), est disponible pour le développement d'Ethereum.[9] Lorsque Ganache démarre, l'écran Ganache apparaît comme indiqué ci-dessous :

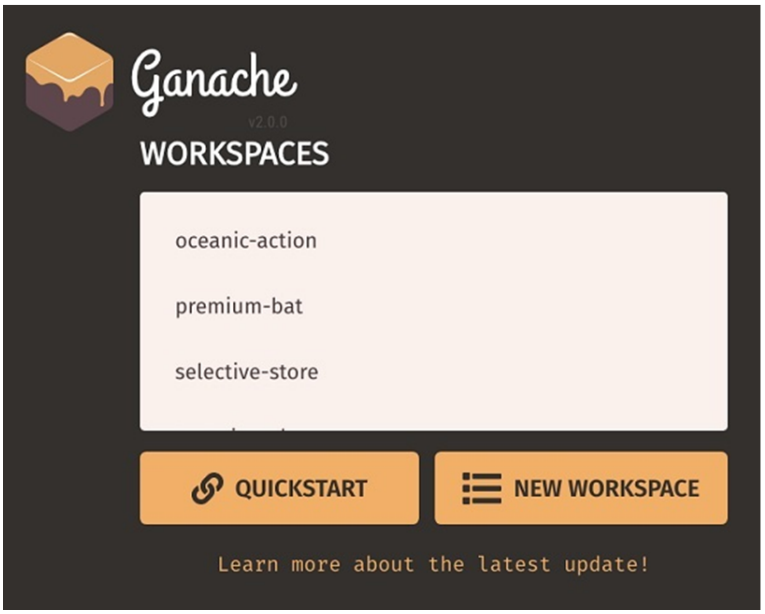

FIGURE 4.1 – Ganache espace de travail

Cliquez sur QUICKSTART pour démarrer Ganache. Vous verrez la console Ganache comme indiqué dans la figure 4.1 .

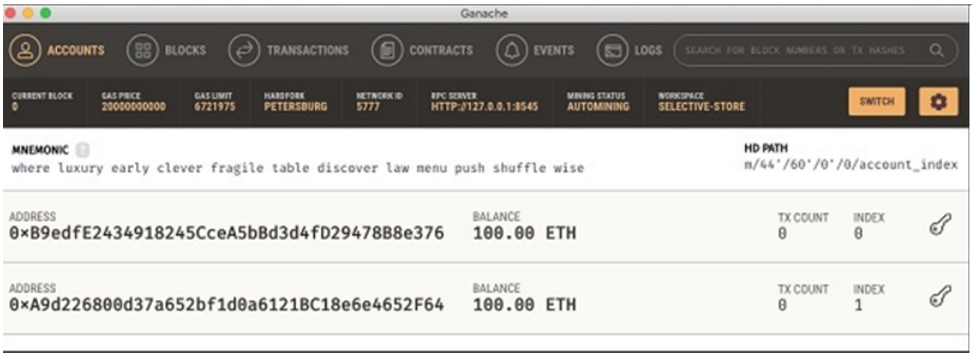

FIGURE 4.2 – Les comptes

La console dans la figure 4.2 montre deux comptes d'utilisateur avec un solde de 100 ETH (Ether - une devise pour les transactions sur la plate-forme Ethereum). Il affiche également un nombre de transactions de zéro pour chaque compte. Comme l'utilisateur n'a effectué aucune transaction jusqu'à présent, ce décompte est évidemment nul.

Node.js

Nœud. js est une plate-forme construite sur l'environnement d'exécution JavaScript de Chrome pour créer facilement des applications réseau rapides et évolutives. Nœud. js utilise un modèle d'E/S non bloquant basé sur les événements qui le rend léger et efficace, parfait pour les applications en temps réel gourmandes en données qui s'exécutent sur des appareils distribués. Node.js fournit également une riche bibliothèque de divers modules JavaScript qui simplifie considérablement le développement d'applications Web utilisant Node.js.[27]

MetaMask

est un portefeuille Ethereum permettant de gérer de l'Éther (ETH) ainsi que tous les jetons fonctionnant sur la blockchain Ethereum comme le Binance Coin (BNB) ou le Basic Attention Token (BAT). Mais ce n'est pas seulement un portefeuille : c'est également un navigateur Ethereum qui vous donne la possibilité d'interagir avec des applications décentralisées d'Ethereum directement depuis votre navigateur internet. Elle laisse les sites web récupérer les données de la blockchain et permet à ses utilisateurs de gérer leurs différents portefeuilles de façon sécurisée.

