Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option : Réseaux et Systèmes Distribués (R.S.D)

Thème

Contrôle d'accès sécurisé dans les systèmes de télésanté

Réalisé par :

- *Yadel Abdelhakim*

Présnté le 03 juillet 2022 devant le jury de :

Mr Benmammar Badr	*(Président)*
Mr Benmouna Youcef	*(Examinateur)*
Mme Amraoui Asma	*(Encadrante)*
Mme Zerga Hidayet	*(Co-Encadrante)*

Année universitaire :2021-2022

Remerciements

Nos remerciements s'adressent à Dieux tout puissant qui nous a donné le courage, la force et les moyens pour réussir et donner le meilleur de nous-mêmes.

Nous ne saurions oublier de remercier nos parents pour leur contribution, leur soutien et leur patience, nos proches, nos amis et toutes les personnes qui nous ont aidé par leur soutien permanent dans nos études ou en dehors. À notre Encadrante Madame Amraoui Asma et notre Co-encadrante Madame Zerga Hidayet pour leur encadrement, leur soutien sans faille et leur disponibilité, leurs conseils, leurs commentaires, leurs corrections et leur qualités scientifiques ont été très précieux pour mener à bien ce travail.

Nous remercions chacun des membres du jury d'avoir consacré une partie de leur temps à la lecture de ce mémoire et pour l'intérêt porté à notre travail en acceptant de l'examiner.

Notre reconnaissance va particulièrement au chef du département et l'ensemble des enseignants du département d'Informatique pour tout ce qui nous a été transmis tout au long de notre formation.

Dédicaces

Je dédie ce modeste travail :

À mon très cher père qui a toujours répondu présent dans les moments les plus difficiles. Son soutien et son encouragement m’ont toujours donné la force de poursuivre mes études.

À ma très chère maman, qui a su me donner l'attention, l'affection, l'aide et l'amour qui m'ont permis d'achever ce projet dans de bonnes conditions. Aucune dédicace ne pourra compenser les sacrifices de mes parents.

À tous ceux qui m'ont enseigné dans cette vie, les valeurs et la morale.

À mon très chère frère Yacine.

À mes très chères cousins,cousines Marwa , Mehdi, Sofiane, Zoubida, Yasmine,Hadjer, Neila , Akram, Lina, Hamza ,Selma ,Imene.

À mes très chères amis,amies Amine ,Mounir, Hadjer.

À tous mes camarades de la promotion.

À tous ceux et toutes celles qui m’ont soutenu de près ou de loin durant cette année.

Résumé :

Ce travail consiste à utilisé la technologie blockchain et les smarts contracts pour la gestion des dossiers électroniques médicaux (DEM) afin de rendre les données le plus privé possible pour le détenteur de ces ressources tout en lui laissant la liberté de choisir les acteurs qui peuvent y accéder à l'aide d'un système de contrôle d'accès contractuel bien établie. La réalisation de l'application s'est faite sous l'éditeur MICROSOFT VISUEL STUDIO en utilisant les langages de programmation JavaScript, HTML, CSS et le Framework Bootstrap pour le front-end et l'environnement de développement REMIX sous le langage SOLIDITY et le simulateur de la blockchain Ethereum GANACHE pour le back-end.

Mots clés: blockchain, contrôle d'accès, contrat intelligent, dossier électronique médical

Abstract :

This work consists of using blockchain technology and smart contracts for the management of electronic medical records (DEM) to make the data as private as possible for the holder of his resources while leaving him the freedom to choose the actors who can use it. accessed using a well-established contractual access control system. The realization of the application was done under the editor MICROSOFT VISUAL STUDIO using the JavaScript, HTML, CSS programming languages, and the Bootstrap Framework for the front-end and the REMIX development environment under the SOLIDITY language and theEthereumm GANACHE blockchain simulator for the back-end.

Keywords: blockchain, access control, smart contract, electronic medical record

ملخص

يتكون هذا العمل من استخدام تقنية blockchain والعقود الذكية لإدارة السجلات الطبية الإلكترونية (DEM) من أجل جعل البيانات خاصة قدر الإمكان لصاحب موارده مع ترك حرية اختيار الممثلين الذين يمكنهم استخدامها. الوصول إليها باستخدام نظام راسخ للتحكم في الوصول التعاقدي. تم تنفيذ التطبيق تحت محرر MICROSOFT VISUEL STUDIO باستخدام لغات البرمجة JavaScript و HTML و CSS و Bootstrap Framework

للواجهة الأمامية وبيئة تطوير REMIX تحت لغة SOLIDITY ومحاكاة GANACHE ethereum blockchain للواجهة الخلفية.

الكلمات المفتاحية: blockchain ، التحكم في الوصول ، العقد الذكي ، السجل الطبي الإلكتروني

Table des matières :

Table des figures :

Table des tableaux :

- **Liste des acronymes :**

ABI : Interface binaire d'applications

DAC : Contrôle d'accès discrétionnaire

DEM : dossiers électroniques médicaux

DDOS : Attaque par déni de service

DAPPS : Application décentralisé

EVM : Ethereum Virtual Machine

IDE: Environnement de développement

IoT : Internet des objets

IoMT : Internet des objets des objets médicaux

MAC : Contrôle d'accès obligatoire

ORBAC : Contrôle d'accès basé sur l'organisation

RBAC : Contrôle d'accès basé sur le rôle

TMAC : Contrôle d'accès basé sur TeamM

1. Introduction générale

- **Contexte**

La blockchain est un grand livre numérique qui regroupe et enregistre les transactions et les données impossible à effacer une fois graver dans l'un des blocs de cette chaine de bloc à l'aide de ses mineurs qui sont là à vérifier et confirmer les blocs en suivant un consensus précis pour faire l'unanimité au jugement de ce bloc, c'est-à-dire accepté ou refusé.

La blockchain est une technologie révolutionnaire qui permet l'intégrité, la sécurité, la traçabilité de ses données à l'aide de son système de vérification décentralisé et indépendant de toutes entités extérieures. Avec ses mineurs dispersés dans le monde, la blockchain met dans l'ombre la plupart des réseaux centralisés actuels et qui s'ouvre à quasiment tous les secteurs. Mais son principal avantage est l'intégration des contrats intelligents qui peuvent exécuter automatiquement les termes d'un contrat. Lorsque la condition préconfigurée dans un contrat intelligent entre les entités participantes est remplie, puis les parties impliquées dans un accord contractuel peuvent être automatiquement payées conformément au contrat dans une manière transparente.

C'est pour toutes ces raisons qu'on a choisi de vous présenter cette application qui a pour but de contrôler l'accès aux données dans le domaine d'e-santé à l'aide de la technologie Blockchain.

- **Problématique**

Lorsqu'une société veut mettre un système sécurisé pour permettre l'authentification elle se tourne généralement vers des solutions centralisées, mais ses données sont facilement falsifiables et le coût est parfois élevé, pour préserver une sécurité élevée en utilisant par exemple l'authentification facile où biologique.

- **Contribution**

Afin d'établir un mécanisme de contrôle d'accès via la blockchain, nous allons passer par deux étapes essentielles à savoir l'enregistrement de chaque utilisateur pour accéder aux ressources via son contrat intelligent et ensuite la demande d'accès aux données médicales.

Chaque acteur géré par la blockchain doit posséder un contrat intelligent pour pouvoir accéder à la ressource, ce contrat doit être créé par l'acteur qui possède l'information et qui veut partager avec les différents acteurs dans la blockchain, dans ce contexte le médecin ou l'infirmier aura l'accès aux données médicales.

- **Organisation du rapport**

Ce document est constitué de trois chapitres, ainsi qu'une introduction générale et une conclusion générale.

Dans le premier chapitre, nous allons faire une présentation sur l'E-santé et l'internet des objet IoT, nous allons parler sur le développement des deux domaines ainsi que la relation entre eux.

Dans le deuxième chapitre, nous parlerons de la blockchain et ses principaux points fort et ses caractéristiques, nous montrons l'importance de la sécurité des données médicales et le contrôle d'accès en utilisant les contrats intelligents.

Dans le troisième chapitre, nous allons présenter la plateforme Ethereum et la blockchain ainsi que le développement et déploiement des contrats intelligents pour contrôler l'accès, les différents outils utilisés pour l'environnement de développement ainsi la présentation de l'algorithme de contrôle d'accès, et enfin un test sur notre application.

I. CHAPITRE 1 : INTERNET DES OBJETS ET E-SANTÉ

I.1 Introduction

La forte croissance des objets médicaux connectés a fondamentalement transformé le secteur de la santé. Qu'il s'agisse d'objets connectés à usage personnel - une montre connectée enregistrant le rythme cardiaque par exemple – ou à usage médical pour améliorer la prise en charge, le traitement ou la réactivité en cas de donnée anormale, tous ces équipements de tous types qui recueillent et transmettent des données sur la santé des patients, sont regroupés sous le terme générique "Internet des objets Médicaux" ou IoMT. [1]

L'IoMT constitue une partie de l'internet des objets (IoT) axée sur les soins de santé et englobe tout un système de dispositifs médicaux, de logiciels et de systèmes et services de soins de santé interconnectés qui échangent des données en temps réel au moyen de technologies de mise en réseau. Leur mise en œuvre massive dans le secteur de la santé suppose de relever un certain nombre de défis. [1]

L'Internet des objets (IoT) transforme actuellement les soins de santé tels que nous les connaissons. Les appareils connectés génèrent et transmettent des données pour améliorer les résultats des patients, rendre les lieux de travail et les workflows plus efficaces, réduire les erreurs médicales et même permettre aux bâtiments de répondre davantage aux besoins des personnes qui l'occupent. [2]

En raison de leur capacité à accéder en temps réel aux dossiers médicaux partout et depuis n'importe quel appareil, les appareils connectés sont parfois des cibles privilégiées pour les pirates. La protection de la confidentialité des patients est primordiale [2]

Dans ce chapitre, nous allons définir la notion d'IoT avec ses domaines d'application et nous nous intéresserons au domaine de l'e-santé particulièrement où nous donnerons ses impacts sur la vie quotidienne.

