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 à base de blockchain dans les systèmes de télésanté

Hamel Marwa

Zerguit Hadjer

Présenté le 27 juin 2022 devant le jury composé de :

-Mme Labraoui Nabila (présidente)

- Abdeldjelil Hanane (Examinatrice)

-Mme Amraoui Asma (Encadrante)

-Mme Zerga Hidayet (Co-Encadrante)

Année Universitaire : 2021-2022

Remerciements

Avant toute chose, on tient à remercier Allah, le tout puissant, pour nous avoir donné la force et la patience d'achever ce travail.

Nos sincères remerciements À notre Encadrante **Madame Amraoui Asma** et notre Co-encadrante **Madame Zerga Hidayet** pour l'aide, l'orientation, la guidance qu'il nous accordé durant l'accomplissements de ce modeste travail.

Nous tenons à remercier "**Mme Labraoui.N** "et "**Mme Abdeldjelil.H**», d'avoir accepté d'examiner et d'évaluer notre projet.

Nos vifs remerciements vont à nos parents sans qui nous ne serons pas ici aujourd'hui, ainsi qu'à nos familles frères/sœurs et amis pour leur soutiens et encouragements.

Enfin, nous remercions tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Merci

Table des matières

Liste des figures

Liste des acronyms

ABAC	Attribut Based Access Control
ACL	Access Control List
API	Interface Application
CNIL	Commission Nationale de l'Informatique et des Libertés
DAC	Discretionary Access Control
DME	Dossier Medical Electronique
DMP	Dossier Medical Personnel
IAB	Internet Architecture Board
IoT	Internet of Things
MAC	Mandatory Access Control
M2M	Machine to Machine
NFT	Non-Fungible Token
OMS	Organisation Mondiale de la Santé
RBAC	RoleBased Access Control
RFID	Radio Frequency Identification
TCSEC	Trusted Computer System Evaluation Criteria
TIC	Technologies de l'Information et de la Communication
WSN	Wireless Sensor Network

Résumé

La technologie Blockchain a le potentiel de transformer le secteur de la santé, en plaçant le patient au centre de système de la santé et en augmentant la sécurité, la confidentialité et l'interopérabilité des données. Cette technologie pourrait fournir un nouveau modèle pour les échanges d'informations sur la santé en rendant les dossiers médicaux électroniques plus efficaces et sécurisés. Bien qu'il ne s'agisse pas d'une panacée, ce nouveau domaine en évolution rapide offre un terrain fertile pour l'expérimentation, l'investissement et les tests. Étant donné que les antécédents médicaux d'un patient sont la première pierre angulaire d'une bonne médecine, la recherche dans ce domaine est relativement nouvelle mais en croissance rapide. Ainsi, les chercheurs et praticiens en informatique de la santé ont toujours du mal à suivre le rythme des progrès de la recherche dans ce domaine... Dans ce modeste travail nous appliquerons le concept de la technologie blockchain et le NFT pour réaliser un système de contrôle d'accès aux données de patient en utilisant les contrats intelligents qui permet aux patients d'être les véritables propriétaires de leurs données sensibles et de les partager en toute sécurité.

Mots clés : blockchain, NFT, contrôle d'accès, contrat intelligent.

Abstract

Blockchain technology has the potential to transform the healthcare industry, placing the patient at the center of the healthcare system and increasing data security, privacy and interoperability. This technology could provide a new model for the exchange of health information by making electronic medical records more efficient and secure. While not a panacea, this new and rapidly evolving field provides fertile ground for experimentation, investment and testing. Since a patient's medical history is the first cornerstone of good medicine, research in this area is relatively new but growing rapidly. Thus, health informatics researchers and practitioners continue to struggle to keep pace with advances in research in this domain. In this modest work we will apply the concept of blockchain technology and NFT to realize a patient data access control system using smart contracts that allows patients to be the true owners of their sensitive data and to share it securely.