Utiliser MetaMask permet de diminuer fortement les risques d'hameçonnage (phishing) ou de vol par des sites webs corrompus car votre clé privée reste dans MetaMask. MetaMask

dispose de plus d'un outil anti-phishing avec une liste de sites webs corrompus mise à jour très régulièrement.

À l'heure actuelle, cette extension est disponible sur 4 navigateurs : Chrome, Firefox, Opera et Brave.[21]

4.3 Implémentation

Langages de programmation :

Javascript

est un langage de programmation principalement utilisé pour créer des pages web interactives. Ce langage, incorporé dans un document HTML, n'est pas visible dans la fenêtre du navigateur. Il sert à améliorer le Langage html en effet, il permet d'exécuter des commandes du côté client (c'est-à-dire au niveau du navigateur et non du serveur web). Ce code qui est exécuté par le navigateur Web est utile pour toutes les interactions du client sur la page Web. Ce langage permet de manipuler des objets au sens informatique : créer des fenêtres spécifiques, contrôler les données saisies dans les formulaires, redimensionner certains objets, rediriger des liens.[13]

HTML (Hyper Text Markup Language)

L'HTML est le format de données conçu pour représenter les pages web. C'est un langage de balisage permettant d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des programmes informatiques. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation (JavaScript) et des formats de présentation (feuilles de style en cascade). HTML est initialement dérivé du Standard Generalized Markup Language(SGML) .[12]

CSS

est un langage utilisé pour rendre attrayante la présentation des pages HTML. C'est un concept présent dès l'origine du web. Il nous aide à décrire l'apparence que devra avoir notre site : la couleur et la police de texte, la taille des titres, les marges, la position des menus, etc.[6]

Solidity

Solidity est un langage haut-niveau, orienté objet dédié à l'implémentation de smart contracts. Les contrats intelligents (littéralement contrats intelligents) sont des programmes qui régissent le comportement des comptes dans l'état d'Ethereum.[32]

4.4 Les commendes à exécuter

Déplacez-vous dans le répertoire du projet puis exécutez (en cmd) :-

•**truffle compile**

•**truffle migrate –reset**

•**npm run dev**

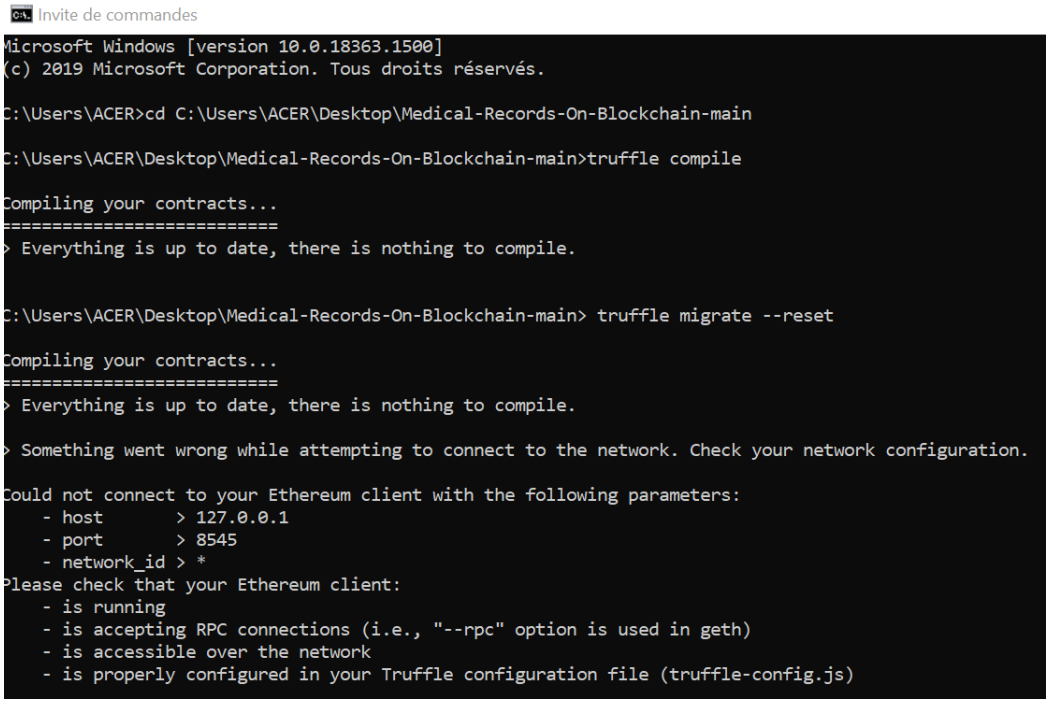

FIGURE 4.3 – Les commandes à exécuter

4.5 Développement de l'application

Dans cette partie, nous allons présenter les différentes phases de la réalisation de notre projet en mentionnant des imprimes écrans de notre application.