I.2 IoT (internet des objets)

I.2.1 Définition

L'internet des objets désigne l'ensemble des infrastructures technologiques utilisées pour mettre en lien les objets technologiques et institué une communication et connexion à l'aide de la connexion internet.

La figure I-1 représente les objets connectés :

Figure I-1 Illustration visuelle des objets connectés

Les objets peuvent variées d'appareils physique de tous les jours comme une machine à lavé, télé … jusqu'aux systèmes plus complexes comme les avions, les voitures … Chaque objet pilotable à distance détient sa propre carte d'identité qui le rend unique et reconnaissable, dans la plupart des cas une adresse IP. C'est ce numéro d'identification numérique qui va permettre de trouver cet objet et de lui donner des instructions à partir d'un ordinateur ou d'un téléphone portable.

I.2.2 Domaines d'application

Les secteurs d'application de l'IoT sont assez vastes parmi les principaux secteurs :

- **Fabrication**

Dans le monde de l'industrie l'IoT bénéficie les fabricants d'un avantage considérable sur la détection des problèmes de fonctionnement ou de panne à l'aide des capteurs en communication constante qui stop la production et désigne le dispositif à changer pour assurer la fluidité de la production et diminuer les coups tout en gagnant du temps et le personnel.

- **Automobile**

L'IoT est utilisé de plus en plus dans le monde de l'automobile avec l'intelligence l'intégration de l'intelligence artificiel et tous les gadgets mis en disposition permet une autonomie quasi-totale du véhicule. Ou bien même en fournissant des informations de l'extérieur comme les problèmes de circulation ou autre ou bien des informations sur l'état du véhicule et ses besoins.

- **Transport et logistique grande distribution**

Les systèmes de transport et de logistique bénéficient d'une grande diversité d'applications IoT. Les parcs de voitures, camions, navires et trains qui transportent du stock peuvent être réacheminés en fonction des conditions météo, ou encore de la disponibilité des véhicules ou des chauffeurs grâce aux données issues des capteurs IoT. Le stock lui-même peut également être muni de capteurs en vue de son suivi, ou à des fins de contrôle de température. Les secteurs agro-alimentaire, floral et de l'industrie pharmaceutique transportent souvent un stock sensible aux variations de températures. Ceux-ci bénéficieraient largement d'applications IoT de contrôle qui envoient des alertes lorsque les températures augmentent ou baissent à un niveau dangereux pour le produit. [3]

- **Secteur public**

Les avantages de l'IoT dans secteur publique le rendent indispensable une des exemples de l'utilisation de l'IoT est le système conçu par certains services publics qui peuvent rentrer en contacte et avertir leurs utilisateurs à grande échelle de coupure d'électricité où autre, ou bien un autre exemple de dispositif IoT qui peuvent aider à récolter des informations suite à une défaillance.

- **Santé**

La surveillance des actifs par IoT offre de nombreux avantages au secteur de la santé. Médecins, infirmières et aides-soignants doivent souvent connaître la localisation exacte des actifs d'assistance aux patients, tels que les fauteuils roulants. Lorsqu'un fauteuil roulant d'hôpital est équipé de capteurs IoT, il peut être suivi à partir de l'application de surveillance, de telle sorte qu'un soignant qui en a besoin peut rapidement trouver le fauteuil roulant disponible le plus proche. De nombreux actifs d'hôpital peuvent être suivis ainsi afin de garantir une utilisation correcte, ainsi que la prise en compte financière des actifs physiques dans chaque service. [3]

I.2.3 Architecture de l'internet des objets

L'architecture d'un système IoT est composée de plusieurs niveaux qui communiquent entre eux pour relier le monde tangible des objets au monde virtuel des réseaux et du cloud. Tous les projets

n'adoptent pas une architecture formellement identique, néanmoins il est possible de schématiser le parcours de la donnée.

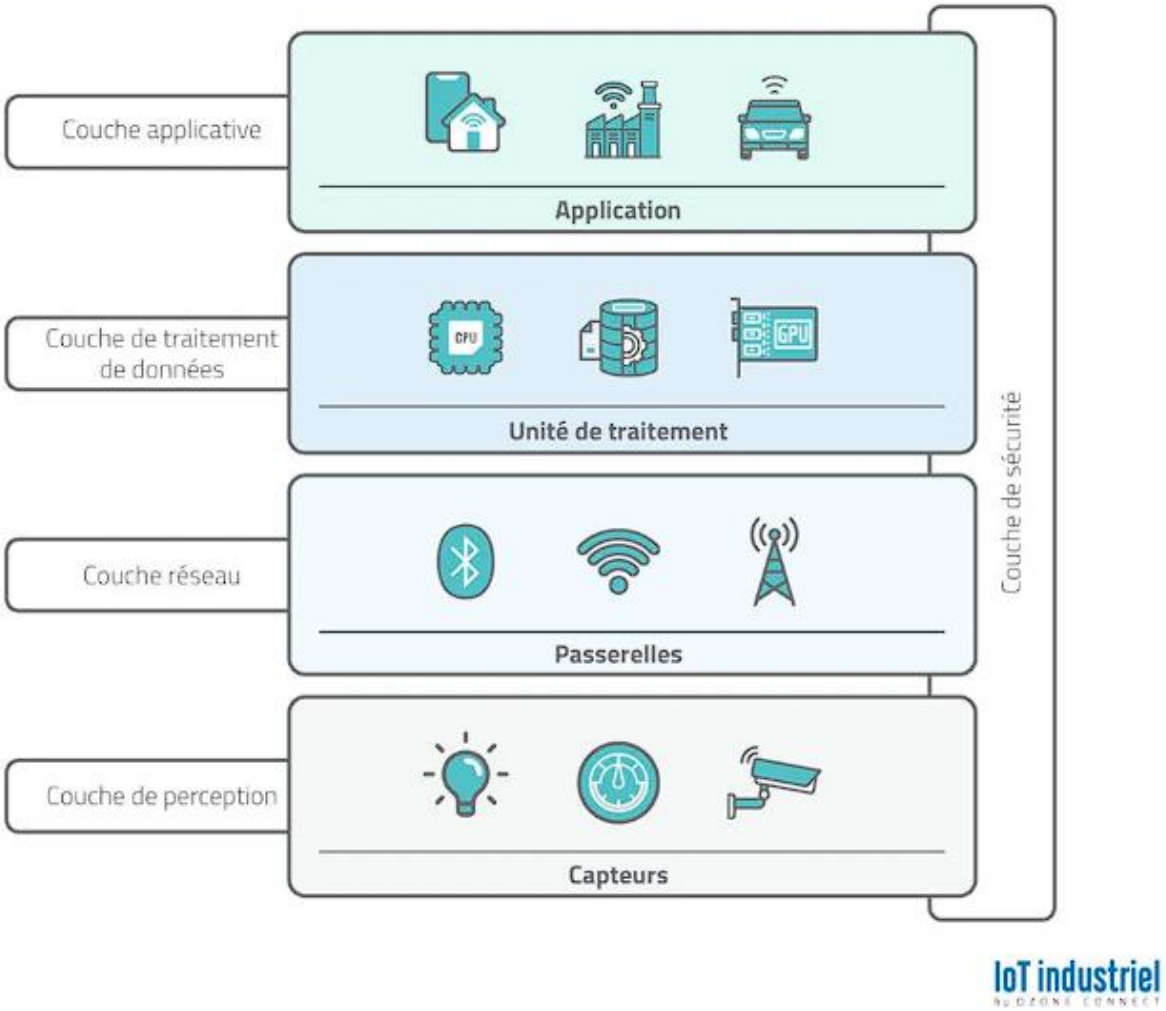

Figure I-2 l'architecture de l'IoT

La figure I -2 illustre l'architecture de l'IoT qui est composée de 4 blocks essentiel :

- **Couche de perception**

Constitué de capteurs qui ont pour rôle de récolter des informations, muni d'un système d'exploitation ils envoient ses données à travers des passerelles vers l'unité de traitement.

- **Couche réseaux**

Elle sert de passerelle entre la couche de traitement et la couche de perception à l'aide de plusieurs technologies réseaux tel que l'internet, les réseaux cellulaires, les réseaux Bluetooth …

- **Couche de traitements de données**

C'est la partie la plus importante de ce système puisque c'est le cerveau qui traite les données et les transmet de façon intelligente aux objets finaux pour aller au bout du processus.

- **Couche application**

La couche finale constituée d'objets qui sont là pour recevoir les instructions et les informations fournies par l'unité de traitement.