Keywords: blockchain, NFT, access control, smart contract

ملخص

تتمتع تقنية blockchain بالقدرة على تحويل صناعة الرعاية الصحية، ووضع المريض في مركز نظام الرعاية الصحية وزيادة أمن البيانات والخصوصية وقابلية التشغيل البيني. يمكن أن توفر هذه التكنولوجيا نموذجًا جديدًا لتبادل المعلومات الصحية من خلال جعل السجلات الطبية الإلكترونية أكثر كفاءة وأمانًا. على الرغم من أنه ليس حلاً سحريًا، إلا أن هذا المجال الجديد سريع التطور يوفر أرضًا خصبة للتجريب والاستثمار والاختبار. نظرًا لأن التاريخ الطبي للمريض هو حجر الزاوية الأول للطب الجيد، فإن البحث في هذا المجال جديد نسبيًا ولكنه ينمو بسرعة. وبالتالي، لا يزال الباحثون والممارسون في مجال المعلوماتية الصحية يكافحون لمواكبة تقدم البحث في هذا المجال ... في هذا العمل المتواضع، سنطبق مفهوم تقنية blockchain و NFTلتحقيق نظام للتحكم في الوصول إلى بيانات المريض باستخدام عقود ذكية تسمح للمرضى بأن يكونوا المالكين الحقيقيين لبياناتهم الحساسة ومشاركتها.

الكلمات الرئيسية: blockchain,NFT، التحكم في الوصول، العقد الذكي

Introduction générale

- ## Introduction

La technologie Blockchain est propagée en 2008, coïncidant avec l'émergence de la première monnaie numérique Bitcoin. Cette technologie distribué aide à rendre plus sûres et plus transparents les données des utilisateurs et les permet de réaliser des transactions sécurisées.

Le domaine de la santé est parmi les domaines les plus bénéficie de la technologie Blockchain, car il s'agit de protéger et sécuriser le partage des informations et les données des patients. Ces données étaient stockées dans les bases de données connues, ce qui les rendait moins sécurisé. Parmi les solutions proposées pour sécuriser les informations d'un patient et assurer la confidentialité et l'interopérabilité des données, on trouve la technologie de blockchain. Elle peut assurer l'intégrité et la confidentialité des données de santé dans tous les systèmes d'information en raison de sa nature décentralisée et de son immuabilité.

- ## Problématique

Dans un domaine lorsqu'une veut sécuriser l'accès aux données et ressources, on met en place un système centralisé sécurisé par l'authentification et l'autorisation, mais le problème se pose lorsque plusieurs utilisateurs veulent sécuriser le partage d'information en mettant des politiques pour contrôler l'accès à ces ressources.

- ## Solution

Pour résoudre ce problème dans notre projet de fin d'étude, nous cherchons à explorer la technologie de blockchain pour gérer les identités et les politiques de contrôle d'accès aux ressources combiner avec la technologie de jeton non fongible (NFT). Dans ce contexte, nous avons développé une application de santé qui est un exemple classique d'utilisation des blockchains en dehors de monnaies électroniques.

- ## Organisation

La mémoire est organisée de la façon suivante :

• Le premier chapitre présente en détaille la relation entre l'internet des objets et la E-santé.

• Le deuxième chapitre présente la technologie de la blockchain et le contrôle d'access

• Le troisième chapitre offre la conception et les résultats du système proposé.

• On termine notre mémoire par une conclusion générale.

CHAPITRE 1 : INTERNET DES OBJETS ET E-SANTÉ

1. Introduction

De nos jours, le monde dépend des appareils électroniques partout à la maison, au travail et même à l'intérieur du corps humain. À la suite du développement continu dans le domaine de l'informatique, nous voyons une variété d'appareils avancés qui sont entrés dans la composition des maisons, qui aident à assurer le confort, la sécurité et même les soins de santé, en communiquant les uns avec les autres.

Dans le domaine de la santé, nous trouvons l'opportunité de rechercher des solutions technologiques qui améliorent l'efficacité et permettent d'économiser de l'argent. Cet avantage peut aider au développement de ce domaine.