4.5.1 la forme choisir un profile

La figure suivante montre La Forme choisir un profile :

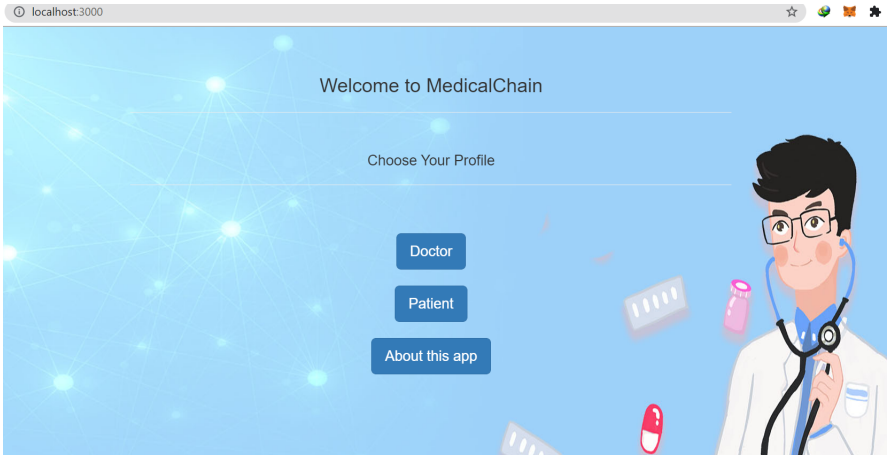

FIGURE 4.4 – Choisir un profile

4.5.2 la forme clé privé d' un compte

La figure suivante montre La Forme clé privé d' un compte :

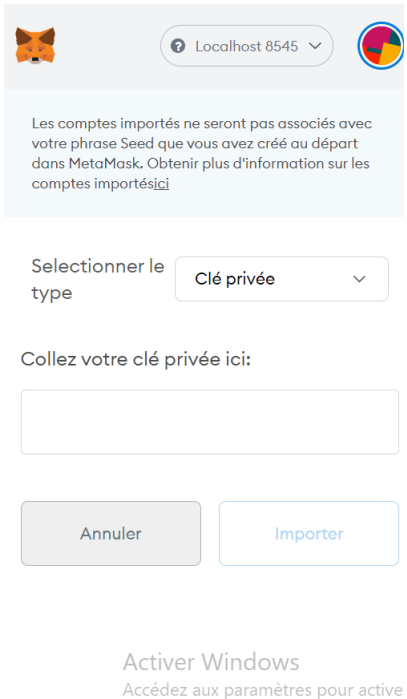

FIGURE 4.5 – Clé privé d' un compte

4.5.3 La forme information sur le compte

La figure suivante montre La Forme information sur le compte :

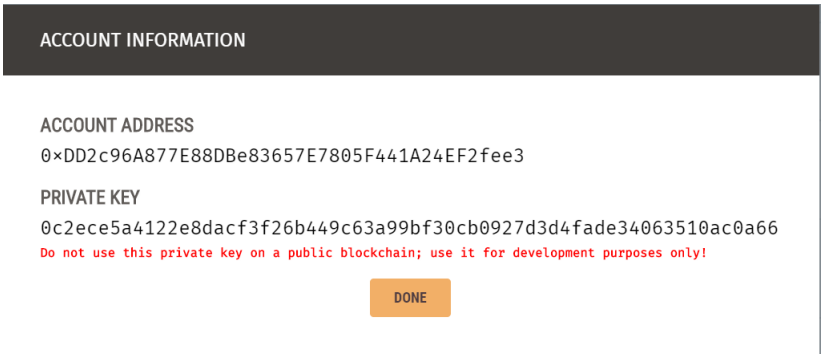

FIGURE 4.6 – Informaton sur le compte

4.5.4 La forme informations sur l'application

La figure suivante montre La Forme informations sur l 'application :