I.2.4 Vulnérabilités et menaces dans l'internet des Objets

- **Chaque objet connecté à un potentiel exploitable caché :**

Même si votre cafetière a pour tâche première de faire du café, son système d'exploitation est capable de faire beaucoup plus en arrière-plan. Sachant cela, un hacker peut s'introduire dans une entreprise ou chez un particulier par ce biais. [4]

- **Objets connectés oubliées** :

Ces objets, comme les alarmes ou les détecteurs de mouvement sont conçus pour fonctionner pendant des années. On a donc tendance à les oublier lors des tournées de maintenance. C'est une erreur de notre part, et une aubaine pour les cybercriminels ! [4]

- **Donner moins d'importance sur la sécurité des objets moins importants** :

Les cybercriminels s'en prennent de plus en plus à ces catégories, et s'intéressent davantage à l'écriture de données plutôt qu'à la lecture. Par exemple dans une usine, un cybercriminel n'a aucun avantage à retirer du piratage du débit d'un tuyau. En revanche, s'il en prend le contrôle, il pourrait changer ce débit et provoquer un incident. Nous n'imaginons même pas ce qu'il pourrait se passer sur des objets connectés dans le milieu médical ! [4]

- **Manque de la sécurisation des objets par les fabricants :**

Certains objets ne sont même pas calibrés pour pouvoir changer leur mot de passe. La plus importante des vulnérabilités provient souvent des fabricants eux-mêmes. [4]

I.3 E-santé (la santé numérique)

I.3.1 Définition

La E-santé ou la santé électronique est l'ensemble des moyens liés à la santé qui utilisent les technologies de communication et de l'information, internet élu le meilleur moyen de ses derniers avec l'intégration des applications pour smartphones et les objets connectés, le secteur de la santé ne cesse d'aller vers l'avant et de progressé.

I.3.2 Impacts potentiels de l'e-santé

- **Impact économique :**

Après l'apparition du COVID-19 le secteur de l'E-santé a connu une croissance sans nom, avec une réduction de frais inconsidérable due au personnel médical, l'entretient où autre.

- **Disponibilités :**

La télémédecine permet l'accès à distance d'un patient à un professionnel de la santé

- **Efficacité :**

L'efficacité des structures de soins est décuplée et l'expérience des patients améliorée grâce au numérique et à l'automatisation

- **Fiabilité :**

La décision médicale et paramédicale est rendue plus fiable et sûre avec l'aide de l'intelligence artificielle

- **Fluidité :**

La circulation des informations médicales entre professionnels est fluidifiée au bénéfice des patients, par la dématérialisation des échanges.

I.3.3 Risques potentiels de l'e-santé

Avec les systèmes et les applications assez centralisées actuelles le partage de données sensible entre le patient et le médecin au billet de l'internet expose le patient à un potentiel de piratage où de falsification de données sensibles.

Le problème le plus courants est le phishing attack qui a pour but de récolter les informations sur le mot de passe du client en se prenons pour le site officiel de l'entreprise, alors qu'avec la technologie blockchain le problème est vite réglé avec les adresses privées pour le contrôle d'accès

à l'espace client de manière automatique une fois que le compte du client sur la blockchain est relié au smart contract.

I.4 Internet des objets et E-santé

L'Internet des objets médicaux (IoMT), qui fait partie des technologies de l'Internet des objets (IoT), englobe les appareils et les applications interconnectés utilisés dans l'informatique médicale et de santé. Les appareils IoMT connectent les patients, les médecins et les appareils médicaux (équipements hospitaliers, équipements de diagnostic et technologie portable) en transmettant des informations sur un réseau sécurisé. [5]

Les nouvelles technologies de l'information et de la communication sont au cœur de l'évolution de notre système de santé et facilitent la circulation d'informations entre les différents acteurs. Les Big Data et l'Internet des Objets ouvrent des perspectives inédites de gains d'efficacité, que cela soit dans les domaines de la recherche, de la prévention, de la compréhension des maladies ou de l'efficacité des médicaments. L'analyse des données collectées par les médecins, l'hôpital ou par les patients eux-mêmes via des objets connectés permet de les contextualiser et leur croisement contribue à forger une image plus précise de la problématique analysée. [6]

I.5 Conclusion

L'IoT est en train d'améliorer la qualité des services de E-santé et même de la santé en général en changeant la manière de collecter les informations et les données dans les hôpitaux, les cliniques… et de mettre en œuvre des automatismes et des analyses assez poussés qui améliorent la qualité de service et le professionnalisme du personnel médical et mettre à disposition le confort nécessaire au travail ce qui les rend plus efficaces. Les données recueillies auprès de ces appareils peuvent ensuite être analysées par l'organisation pour :

• Améliorer les soins aux patients, en offrant des prestations de soins nouvelles ou améliorées et des services pour permettre aux organismes de santé gérant des données de se différencier de la concurrence. [7]

• Optimiser les processus, en développant de nouveaux services et solutions qui augmentent l'efficacité et réduisent les coûts d'exploitation. [7]

• En savoir plus sur les besoins et les préférences des patients, permettant aux organismes de santé d'offrir de meilleurs soins et une expérience de soins personnalisée. [7]

II. CHAPITRE 2 : BLOCKCHAIN ET CONTRÔLE D'ACCÈS

II.1 Introduction

Depuis le temps, la sécurité informatique est convoitée et recherchée par toutes les organisations qui veulent s'assurer de : l'intégrité de leurs données (garantir que les données sont bien celles que l'on croit être), la disponibilité (maintenir le bon fonctionnement du système d'information) et La confidentialité (rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction) tous en garantissent l'accès aux utilisateurs légitimes.

Cependant il existe au jour d'aujourd'hui le cloud Security une façon de rendre les données un peu plus sécurisées mais totalement centralisé, contrairement à la blockchain qui rend le processus totalement décentralisé.

La figure II-1 représente le cloud computing centralisé vs décentralisé :

Figure II-1 Le cloud computing centralisé vs décentralisé

La blockchain est une approche décentralisée contrairement aux services actuels qui permettent le stockage de données et la transmission d'informations de manière centralisé. Elle utilise un type de réseau informatique Pair à Pair pour garantir une décentralisation et une protection optimal.

II.2 Blockchain

II.2.1 Définition

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. [8]

Comme son nom l'indique la blockchain est une chaine de bloque où chaque block représente un registre constitué d'information vérifié au préalable par les vérificateurs (appelé aussi mineurs) du réseau, qui ont pour but de s'assurer de la nature et de l'existence de l'information. Une fois le registre totalement vérifié et sécurisé il se lie au bloque précédent à l'aide de leurs numéros d'identification spécifique à chaque block ou bien d'utiliser la dernière information du précédent block comme spécificité de liaison avec le nouveau block.

La figure II-2 représente un exemple sur un registre de blockchain :

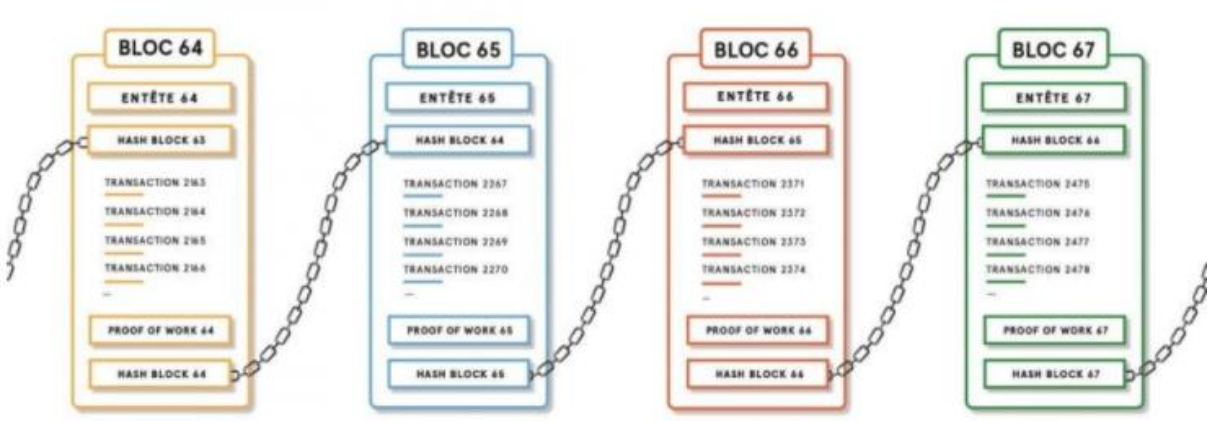

Figure II-2 : Registre de la blockchain

Un block comporte généralement 3 parties :

1-partie Données/Informations

2-Hash-ID unique du block

3-Hash précédent-Hash du bloc précédent

La figure II-3 représente un exemple sur l'architecture d'une blockchain :

Figure II-3: Architecture de la blockchain

Chaque nœud du réseau contient une copie de ce registre enregistré impossible a modifiée ou a supprimé une fois l'information vérifié et signé. Chaque ajout d'information sur le registre du nœud déclenche une mise à jour général du registre de chaque nœud du réseau.

La grande spécificité de la technologie blockchain est que chaque information inscrite est cryptée et cachetée par un numéro de série unique à l'aide de la cryptographie.

II.2.2 Les types de blockchain

Il existe 3 types de blockchain :

- La blockchain publique :

C'était le premier type de blockchain qui existait, et il se réfère à des blockchains qui sont accessibles au public depuis Internet, ce type de blockchain garde ses données, ses logiciels de développement ouverts au public afin que chacun puisse les revoir, les auditer, les développer ou les améliorer. Pour y parvenir, les blockchains publiques ont des mesures de sécurité qui garantissent qu'aucun acteur malveillant ne peut facilement modifier le fonctionnement de celles-ci. En bref, toute mesure qui contribue à améliorer la sécurité du réseau y est mise en œuvre. Le but de tout cela est de maintenir le réseau en marche et de préserver sa décentralisation. [9]

Ses principales caractéristiques :

- Permet à n'importe qui de faire partie
- Le fonctionnement du réseau est complètement transparent et ouvert
- Il n'y a pas d'entités centralisé

- La Blockchain privé :

Plus tard, avec l'évolution de la technologie blockchain et son expansion, de nombreuses entreprises s'y sont intéressées. Cela a conduit au développement de solutions de blockchain privées ou autorisées. Ce type de blockchain a généralement les mêmes éléments qu'une blockchain publique, mais contrairement à ceux-ci, les blockchains autorisées dépendent d'une unité centrale qui contrôle toutes les actions en son sein. Cette unité centrale est ce qui permet l'accès aux utilisateurs, en plus de contrôler leurs fonctions et autorisations au sein de la blockchain. Ce sont généralement des options de développement de logiciels propriétaires, bien qu'il existe également des développements de logiciels libres. L'un des développements les plus importants de la blockchain privée dans le monde de la cryptographie est **Hyperligue**. Ce projet a commencé par le **Fondation Linux** et plusieurs entreprises du secteur technologique sont le meilleur exemple de blockchain privée. On peut également citer le cas de **Corde** de **R3** o **Quorum** de **JPMorgan** [9]

Ses principales caractéristiques :

- L'accès au réseau est autorisé que par l'unité central de contrôle.
- L'accès à l'information est privé.
- L'accès aux différentes informations de la Blockchain se fait généralement par une hiérarchie au sein de l'entreprise.