Dans ce contexte, le E-santé est introduit est défini comme l'utilisation des dispositifs électroniques et d'autres technologies pour aider à la pratique des soins de santé, comme les prescriptions médicales et la surveillance à distance des patients.

Dans ce chapitre, nous présentons les généralités de l'Internet des objets (IoT). Nous présentons également un tour d'horizon sur l'architecture de l'IoT, et ses domaines d'application et ses caractéristiques ainsi que ses avantages et ses inconvénients. Ensuite nous expliquerons la e-santé où nous parlons sur le système e-santé, le dossier médical électronique et personnel, enfin nous aborderons les exigences de sécurité des applications e-santé.

2. Internet des Objets (IoT)

2.1 Définition

- L'IoT est un réseau qui réalise la connexion entre les objets et Internet via des protocoles qui permettent la communication et l'échange d'informations entre eux **[1].**
- L'IoT peut se définir aussi comme étant un réseau qui permet d'identifier directement à travers des systèmes d'identification électroniques uniques, et des dispositifs mobiles sans file. Ainsi que L'absence d'ambiguïté dans les unités numériques a conduit à la possibilité de récupérer, transférer, stocker et traiter des données sans interruption entre les sciences physiques et virtuelles **[2].**

2.2 Fonctionnement de l'IoT

L'IoT permet l'interconnexion des différents objets intelligents via internet. Il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT qui sont leur clé tel que RFID (Radio Frequency Identification), WSN (Wireless Sensor Network) et M2M (Machine to Machine), et sont définies ci-dessous **[1].**

• **RFID (Radio Fréquence Identification) :** Le terme RFID englobe toutes les technologies qui utilisent les ondes radio pour l'identification automatique des objets ou des personnes.

Cette technologie fonctionne en envoyant des ondes radio pour être stockées et récupérées à distance à l'aide d'une étiquette, dans le but de transmettre des données de celle-ci à des objets ou de pouvoir les identifier à distance.

- **WSN (Wireless Sensor Network) :** C'est un ensemble de nœuds qui communiquent sans fil et qui sont organisés en un réseau coopératif. Ces nœuds se caractérisent par une capacité de traitement, contenant différents types de mémoires, un émetteur-récepteur RF et une source d'alimentation pouvant accueillir divers capteurs et actionneurs. Nous concluons donc que WSN est un réseau de capteurs sans fil qui peut être une technologie essentielle pour le travail de l'Internet des objets.
- **M2M (Machine to Machine) :** Fait référence à des technologies permettant à des systèmes sans fil et câblé de communiquer avec d'autre périphérique de même capacité. Il représente également le lien entre les technologies de l'information et les objets intelligents dans afin de donner à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information d'une organisation.

2.3 Caractéristiques générale de l'IoT

- Les caractéristiques générales de l'IoT sont les suivantes :

- **Connectivité :** Est une exigence importante de l'infrastructure IoT. Les objets de l'IoT doivent être connectés à l'infrastructure IoT. N'importe qui, n'importe où, n'importe quand, la connectivité doit être garantie à tout moment sans connexion, rien n'a de sens.
- **Sécurité :** A la mesure que nous tirons profit de l'IoT, nous ne devons pas oublier sur la sécurité. En tant que créateurs et destinataires de l'IoT, nous devons concevoir pour la sécurité. Cela inclut la sécurité de nos données et la sécurité de notre bien-être physique. Sécuriser le point de terminaison, les réseaux et les données se diriger à travers l'ensemble de celui-ci signifie créer un paradigme de sécurité qui évoluera.
- **Intelligence et identité :** L'extraction de connaissances à partir des données générées est très importante. Par exemple, un capteur saisi des données, mais ces données ne seront utiles que si elles sont interprétées correctement. Chaque appareil IoT a une identité unique. Cette identification est utile pour suivre l'équipement et parfois pour interroger son état **[3]**

2.4 Domaines d'application

L'IoT couvrira un large éventail d'applications (comme le montre la figure 1) et de dans presque tous les domaines auxquels nous sommes confrontés tous les jours. Cela permettra l'émergence d'espaces intelligents autour de l'informatique omniprésente.