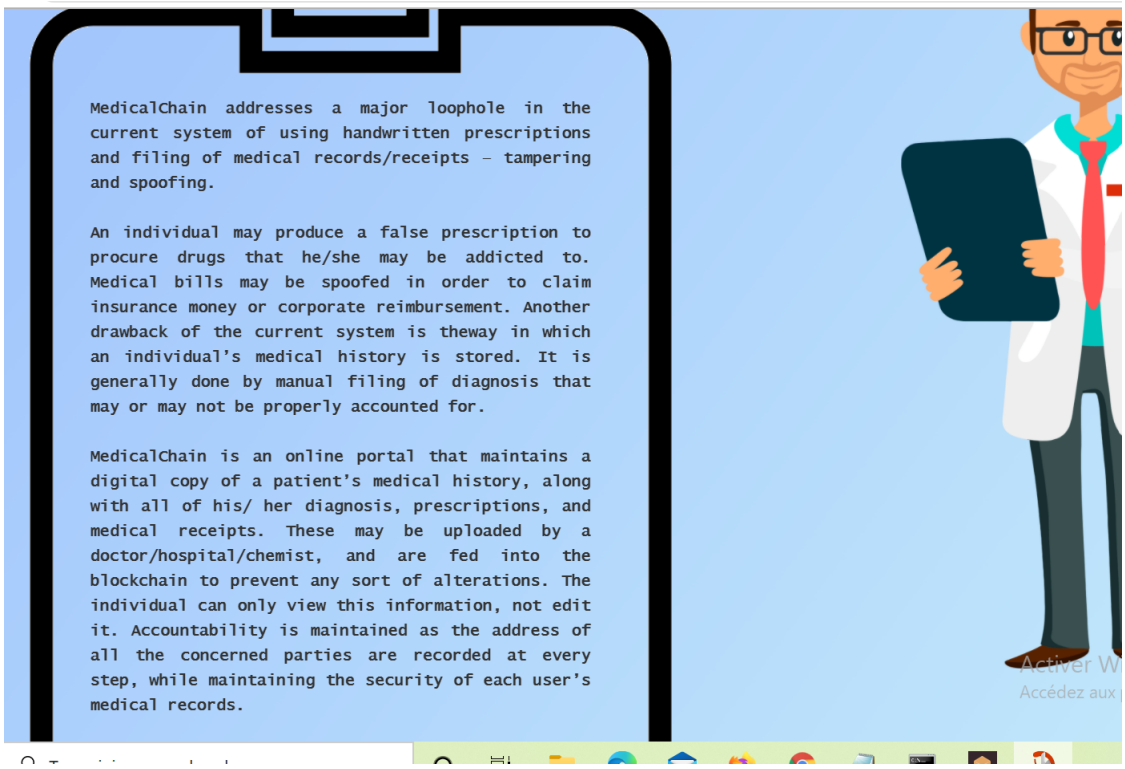

FIGURE 4.7 – Informattion sur l' application

4.5.5 La forme page d'accueil des médecins

La figure suivante montre La Forme page d' accueil des médecins :

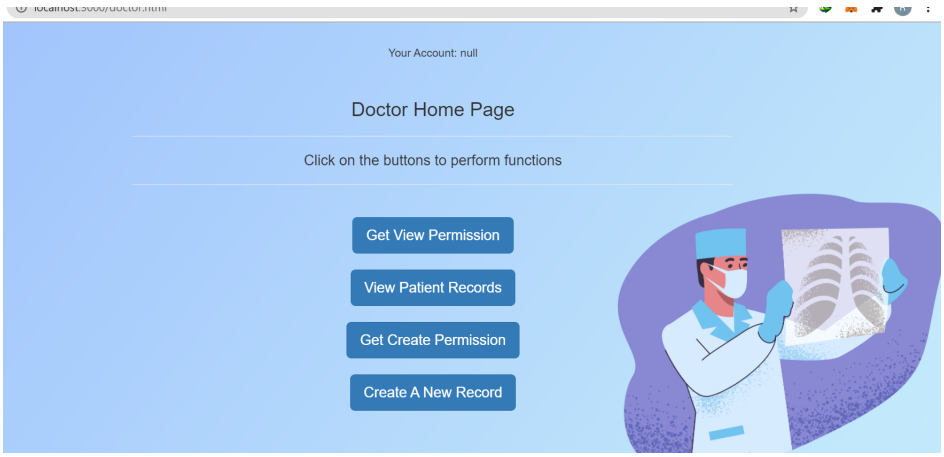

FIGURE 4.8 – page d'accueil des médecins

4.5.6 La forme page d'accueil des Patients

La figure suivante montre La Forme page d 'accueil des patients :