- blockchain hybride :

Ce type de blockchain est une fusion entre les blockchains publiques et privées. C'est une tentative de tirer parti du meilleur des deux mondes. Dans ces blockchains, la participation au réseau est privée. Autrement dit, l'accès aux ressources du réseau est contrôlé par une ou plusieurs entités. Cependant, le registre est accessible au public. Cela signifie que n'importe qui peut explorer tout ce qui se passe sur cette blockchain bloc par bloc.

Par exemple, ces types de réseaux blockchain sont très utiles pour les gouvernements ou les entreprises qui souhaitent stocker ou partager des données de manière sécurisée. Un cas d'utilisation parfait se produit dans le secteur de la santé, où la blockchain est utilisée pour stocker les données de ses lignes de production de médicaments. Les données stockées peuvent être examinées par l'autorité compétente afin de contrôler la qualité, tant au niveau de l'entreprise elle-même que du gouvernement. L'objectif de l'application de ce modèle de blockchain est de maintenir un haut niveau de transparence et de confiance. [9]

Ses principales caractéristiques :

- L'accès au réseau est autorisé que par l'unité central de contrôle.
- L'accès à l'information est public**.**

II.2.3 Les caractéristiques d'une blockchain

1. Les données stockées dans la blockchain sont immuables et ne peuvent pas être modifiées facilement

2. La décentralisation totale du réseau, absence d'autorité centrale pour contrôler le réseau

3. La blockchain fournit un réseau Peer to Peer. Cette caractéristique de la blockchain supprime l'exigence d'« autorisation de tiers », car tout le monde dans le réseau est lui-même en mesure d'autoriser et vérifier les informations .

II.2.4 Application de la blockchain dans les soins de la santé

Le potentiel de la technologie de blockchain est visible dans les domaines de la médecine, de la génomique, de la télémédecine, de la télésurveillance, de la cyber santé, des neurosciences et des applications de soins de santé personnalisés, grâce à son mécanisme de stabilisation et de sécurisation de la série de données avec laquelle les utilisateurs peuvent interagir avec différentes interactions à travers différents types de transactions. [10]

La figure II-4 représente l'application des blockchains dans le domaines de la santé :

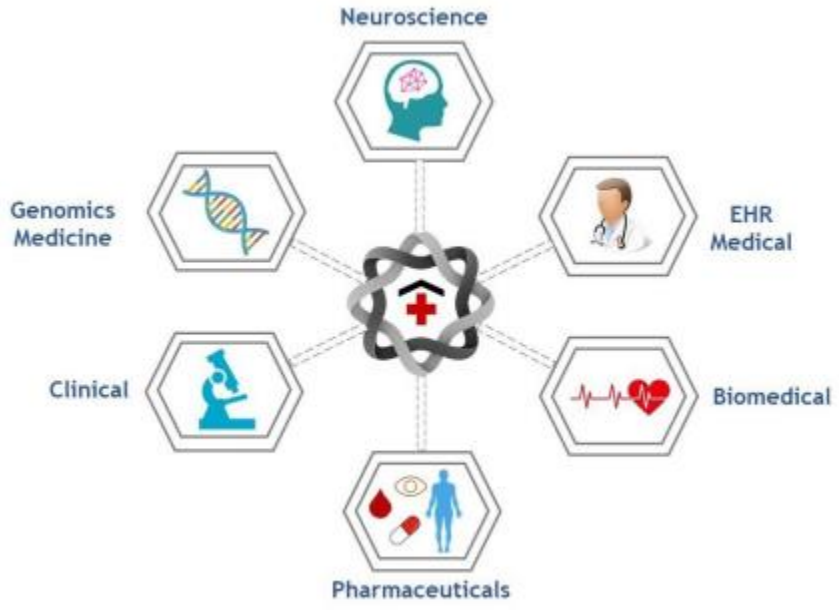

Figure II-4 : Application des blockchains dans le domaine de la santé

II.3 Contrôle d'accès

II.3.1 Définition

Le contrôle d'accès est un moyen de limiter l'accès à un système ou à des ressources physiques ou virtuelles. En informatique, le contrôle d'accès est un processus par lequel les utilisateurs se voient accorder l'accès et certains privilèges aux systèmes, ressources ou informations. [11]

Dans les systèmes de contrôle d'accès, les utilisateurs doivent présenter des informations d'identification avant de pouvoir leur accorder l'accès. Dans les systèmes physiques, ces informations d'identification peuvent prendre plusieurs formes, mais les informations d'identification qui ne peuvent pas être transférées offrent la plus grande sécurité. [11]

Pour la sécurité informatique, le contrôle d'accès comprend l'autorisation, l'authentification et l'audit de l'entité essayant d'accéder. Les modèles de contrôle d'accès ont un sujet et un objet. Le sujet - l'utilisateur humain - est celui qui essaie d'accéder à l'objet - généralement le logiciel. Dans les systèmes informatiques, une liste de contrôle d'accès contient une liste d'autorisations et les utilisateurs auxquels ces autorisations s'appliquent. Ces données peuvent être consultées par certaines personnes et non par d'autres personnes ,et sont contrôlées par le contrôle d'accès. Cela permet à un administrateur de sécuriser les informations et de définir des privilèges quant aux informations auxquelles on peut accéder, qui peut y accéder et à quelle heure elles peuvent être consultées. [11]

Catégorie :

Les quatre catégories principales de contrôle d'accès sont les suivantes :

- Contrôle d'accès obligatoire
- Contrôle d'accès discrétionnaire
- Contrôle d'accès en fonction des rôles
- Contrôle d'accès à base de règles

II.3.2 Les modèles

- DAC (Discretionary access control): Il est plus connu en français sous le nom de contrôle d'accès discrétionnaire. DAC est un modèle de contrôle d'accès dans lequel des moyens sont mis en place pour limiter l'accès aux données. Ce modèle permet à son utilisateur d'accorder l'accès à l'objet souhaité.
- MAC (Mandatory access control) : Le contrôle d'accès obligatoire est un système de contrôle d'accès dans lequel la décision de protection ne revient pas au propriétaire de cet outil.
- TMAC (Team based access control) : Ce système de contrôle d'accès est un modèle mettant en relation des utilisateurs ayant des rôles différents et travaillant en collaboration pour accomplir une tâche spécifique. [12]
- ORBAC (Organization Based Access Control) : Il s'agit d'un modèle fondé sur l'organisation datant de 2003 ayant pour politique d'autorisation de contrôler l'accès centré sur le concept d'organisation . [12]
- RBAC (contrôle d'accès basé sur le rôle) : c'est un concept de sécurité où les droits sont accordé en fonction du rôle de l'utilisateur dans l'entreprise.
  L'affectation se fait généralement en arrière plan par un administrateur chargé de la distribution des droits d'accès.

  La mise en œuvre d'un contrôle d'accès basé sur le RBAC optimise l'efficacité du système de sécurité , protège les données du vol , réduit le travaille des administrateur et laisse un champ d'enquête assez clair en cas de problème.

II.3.3 Les contrats intelligent

Les **contrats intelligents** (en anglais : ***smart contracts***) sont des protocoles informatiques qui facilitent, vérifient et exécutent la négociation ou l'exécution d'un contrat, ou qui rendent une clause contractuelle inutile (car rattachée au contrat intelligent). Les contrats intelligents ont généralement une interface utilisateur et émulent la logique des clauses contractuelles. Cependant, les contrats intelligents sont du code informatique, et si l'interface utilisateur venait à disparaître, il serait toujours possible d'interagir avec ceux-ci. Seul un arrêt du réseau sur lequel les contrats intelligents sont hébergés pourrait mener à son inaccessibilité. [13]

La nécessité d'avoir un intermédiaire(banquier, notaire …)pour fixer les termes du contrat entre deux personnes ne sera plus nécessaire puisque le smart contrat se déclenche automatiquement une fois tous les conditions sont réunis.

La figure II-5 représente les étapes de réalisation d'un contrat intelligent :

Figure II-5: Les étapes pour réaliser un smart contract.

II.3.4 Pourquoi utiliser les smart contract ?

La figure II-6 représente les bienfaits des contrats intelligents :

Figure II-6: Les bienfaits des smarts contracts

- Transparence :

Une fois les termes du contrat établie personne ne peux les modifiée qui oblige l'ensemble des parties concernées par le contrat à être **totalement transparent dans leurs démarches.**

- Vitesse :

Pour exécuter les contrats manuellement cela prend en moyenne des jours au smart contract qui s'exécute instantanément une fois les conditions respectées.