Figure 1 Domaines d'application de l'IoT

Parmi ces espaces intelligents, on peut citer : **[8]**

2.4.1 Les villes intelligentes (Smart Cities)

Une ville intelligente utilise les Technologies de l'Internet des objets (IoT) dans différents secteurs d'activité afin d'améliorer la vie quotidienne des utilisateurs et des citoyens. **[4]**

Smart Street Lighting (Figure 2) est un exemple d'application de la ville intelligente. Le système s'active lors de la détection d'un piéton ou un véhicule. Lors de la disparition du mouvement, le système ajuste la luminosité à un niveau minimal optimisé. **[5]**

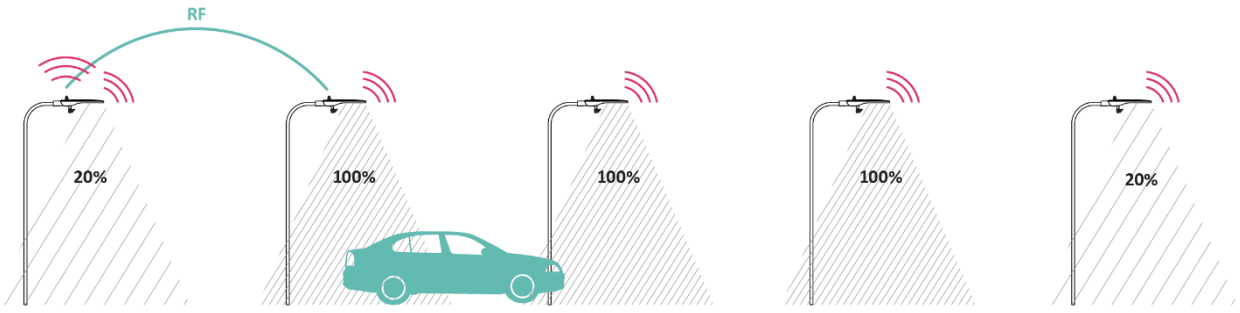


Figure 2 Infographie sur l'éclairage public intelligent

2.4.2 La domotique (Smart Home / Home Automation)

La domotique est l'utilisation des TIC chez soi pour une vie quotidienne plus confortable.

Smart Lock (Figure 3) est l'une des applications de l'IoT domotique, qui est une serrure attachée à la porte et connectée à un smartphone, elle se ferme automatiquement dès que la personne quitte la maison, elle envoie une notification au téléphone à chaque fois une personne entre ou quitte la maison, en plus d'autres fonctionnalités. **[6]**

L'image suivante représente le Smart Lock de 'August' :

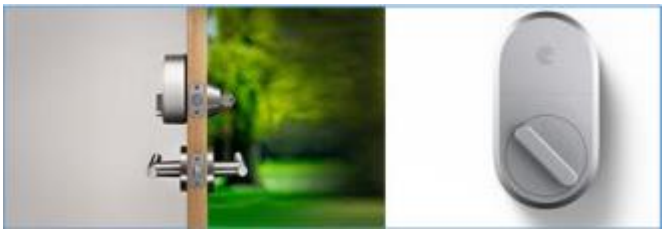


Figure 3 Serrure intelligente [6]

2.4.3 Agriculture intelligente (Smart Agriculture)

L'application de l'IoT joue un grand rôle dans l'agriculture pour faciliter les tâches des agriculteurs, tels que l'arrosage, l'épandage d'engrais et d'autres.