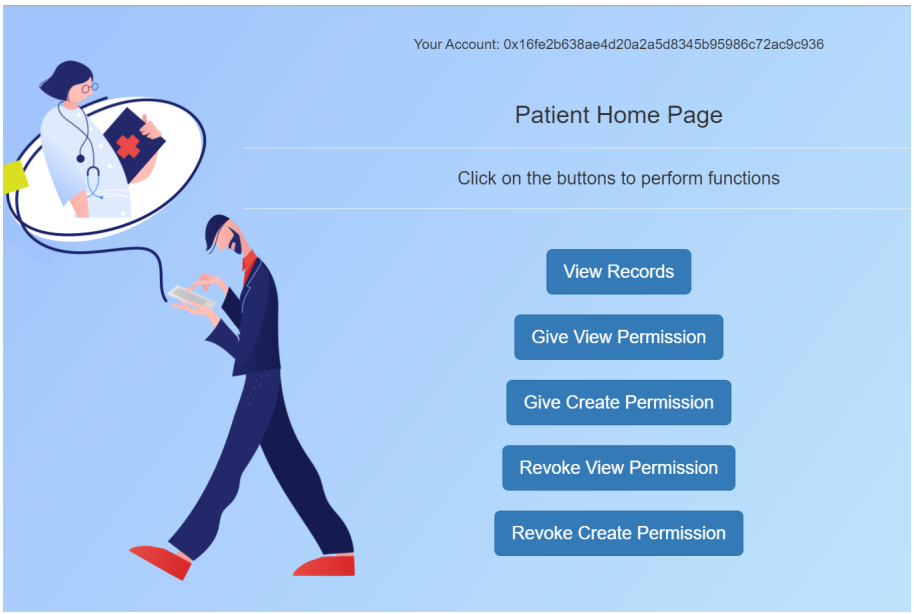

FIGURE 4.9 – page d'accueil des Patients

4.5.7 La forme confirmation

La figure suivante montre La Forme iconfirmation :

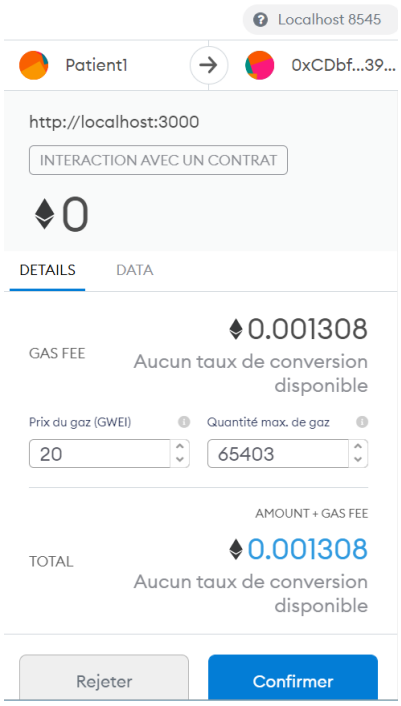

FIGURE 4.10 – Confirmation

4.5.8 La forme créer un nouvel enregistrement

La figure suivante montre La Forme créer un nouvel enregistrement :