- Précision :

La formulation des contrats se fait de manière explicité et clair cela rend la tâche précise avec moins de risque contrairement au contrat manuel.

- Sécurité :

Grace a la technologie blockchain une fois un smart contact déployer il est impossible de le supprimer ou de le modifier ce qui l'es rendent totalement autonomes et cela permet à l'utilisateur d'avoir une confiance totale entre les utilisateurs

- Frais :

Les smarts contracts illuminent une grande partie intermédiaire qui peuvent coûter cher à l'utilisateur pendant la procédure de l'exécution du contrat (banquier, notaire …) ses honoraires dus aux intermédiaires ne sont plus nécessaires.

II.3.5 Utilisation de la Blockchain et les contrats intelligent pour les contrôles d'accès

Dans une blockchain chaque membres ou entités appartenant à son environnement a la caractéristique d'avoir une identité unique grâce au système de cryptographie des données et sa puissante capacité à préserver en toutes sécurité ses deniers.

Cependant, il existe plusieurs manières d'accéder à des services proposés par une société à l'aide de la blockchain et spécifiquement avec les contrats intelligents qui permettent de donner accès aux services aux utilisateurs éligible en passant par une condition définie par les développeurs afin de déclencher ce contrat.

II.3.6 Blockchain et Internet des objets

Dans la structure centralisée d'origine, les informations collectées et stockées par l'Internet des objets sont concentrées dans la base de données du fournisseur. Tant que le fournisseur en a besoin, il peut utiliser toutes les données de l'utilisateur à tout moment, et l'utilisateur ne le remarquera pas. Cependant, en utilisant l'architecture du réseau blockchain, les données sont

cryptées avant l'envoi des données et l'authentification est ajoutée avant toute opération. Tant qu'une opération sur les données personnelles est effectuée, les données doivent être déchiffrées par authentification d'identité. Autorisation, dans le même temps, les enregistrements des opérations et autres messages sont enregistrés sur le réseau blockchain et décentralisés .

À l'ère où les grandes entreprises ont un poids de données, toutes les données sont très précieuses. La blockchain est un ensemble de moyens de déterminer la propriété numérique. Toutes les choses numériques peuvent être facilement copiées à un coût nul. Afin de garantir que les données ne se propagent pas à un coût nul et n'affectent pas la formation du marché des données et du système de valeur, la blockchain fournit une garantie technique efficace pour la confirmation des droits de propriété des données. [14]

La figure II-7 représente un schéma représentatif du réseau IoT utilisant la Blockchain :

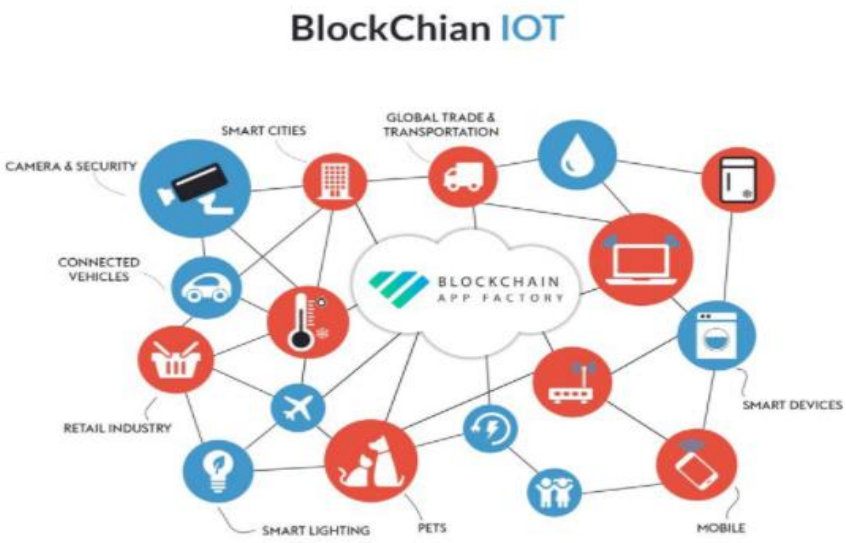

Figure II-7: Blockchain et IoT

II.3.7 Le contrôle d'accès dans l'internet des objets

L'Internet des objets (IoT)est un concept basé sur l'idée que tous nos objets de la vie quotidienne seront un jour connectés à Internet. En quelques années seulement depuis son apparition, il a été adopté dans divers secteurs grâce à son potentiel. Cependant, sa forte intégration soulève encore plusieurs questions et se heurte à de nombreux défis. L'un des principaux défis est "comment garantir la confidentialité et établir une sécurité solide pour cette nouvelle technologie". [15]

Au jour d'aujourd'hui L'Internet des objets utilise le cloud computing comme ressource de stockage de données et le contrôle des flux de communications entre les objets, ici le contrôle d'accès est plus facile à mettre en place et à administrer ou même à mettre à jour, par contre il est extrêmement facile de recevoir des attaques de type DDoS ou autres puisque c'est centralisé.

La solution au problème est d'élaborer un système décentralisé et sécurisée tout en établir un contrôle d'accès au système où au donné, qui est la blockchain. Elle permet de désigner plusieurs administrateur grâce au système de gouvernance.

La gouvernance se fait avec une preuve d'appartenance d'entité unique inscrite sur la blockchain comme c'est le cas des blockchains utilisant les tokens comme preuve de gouvernance.

II.3.8 Le contrôle d'accès dans la santé

Malgré le fait que les lieux de santé public soit a priori ouvert à tout le monde certain endroit nécessite un système de contrôle d'accès a certaine zone comme le parking ou bien les blocs opératoires pour éviter la perte de contrôle des personnes avec des troubles mentales et autres, et aussi de faire ressentir la sécurité au personnel travaillant dans les meilleures conditions possibles.

Concernant l'architecture technique, deux solutions sont envisageables : un réseau filaire pour les zones sensibles et les portes extérieures ; un système autonome ou connecté en radio (cylindres, poignées intelligentes, etc.) à l'intérieur des sites.
Les avantages d'un système du contrôle d'accès sont multiples : traçabilité assurée, pas de risque de perte de clé physique, moins de coût dans les dépenses pour le personnel de sécurité , pas de risque sur le problème d'infiltration ,conservation de la confidentialité, plus de sécurité …

II.4 Conclusion

La blockchain nous donne un large terrain d'intervention sur différents secteurs :la sécurité pour les contrôles d'accès, l'acheminement et la sécurité des transferts des données, le stockage de données … de façon très autonomes et scalable a l'intégration de plusieurs institutions aux partages des données entre eux de manière transparente et décentralisé.

III. CHAPITRE 3 : CONTRIBUTION ET RÉSULTATS

III.1 Introduction

Les systèmes de contrôle d'accès sont utilisés dans la sécurité informatique pour mettre en ouvres de conditions d'accès afin de spécifier l'accès de l'utilisateur a la ressource numérique où physique. En utilisant la technologie blockchain qui se caractérise par sa durabilité, immuabilité, fiabilité et sa sécurité, cette technologie devient de plus en plus demandé dans la plupart des secteurs tel que la santé.

La blockchain élimine la part des tiers du système, par conséquent, elle assure la confidentialité avec son système de sécurisation des transactions sur une chaîne de block qui garde tout l'historique de ses derniers intègre. Il existe deux types de systèmes de contrôle d'accès, le contrôle d'accès logique et le contrôle d'accès physique. La plupart des études sur les systèmes de contrôle d'accès se concentrent sur le contrôle d'accès logique.

III.2 Contribution

III.2.1 Contrôle d'accès

Le contrôle d'accès se fait par rôle, il va nous permettre de contrôler l'accès aux objets connectés du patient selon le rôle choisi dans la politique d'accès. On a choisi le rôle comme base au contrôle d'accès pour mieux optimiser et sécurisé l'accès aux données par exemple un medecin a logiquement plus de champ d'accès aux ressources du patient qu'un infirmier.

III.2.2 Spécificité du contrats intelligent

Chaque patient déploie son propre contrats intelligent lors de la création du compte avec une liberté d'ajout des termes de contrats avec le personnel médical souhaitais.

Pour chaque patient, un contrat intelligent déployer.

III.3 Conception système

III.3.1 Acteurs

Dans notre application y'aura d'interaction avec 3 acteurs :

- Administrateur : qui a pour rôle d'enregistrer le personnel médical au sein de la blockchain.

- Le patient : c'est celui qui ajoute la politique d'accé du médecin à ses ressources personnelles.
- Le personnel médical : c'est celui qui accède à la ressource du patient permis.