L'image suivante (Figure 4) représente une infographie d'un système d'arrosage :

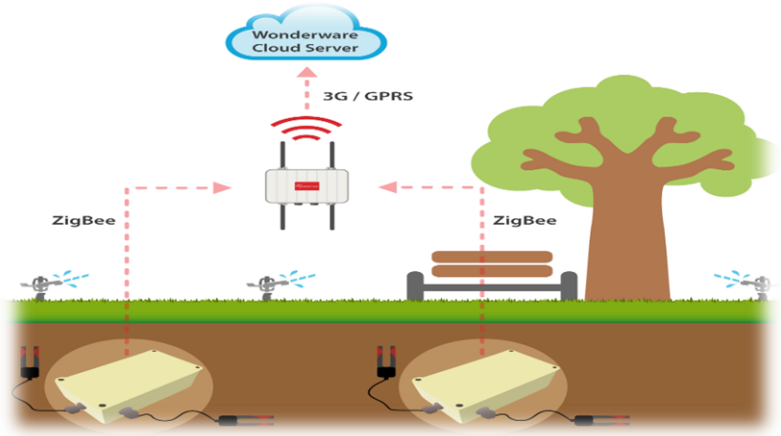


Figure 4 Agriculture intelligente (Système d'arrosage) [7]

2.4.4 La E- santé (Smart Heath)

Dans le domaine de la santé, l'IoT permettra le contrôle et le suivi des signes cliniques des patients, surtout pour des personnes âgées. Ainsi faciliter la télésurveillance des patients à domiciles, et trouver des solutions pour l'autonomie des personnes à mobilité réduite**.[8]**

2.4.5 L'industrie

Dans l'industrie l'IoT permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers. **[8]**

2.5 Architecture de l'IoT

Vu le développement rapide de l'IoT, il devenait nécessaire d'avoir une architecture de référence qui permettrait d'uniformiser la conception des systèmes et favoriserait L'interopérabilité et la communication entre les différents écosystèmes de l'IoT.

2.5.1 Architecture proposée par Internet Architecture Board (IAB)

En mars 2015, le comité Internet Architecture Board (IAB) édite la RFC17452, propose quatre modèles communs d'interactions entre des acteurs de l'IoT. **[9]**

- **La communication entre objets :** Ce modèle fonctionne par communication sans fil entre deux objets et les informations sont transférées grâce à l'intégration de la technologie de communication sans fil comme ZigBee ou Bluetooth, etc.
- **La communication des objets vers le cloud** : dans ce modèle, les données collectées par les capteurs sont envoyées aux plateformes de services via le réseau.
- **La communication des objets vers une passerelle** : ce modèle est basé sur un intermédiaire qui fait le lien entre les capteurs et les applications dans le cloud.
- **Des objets au partage des données en back-end2** : Le but de ce modèle est de permettre le partage de données entre les fournisseurs de service. Dépend essentiellement du concept « web programmable ». Les fabricants travaillent à la création d'une interface d'application (API) leur permettant de tirer parti des données collectées par d'autres fabricants.

2.5.2 Architecture en trois niveaux

D'autres organismes proposent un modèle à trois niveaux sont :

• **Couche de perception :** C'est la couche physique, qui dispose des capteurs pour la détection et la collection d'informations sur l'environnement. Elle détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement **[10]**

• **Couche réseau :** Cette couche est responsable de la connexion à d'autres objets intelligents, à des dispositifs réseau et à des serveurs. Ses caractéristiques sont également utilisées pour la transmission et le traitement des données des capteurs **[10].**

• **Couche application :** Cette couche est responsable de la prestation de services spécifiques à l'application à l'utilisateur. Elle définit diverses applications dans lesquelles l'Internet des objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente **[10].**

2.5.3 Architecture en sept couches (le modèle Cisco)

Les architectures des couches superposées sont proposées par des différentes entreprises comme l'entreprise américaine Cisco. En octobre 2013, Jim Green présente « Building the Internet of Things », le modèle envisagé par son entreprise pour l'IoT, Il est composé de 7 couches (figure 5).