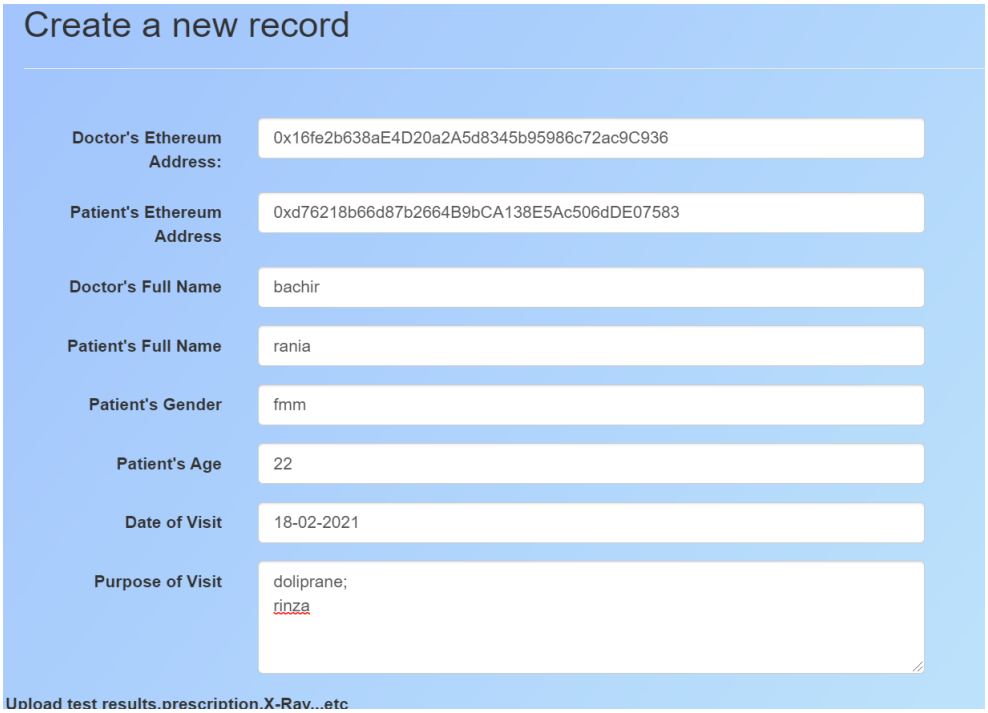

FIGURE 4.11 – créer un nouvel enregistrement

4.5.9 La forme choisir un fichier

La figure suivante montre La Forme choisir un fichier :

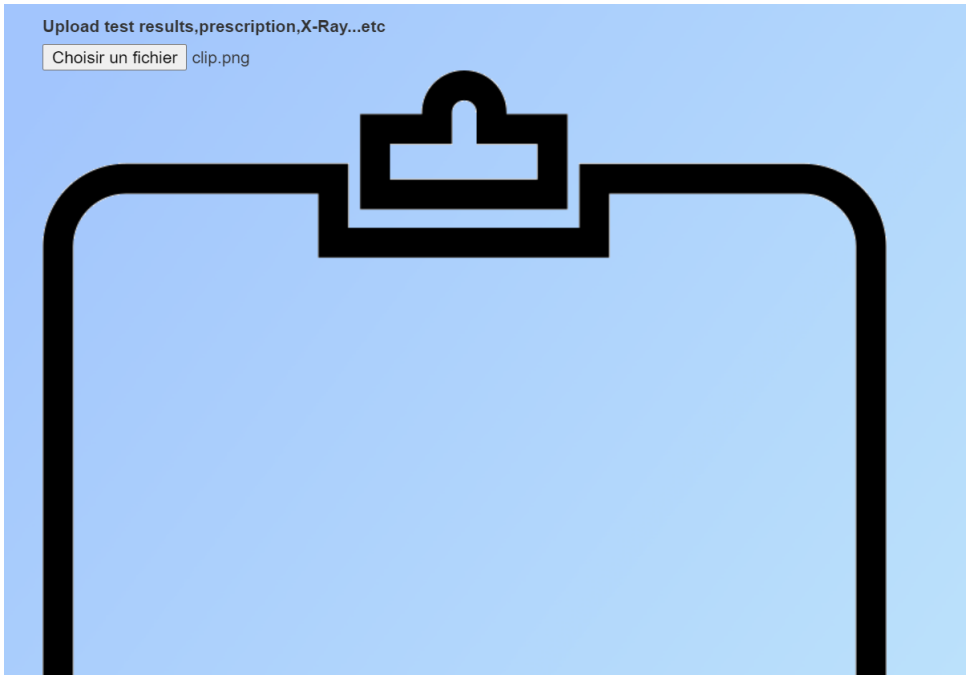

FIGURE 4.12 – Choisir un fichier

4.5.10 La forme résultats

La figure suivante montre La Forme résultas :