III.3.2 Besoins fonctionnels et non fonctionnels

- **Les besoins fonctionnels**
    - Authentification
    - Ajout de la politique
    - Suppression de la politique
    - Modification de la politique
    - Accès aux ressources
- **Les besoins non fonctionnels**
    - Rapidité du système
    - Fiabilité des données
    - Authenticité des données
    - Traçabilité des transactions

III.3.3 Diagrammes

Diagramme de cas d'utilisation :

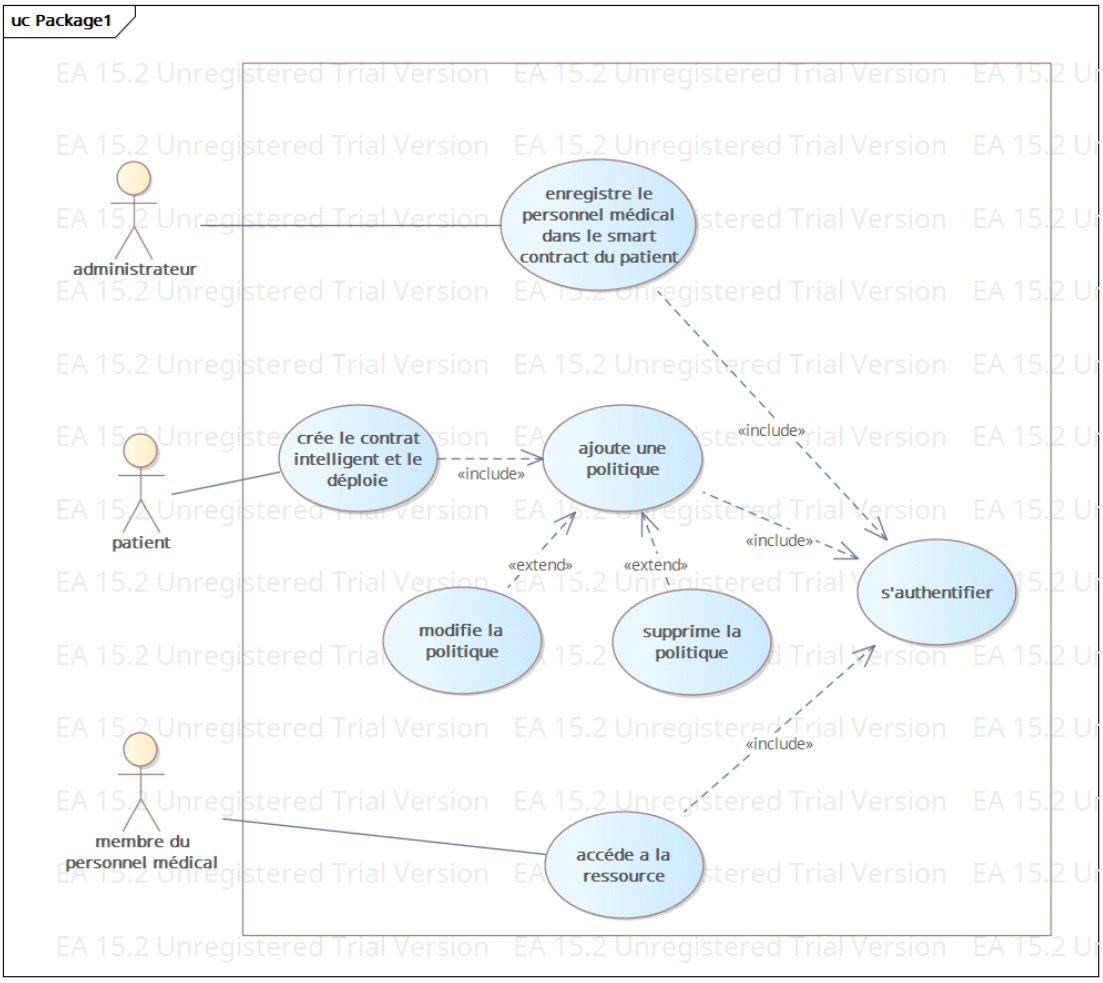

Figure III-1 : Diagramme de cas d'utilisation

-le patient crée et déploie le contrat intelligent après avoir créé son compte sur l'application.

-l'administrateur enregistre le personnel médical au sein du contrat.

-le patient ajoute les politiques d'accées à ses ressources pour chaque membre du personnel voulut.

-le membre du personnel accédes a la ressource du patient si sa lui est permis.

III.4 Implémentation

III.4.1 Outils de développement

Front-end :

Pour le développement front-end , on a utilisé les langages de développement WEB tel que le HTML,CSS,JAVASCRIPT et pour rendre notre site web responsif adapté à toute appareille électronique on a utilisé la bibliothèque BOOTSTRAP .

Back-end :

Pour la création de notre contrat intelligent, voici tout ce dont nous avons besoin :

- Une Blockchain de développement.
- Un contrat en Solidity.
- Un environnement de développement.

Blockchain de développement :

Dans notre projet, on a utilisé la blockchain Ethereum qui permet de développer des applications d'interaction décentralisé (DAPPS) à l'aide des contrats intelligents.

Pour réaliser notre projet on a utilisé l'application Ganache sur windows qui permet de simuler la blockchain Ethereum de manière privé et gratuite vue que le réseaux ethereum et payants pour déployer et testé le contrat.

Le contrat intelligent :

Pour développer le contrat intelligent on a utilisé le langage de programmation appelé SOLIDITY qui est un langage de programmation orienté objet.

Un environnement de développement :

Afin de programmé et déployé notre contrat dans notre blolckchain privé on passe soit par un IDE de développement tel que REMIX disponible directement sur les navigateur web ou bien Truffle qui est un framework de développement ethereum qui est basé sur Nodejs .

Solidity

Solidity est un langage de programmation de type statique conçu pour développer des contrats intelligents qui s'exécutent sur l'EVM (Ethereum Virtual Machine).

HTML

(HyperText Markup Language) HTML est un langage informatique utilisé pour créer des pages web. Ce langage permet de réaliser de l'hypertexte à base d'une structure de balisage. Par ailleurs, HTML n'est pas un langage de programmation proprement dit comme C, C++, etc. mais plutôt un langage qui permet de mettre en forme du contenu. [16]

CSS

(Cascading Style Sheets) Le CSS pour Cascading Style Sheets, est un langage informatique utilisé sur Internet pour la mise en forme de fichiers et de pages HTML. On le traduit en français par feuilles de style en cascade. [17]

Javascript

Javascript est un langage de programmation qui permet de créer du contenu mis à jour de façon dynamique, de contrôler le contenu multimédia, d'animer des images. [18]

Boostrap

Bootstrap est un framework qui utilise les langages HTML, CSS et JavaScript et qui fournit aux développeurs des outils pour créer un site facilement.

Web.js (Ethereum JavaScript API)

Web3.js est une collection de bibliothèques qui permettent d'interagir avec un nœud Ethereum local ou distant en utilisant HTTP, IPC ou Web socket.

Node.js

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

Ganache

Ethereum Ganache est une blockchain locale en mémoire conçue pour le développement et les tests. Il simule les caractéristiques d'un véritable réseau Ethereum, y compris la disponibilité d'un certain nombre de comptes financés avec l'Ether de test.

III.4.2 Algorithme

Le sujet, l'objet et le propriétaire de l'objet considérés dans notre système sont définis dans le tableau suivant

Sujet	Objet	Propriétaire de l'objet
Patient / personnel hospitalier	Appareils IoT (capteurs)	Patient

Tableau III-1 Le sujet,l'objet,le propriétaire de l'objet de notre application

Notre contrôle d'accès basé sur la blockchain passe par les étapes suivantes :

- Etape 1 (création d'un smart contract) : le propriétaire de la ressource (patient) crée un smart contract en définissant ses politiques d'accès puis le déploie sur la blockchain.
- Étape 2 (Soumettre la requête) : le sujet soumet une requête pour accéder à un objet.
- Étape 3 (récupération du contrat) : Le sujet demande à récupérer le contrat de contrôle d'accès correspondant.
- Etape 4 (Les transactions sont enregistrées dans le nouveau bloc) : Le sujet envoie une transaction qui contient les informations nécessaires au contrôle d'accès. Alors les méthodes de contrôle d'accès peuvent être exécutées
- Etape 5 (rendre la décision d'accès) : Dès que le processus de contrôle d'accès est terminé, le résultat est envoyé au sujet et à l'objet.

Dans la première étape, lors de la création du contrat intelligent, le propriétaire de l'objet devra définir les politiques d'accès à sa ressource en remplissant **le rôle et l'identifiant du sujet** c'est-à-dire le rôle et l'identifiant du patient ou du personnel hospitalier qui peut accéder à son objet, **l'action** que le sujet peut effectuer sur son objet comme lire la donnée ou la modifier ou exécuter un programme, et enfin **la permission** d'accès qui peut être soit autoriser ou refuser.

Le tableau III-2 représente un exemple d'une politique remplie par un patient.

rôle	Identifiant du sujet	Action	Permission	Intervalle entre 2 demande d'acces	limit
medecin	PHid	Lire / ecrire	Oui	1min	3

Tableau III-2 Un exemple d'une politique remplie par un patient

La liste des politiques d'accès

Il faut noter que dans notre système, Les ACC fournissent également des fonctions pour l'ajout, la mise à jour et la suppression de politiques de contrôle d'accès.

- **policyAdd () :** Cet ABI reçoit les informations d'une nouvelle politique de contrôle d'accès et ajoute les informations à la liste des politiques.

- **policyUpdate () :** cette ABI reçoit les informations d'une politique qui doit être mise à jour et met à jour la politique.

- **policyDelete () :** cette ABI reçoit les informations d'identification d'une politique et supprime la politique.

- **accessControl () :** cette ABI reçoit les informations requises pour le contrôle d'accès et renvoie le résultat de l'accès et la pénalité. Lorsque le sujet appelle (en envoyant une transaction) cet ABI pour autoriser sa demande d'accès actuelle, le processus de validation commence. Une fois un éventuel mauvais comportement détecté, l'ACC prend une décision de pénalité sur la mauvaise conduite et applique des contre-mesures basées sur la décision de sanction.

- **deleteACC () :** cette ABI effectue l'opération d'autodestruction pour supprimer le code et le stockage de l'ACC de la blockchain, de sorte que l'ACC ne puisse plus être disponible.

Il faut aussi noter que seul le créateur de l'ACC peut ajouter une nouvelle politique, mettre à jour ou supprimer une politique existante, et supprimer le ACC.
Notre contrat de contrôle d'accès passe par 3 étapes, la vérification d'enregistrement du sujet, et la vérification des droits d'accès.

La vérification d'enregistrement du sujet : le contrat vérifie si le nom et le role du sujet sont valides, le contrat passe à la vérification des droits d'accès, mais dans le cas contraire la demande est rejetée.