Ces modèles montrent l'engouement des entreprises pour les développements des écosystèmes de l'IoT ouverte et interopérable pour être acceptés par les acteurs des marchés. Malgré, ces architectures, il reste des efforts à faire pour proposer un modèle de référence globale qui prend en compte les spécificités de l'IoT.**[9]**

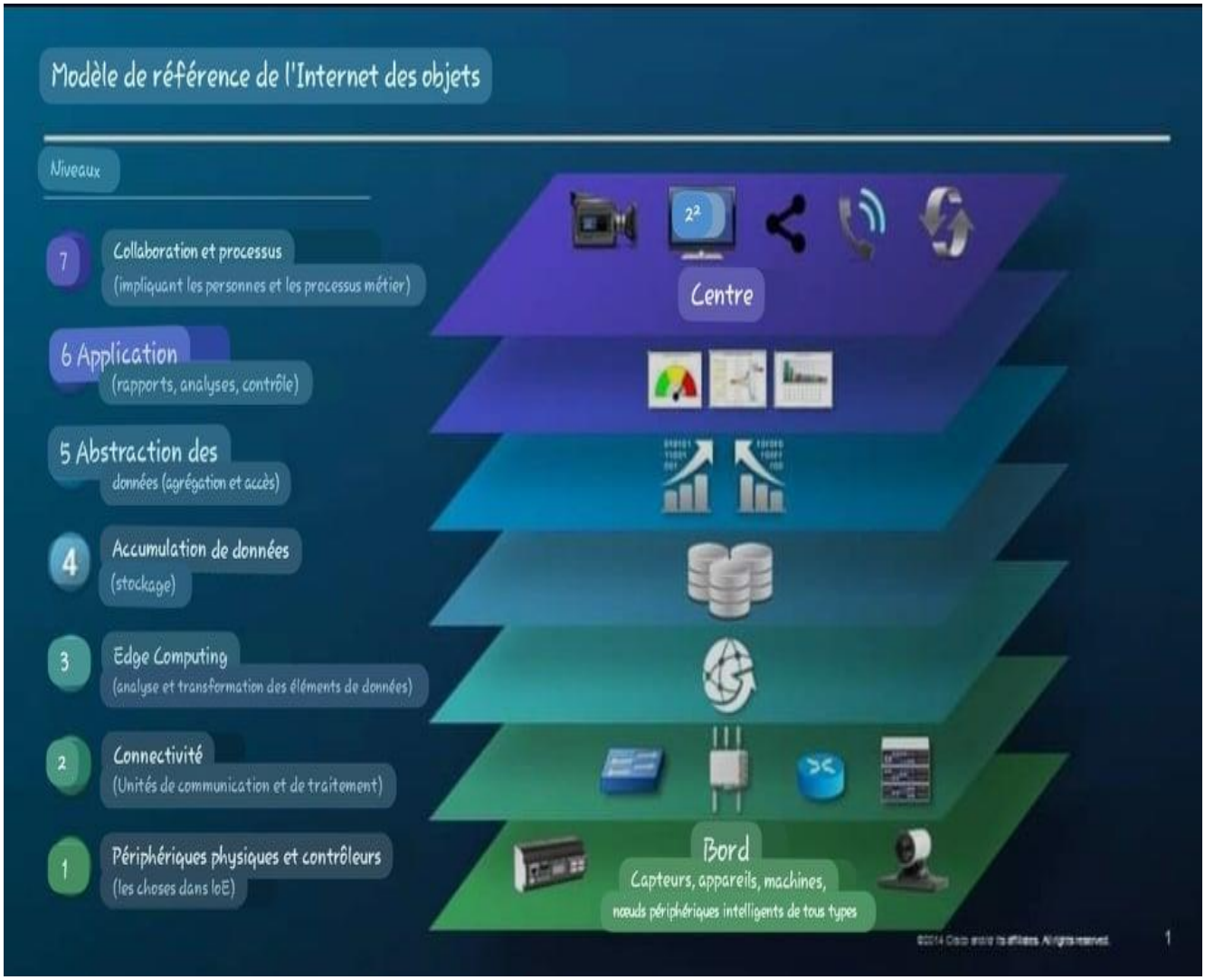


Figure 5 Les différentes couches de l'Internet des objets (selon Cisco)

2.6 Les avantages et les inconvénients d'IoT

2.6.1 Les avantages

Les avantages des IoT sont nombreux, nous pouvons citer les avantages suivants :

- L'amélioration des services traditionnels généraux comme le transport et les parkings.
- La sécurité et la maintenance des lieux publics.
- Suivi le taux de la validité des instructions pour le travail.
- Réduire le temps perdu dans les transactions administratives dans la ville.
- Assurer la sécurité routière.
- Economiser la consommation d'énergie.