FIGURE 4.13 – Résultats

4.5.11 La forme révoquer l'autorisation d'affichage

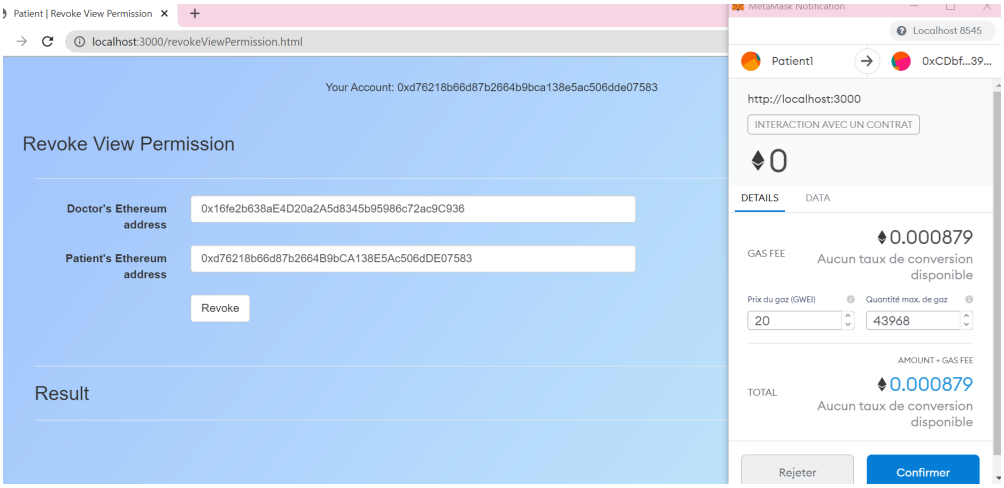

FIGURE 4.14 – révoquer l'autorisation d'affichage

4.5.12 La forme révoquer l'autorisation de création

La figure suivante montre La Forme révoquer 'autorisation de création :

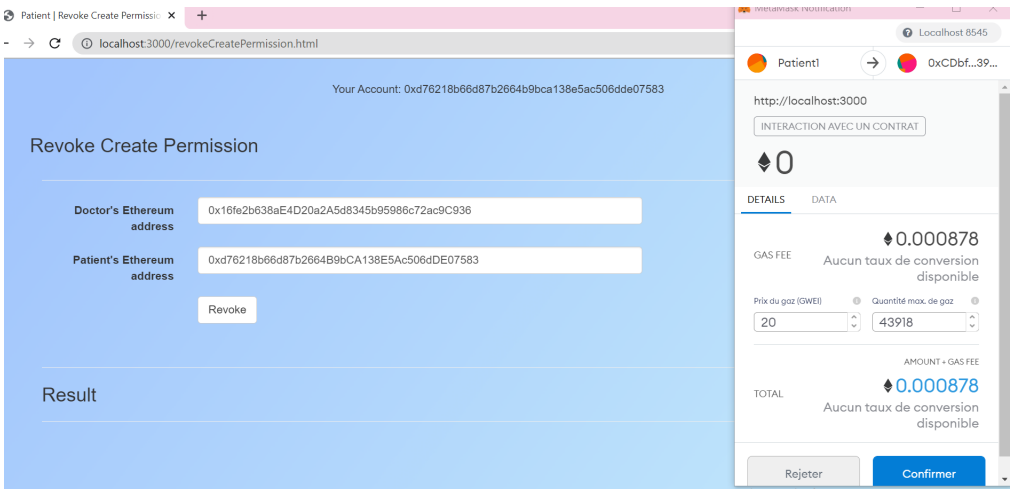

FIGURE 4.15 – révoquer l'autorisation de création

4.6 Conclusion

On a vu dans ce chapitre les outils utilisés pour le développement, on a montré aussi quelques interfaces dans le but de donner une vision globale sur le fonctionnement de notre système.

Conclusion générale

Avec les avantages de la technologie, tels que le la transparence, la confiance, la copie multiple des transactions et le grand livre numérique décentralisé, la technologie Blockchain est fiable et non destructible, et toutes les attaques mentionnées pourraient perturber le fonctionnement du système, pas la technologie. La blockchain la technologie est utile et polyvalente pour notre monde, car elle peut faciliter la plupart des systèmes dans les différentes industries, mais il est nouveau et sa mise en œuvre est une question peu étudiée sur la pratique.

La technologie Blockchain nous promet un bel avenir sans la fraude et la tromperie en raison des avantages de la Technologie blockchain. Les développeurs doivent consacrer plus de temps à l'application pratique et à la mise en œuvre de la Blockchain dans les systèmes déjà existants de la principale directions industrielles, car la Blockchain peut apporter les des systèmes commerciaux, gouvernementaux et logistiques honnêtes et fiables.

À l'avenir, les développeurs peuvent penser aux systèmes amélioration pour augmenter les avantages de la Blockchain technologie et réduire les inconvénients. Par exemple, la réduction de la puissance de calcul pour le processus d'extraction et l'aspect financier de la mise en œuvre de la Blockchain pourrait être mentionné.

Enfin, il est nécessaire d'introduire les cours pratiques à les établissements d'enseignement pour la formation à construire leur propre Système Blockchain et voir tout le processus de la Blockchain application et utilisation de la technologie.

Bibliographie

[1] A.Lewis. *Ledger distribué et Blockchain.* URL : https://bitsonblocks.net/2017/02/20/whats-thedifference-between-a-distributed-ledger-and-ablockchain/.