La vérification des droits d'accès : le contrat vérifie dans la liste des politiques d'accès si le sujet a le droit d'accéder à la ressource ou pas, si c'est le cas il passe à la vérification de la mauvaise conduite sinon la demande est rejetée.

Vérification de mauvaise conduite (validation dynamique) : Le contrat de contrôle d'accès maintient une liste de mauvaise conduite pour chaque sujet, comme indiqué dans le tableau III-3. Si le sujet a fait des demandes d'accès plus fréquentes qu'il n'est autorisé, la demande est rejetée sinon la demande est approuvée et le sujet peut accéder à l'objet.

Resource	Action	Time of misconduct	Penalty	Time of Unblock
IRM	read	01/02/2021; 11:45	1min	01/02/2021; 11:46
RADIO	write	01/02/2021; 12:30	2min	01/02/2021; 12:32

Tableau III-3 Exemple sur le déroulement des mauvaises conduites

Notre algorithme

Algorithm 1 Access control ABI

Input: role,subject, ressource, action, time
Output: result, penalty
Require: *penalty* ← *0*,*result* ← *true*, subjectpolicyList Policies, subjectRegistrationList Registration, SubjectMisconductList List

```
1:  R ← Registration [subject]
2:  P ← Policies [role][subject][ressource][action]
3:  M ← List [subject]
4:  if R == true then
5:      if M.timeOfUnblock ≤ time then
6:          M.timeOfUnblock ← 0
7:          if P.permission == 'allow' then
8:              F ← time - P.ToLR
9:              if F ≤ P.MinInt then
10:                 P.NoFR ← P.NoFR ++
11:                 if P.NoFR ≥ P.Limit then
12:                     Detect a Misconduct MSC
13:                     result ← false
14:                     S ← M.length+1
15:                     penalty ← base*S
16:                     M.timeofUnblock ← time+penalty
17:                     push MSC into the SubjectMisconductList
18:             else
19:                 P.NoFR ← 0
20: else
21:     P.ToLR ← time
22:  Return(result, panalty)
```

Figure III-2 : Algorithme de contrôle d'accès

Le patient déploie un contrat pour chaque médecin ou infirmier et pour chaque ressource, pour les autoriser ou non à accéder à ses données en respectant certaines conditions, le temps minimum autorisé entre 2 demandes successives et une limite de demandes fréquentes sinon le médecin n'aura pas accès et il va être pénalisé (30 secondes accès non autorisée pour chaque mauvaise conduite).

III.5 Résultat

• Seules les personnes autorisées peuvent accéder aux ressources de patient.

• Chaque médecin a un contrat créé par le patient.

• Seul le patient qui peut contrôler les politiques d'accès à ces ressources.

• Un système sécurisé et décentralisé pour stocker les données.

- Consommation :

Chaque contrat consomme 2591883 Gwei lors du déploiement.(exemple du block 131 de la figure III-5)

Chaque appel de fonctions consomme en moyenne 39000 Gwei. (exemple de block 130,129 de la figure III-5)

La figure III-3 illustre quelques exemples de consommation de GAS lors du déploiement du smart contract et l'appels de fonctions :

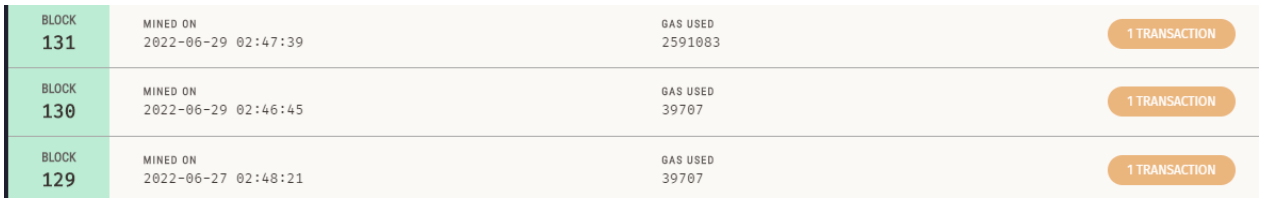

Figure III-3 : Consommation de GAS lors du déploiement du smart contract et l'appels de fonctions

La figure III-4 montre que la politique d'accès a était ajouté avec succès de la part du patient :

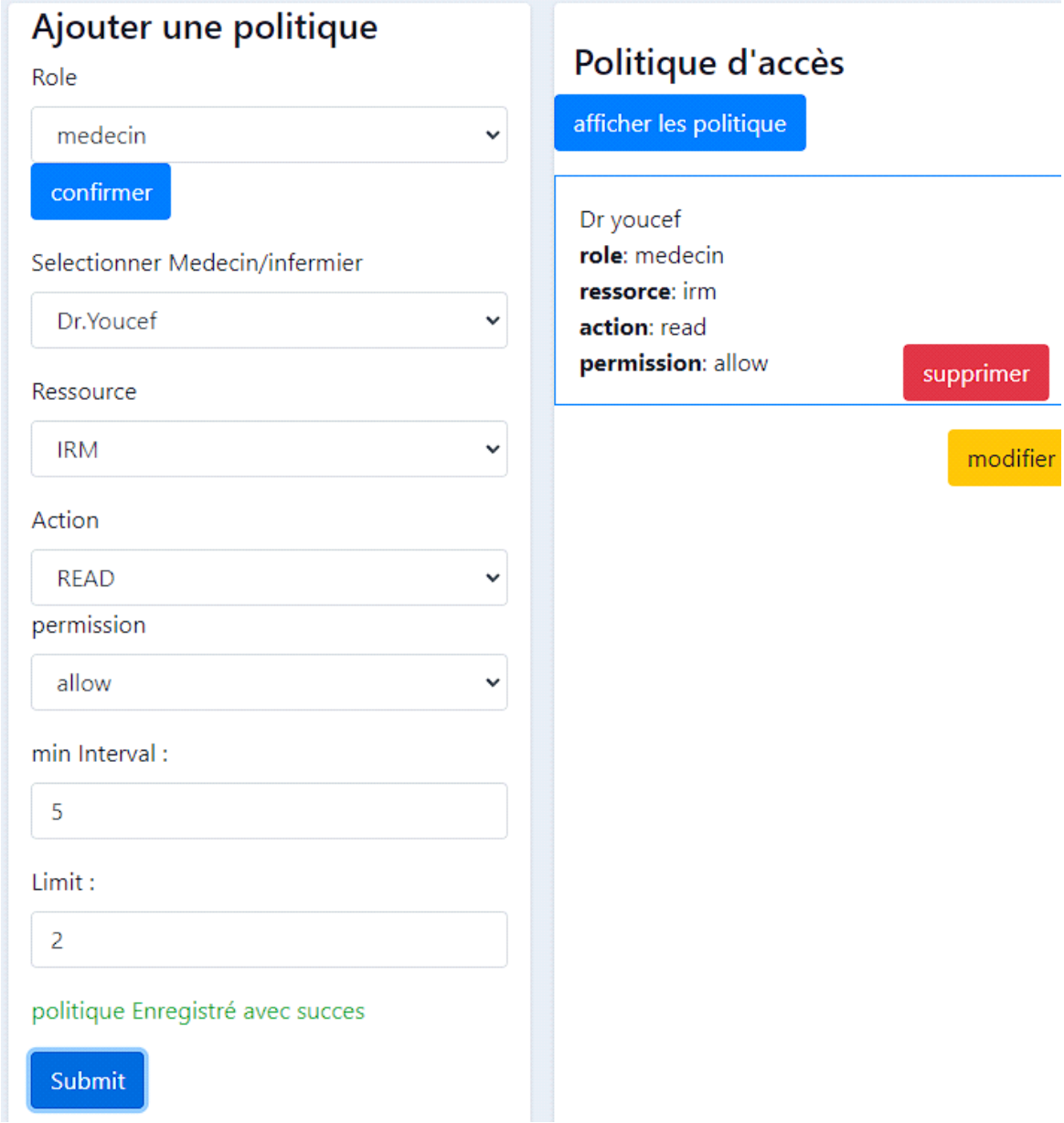

Figure III-4 : Une politique d'accès à était ajouté pour le médecin Youcef avec succès

La figure III-5 montre que le medecin est autorisée à accéder à la donnée du patient Karim :

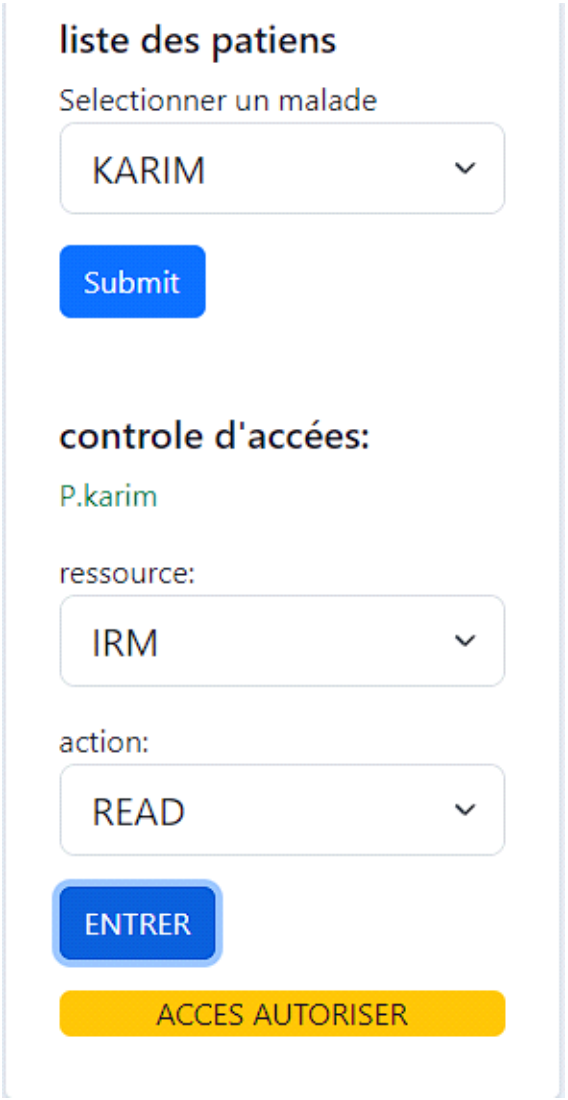

Figure III-5 : Le médecin a accès à la ressource

La figure III-6 montre que l'accès a été refusé pour le médecin pour l'accès à la ressource :