[2] *Centralisée vs décentralisé.* URL : https://fr.bitdegree.org/crypto/tutos/centralisation-et-decentralisation.

[3] *Comment fonctionnent les blockchains ?* URL : https://coin24.fr/dictionnaire/blockchain/.

[4] "composition d' une Blockchain". In : (). URL : https://academy.binance.com/fr/articles/history-of-blockchain.

[5] Thibault Coussin. "Cryptomonnaie". In : *Investir avec succès dans Bitcoin et les cryptomonnaies* ().

[6] *Css.* URL : https://www.memoireonline.com/11/13/7812/m_Conception-et-realisation-d-un-portail-web--l-intention-des-differents-acteurs-burundais9.html.

[7] E. B. @eliasb"V. G. M. @malyala- venu D. B. @dmitry-buterin et B.-A. H. @amonra. *"Proof of Work vs Proof of Stake : Basic Mining Guide," Blockgeeks, 15-Mar-2017. [Online].*

[8] *définition de la Blockchain.* URL : %7Bhttps://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/%7D.

[9] *Ganache.* URL : https://www.tutorialspoint.com/ethereum/ethereum_ganache_for_blockchain.html.

[10] *Hachage de la blockchain.* URL : https://www.crypto-sous.fr/blockchain-fonctionnement/hashing/..

[11] *Historique*. URL : https://academy.binance.com/fr/articles/history-of-blockchain.

[12] *Html*. URL : https://www.techno-science.net/glossaire-definition/Hypertext-Markup-Language.html.

[13] *JavaScript*. URL :]%20http://www.gralon.net/articles/internet-et-webmaster/creation-site-internet/article-javascript---%20presentation-et-applications-1776.htm.

[14] *La notion de réseau pair à pair*. URL : http://www.senat.fr/rap/r17-584/r17-584_mono.html.

[15] "La signature numérique". In : (). URL : https://academy.binance.com/fr/articles/what-is-a-digital-signature.

[16] Tiana LAURENCE. "Role du blockchain". In : *Blockchain pour les Nuls* ().

[17] *Ledger distribué et BlockChain*. URL : Internet:%20http://www.investopedia.com/terms/d/distributed-ledgers..

[18] "Les avantages de l'utilisation de la blockchain dans le monde médical". In : *Cas d'utilisation de la Blockchain : le monde médica* (). URL : https://academy.binance.com/fr/articles/blockchain-use-cases-healthcare.

[19] *Les transactions*. URL : https://blog.ippon.fr/2018/01/08/fonctionnement-dune-blockchain/.

[20] *Merkle tree*. URL : https://fr.bitdegree.org/crypto/tutos/centralisation-et-decentralisation.

[21] *Metamask*. URL : https://www.trade-and-opportunity.com/tutoriel-metamask/.

[22] Sayedli MIRJALILI. "Proof of stake". In : *Proof of Stake - Bitcoin Wiki.* (2017). URL : https://en.bitcoin.it/wiki/Proof%20of%20Stake..

[23] N.SZABO. *Formalizing and securing relationships on public networks.*, URL : http://%20rstmonday.org/ojs/index.php/fm/article/view/548/4691%20[Accessed%2015/02/2017]..

[24] S. NAKAMOTO. In : *Bitcoin : a peer-to-peer electronic cash system* (2008).

[25] S. NAKAMOTO. *Bitcoin : A peer-to-peer electronic cash system.* 2008.

[26] S. NAKAMOTO. *Bitcoin : A peer-to-peer electronic cash system.* 2008.

[27] *Node.js*. URL : https://www.tutorialspoint.com/nodejs/nodejs_introduction.htm.

[28] "P". URL : https://paritytech/parity/wiki/Proof-of-Authority-Chains..

[29] Christophe DEBONNEUIL Matthieu QUINIOU. *Blockchain.* 2019.

[30] M. Riguidel. *Quelque rappels sur les techniques cryptographiques*. 2000.

[31] *Signification*. URL : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203399-p2p-peer-to-peer-definition-traduction-et-acteurs/.

[32] *Solidity*. URL : https://solidity-fr.readthedocs.io/fr/latest/.

[33] F. Tschorsch et B. Scheuermann. "Essentiel bitcoin". In : *Bitcoin and beyond : a technical survey on decentralized digital currencies," IEEE Communications Surveys and Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016* ().

[34] G. Zennor. *L'usage de la cryptographie*. 2002.