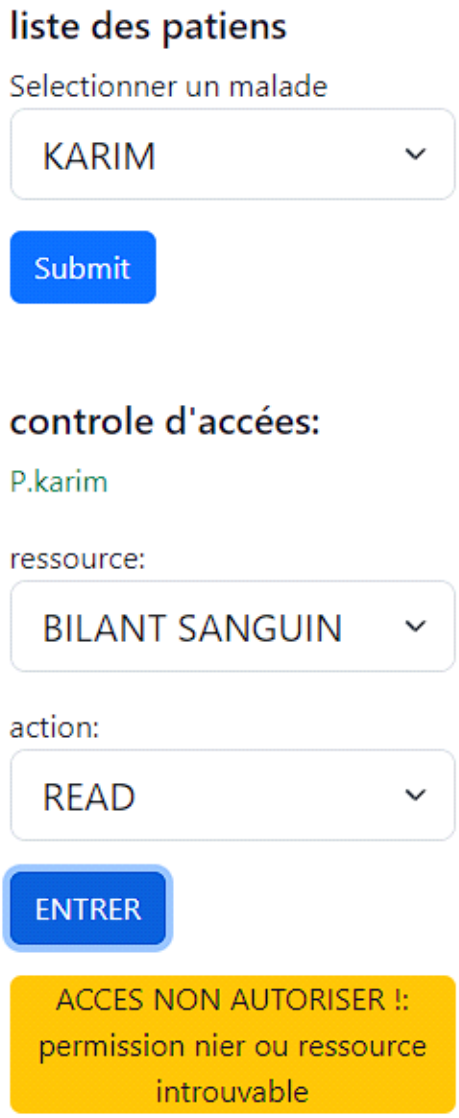

Figure III-6 : Le médecin n'a pas accès à la ressource

III.6 Conclusion

La sécurité est le critère le plus important a soulignée qui pousse un individu a utilisé les méthode informatiques modernes dans plusieurs domaines ; encore plus important dans le secteur de la santé où les données sont ultra sensibles et personnelles , avec la technologie blockchain on a une sureté de l'information protégé de la modification et un flux de partage de données décentralisé ; pour cela nous avons développé un contrat intelligent qui assure la sécurité et le partage des données toute en spécifions les politique d'accé à ses données par le détenteur de ses données.

IV. CONCLUSION GENERALE

CONCLUSION GÉNÉRALE

Grâce à sa décentralisation et son efficacité, la blockchain œuvre à offrir aux utilisateurs un service de sécurité optimal dans le partage de données.

Avec l'adoption des smart contract, le champ de la blockchain s'ouvre de plus en plus au monde et sur tous ses secteurs. Dans le domaine médical où les données sont ultra personnelles et sensibles ; la blockchain offre des solutions à ce problème majeur et garanti une sécurité d'accès. Dans ce contexte, notre travail consiste à établir une liaison de confiance entre le détenteur de la donnée qui est le patient et le personnel médical.

Le contrat se base sur l'ajout de politique d'accès pour le personnel médical sur le rôle de ce dernier afin de définir le poids et le champ d'accès aux ressources du patient.

Pour perfectionner notre système, il est utile de relier notre application web avec une application mobile qui fonctionne à la base de blockchain et appareils connectés dans des hôpitaux et des cliniques médicales d'une manière sécurisée.

Puisque nous aurons des données de grande taille qui rassemblent les dossiers médicaux à partir des objets connectés, nous pouvons utiliser une base de données comme le cloud reliée avec notre blockchain pour contrôler l'accès à ces données et sauvegarder tous les historiques des modifications de données en utilisant les smart contrats.

BIBLIOGRAPHIE ET WEBOGRAPHIE

Bibliographie et webographie

1. Vaz FP. journal du net.. 2022. Disponible sur: https://www.journaldunet.com/ebusiness/internet-mobile/1511755-objets-medicaux-connectes-les-defis-au-dela-de-la-cybersecurite/. date de visite 02-06-2022

2. Disponible sur: https://www.blackberry.com/fr/fr/solutions/iot-internet-of-things/iot-healthcare. date de visite 06-06-2022

3. oracle. Disponible sur: https://www.oracle.com/fr/internet-of-things/what-is-iot/. date de visite 04-06-2022

4. Technologie MN. L'Internet des objets et les risques de cybersécurité qu'ils impliquent. 2018. Disponible sur: https://www.pandasecurity.com/fr/mediacenter/technologie/linternet-des-objets-risques/ date de visite 04-06-2022

5. insider D. Qu'est-ce que l'Internet des objets médicaux (IoMT) ?. Disponible sur: https://www.splunk.com/fr_fr/data-insider/what-is-the-internet-of-medical-things-iomt.html. date de visite 02-06-2022

6. Bride L. L'Internet des Objets et les Big Data au service de l'e-santé.; 2015. Disponible sur: https://www.journaldunet.com/solutions/dsi/1163358-l-internet-des-objets-et-les-big-data-au-service-de-l-e-sante/. date de visite 06-04-2022

7. Simon, Moulin and P.E-santé-Objets connectés et télémédecine e-Health-The internet of things and telemedecine.mars-avril 2016., n° 2 p.

8. Julien Aubert LdLRMM. la blockchain (chaîne de blocs) et ses usages. ; 2018. date de visite 10-03-2022

9. Disponible sur: https://academy.bit2me.com/fr/combien-de-types-de-blockchain-existe-t-il/. date de visite 12-03-2022

10. Ayadi OA.; 2019. Disponible sur: https://www.researchgate.net/publication/335174496_CHAPITRE_III_Etat_de_l'art_de_la_Blockchain. date de visite 10-03-2022

11. Disponible sur: https://fr.theastrologypage.com/access-control. . date de visite 02-06-2022

12. Thomas RK. Flexible team-based access control using contexts. In ; 2001: Conference Paper.

13. Le Grand Dictionnaire terminologique. le 31 janvier 2022..

14 Disponible sur: https://medium.com/flowchain-knowledgecamp/why-iot-blockchain-3fa02531bce4.
. date de visite 07-06-2022

15 Kerkar MN. Plateforme De Sécurité Légère Pour Ido. Blida:; 2019.
.

16 Disponible sur: http://glossaire.infowebmaster.fr/html/ .date de visite le 04-06-2022
.

17 Disponible sur: https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203277-css-
. cascading-style-sheets-definition-traduction/.. date de visite 04-06-2022

18 Disponible sur:
. https://developer.mozilla.org/fr/docs/Learn/JavaScript/First_steps/What_is_JavaScript. .date de visite 04-06-2022

Résumé

Ce travail consiste a utilisé la technologie blockchain et les smarts contracts pour la gestion des dossiers électroniques médicaux (DEM) afin de rendre les données le plus privé possible pour le détenteur de ses ressources toute en lui laissant la liberté de choisir les acteurs qui peuvent y accéder à l'aide d'un système de contrôle d'accès contractuel bien établie. La réalisation de l'application s'est faite sous l'éditeur MICROSOFT VISUEL STUDIO en utilisant les langages de programmation JavaScript, HTML, CSS et le Framework Bootstrap pour le front-end et l'environnement de développement REMIX sous le langage SOLIDITY et le simulateur de la blockchain Ethereum GANACHE pour le back-end.

Mots clés : blockchain, contrôle d'accès, contrat intelligent, dossier électronique médical

Abstrat

This work consists of using blockchain technology and smart contracts for the management of electronic medical records (DEM) in order to make the data as private as possible for the holder of his resources while leaving him the freedom to choose the actors who can use it. accessed using a well-established contractual access control system. The realization of the application was done under the editor MICROSOFT VISUEL STUDIO using the JavaScript, HTML, CSS programming languages and the Bootstrap Framework for the front-end and the REMIX development environment under the SOLIDITY language and the ethereum GANACHE blockchain simulator for the back-end.

Keywords: blockchain, access control, smart contract, electronic medical record

ملخص

يتكون هذا العمل من استخدام تقنية blockchain والعقود الذكية لإدارة السجلات الطبية الإلكترونية (DEM) من أجل جعل البيانات خاصة قدر الإمكان لصاحب موارده مع ترك حرية اختيار الممثلين الذين يمكنهم استخدامها. الوصول إليها باستخدام نظام راسخ للتحكم في الوصول التعاقدي. تم تنفيذ التطبيق تحت محرر MICROSOFT VISUEL STUDIO باستخدام لغات البرمجة JavaScript و HTML و CSS و Bootstrap Framework

للواجهة الأمامية وبيئة تطوير REMIX تحت لغة SOLIDITY ومحاكاة GANACHE ethereum blockchain للواجهة الخلفية.

الكلمات المفتاحية: blockchain ، التحكم في الوصول ، العقد الذكي ، السجل الطبي الإلكتروني