2.6.2 Les inconvénients

- La protection des données, la vie privée et la sécurité sont souvent les principales inquiétudes des sceptiques de l'IOT. Pour calmer ces inquiétudes, il serait utile de donner aux clients les informations relatives au lieu de stockage et à la nature des données qui les concernent **[11].**
- L'installation des objets connectés est couteuse.

3. E-santé (la santé numérique)

3.1 Le Système E-santé

L'e-santé est un domaine clinique d'information concentré où de nombreuses informations sont créées, utilisées et partagées régulièrement. Le stockage et le partage de cette énorme base d'information est également très importants et difficiles en raison de la sensibilité de l'information et de facteurs restrictifs comme la sécurité et la confidentialité de l'information. Dans ce domaine, le partage et la gestion sécurisés de l'information sont essentiels car le personnel médical continue de partager les informations médicales du patient avec les autorités concernées pour des mises à jour et un suivi régulier. Dans cette section, nous allons définir le terme d'E-santé, présenter des dossiers médicaux électroniques et personnels et citer les exigences de sécurité dans ce type de système.

3.2 Définition de l'e-santé

L'E-santé peut d'abord être définie comme l'utilisation des Technologies de l'Information et de la Communication (TIC) pour le transfert et l'échange à distance de données en matière de santé, que ce soit à des fins d'information, de formation, de diagnostic, de traitement, de recherche ou de gestion. L'OMS (Organisation Mondiale de la Santé) a néanmoins rappelé récemment que la « santé » ne se limite pas à la seule dimension des maladies, qu'elles soient aiguës ou chroniques, mais que la santé correspond à un « état de complet de bien-être physique, mental et social ». Le terme « santé » intéresse également les thèmes liés aux limitations

d'activités et de restriction de participation à la vie en société. En fait, l'E-santé concerne deux domaines complémentaires **[12]** :

1. L'ensemble des systèmes d'information du domaine de la santé (et pas seulement de la médecine, le champ d'application étant ainsi très large) incluant les méthodes et technologies d'exploitation et d'analyse des données collectées à partir de ces systèmes d'information variés et diversifiés.

2. La télésanté qui comporte deux volets :

• La télémédecine qui recouvre toutes les techniques et applications permettant d'intervenir à distance pour établir des diagnostics, mettre en œuvre des thérapeutiques, surveiller des traitements, assurer et suivre des soins coordonnés ;

• Les téléservices pour la vie courante et le bien-être social, qui permettent de mettre en œuvre des solutions d'aide et de vigilance vis-à-vis de personnes fragiles et de compensation de la perte d'autonomie. Ces téléservices prolongent le « soin » médical par le « prendre soin » social (en dehors du cadre purement sanitaire).

3.3 Dossier médical électronique

Le Dossier Médical Electronique (DME) est un dossier électronique d'information sur la santé des patients généré par une ou plusieurs consultations dans un contexte de prestation de soins. Ces renseignements comprennent des données démographiques sur les patients, des problèmes, des médicaments, des signes vitaux, des antécédents médicaux, des immunisations, des données de laboratoire et des rapports de radiologie. Le DME est conçu pour automatiser et rationaliser le flux de travail de l'hôpital, la clinique… **[13].**

Un DME pleinement fonctionnel devrait comprendre :

1) Le dossier des patients.
2) Le système de communication des ordonnances ou la saisie informatisée des ordonnances des médecins.
3) Le système de soutien à la prise de décisions.
4) La gestion des documents et des images.
5) la gestion des documents et des notes internes et externes.
6) Statistiques et rapports.

Les données du DME sont généralement recueillies par les fournisseurs de soins de santé du patient employés par un organisme de maintenance sanitaire qui possède et exploite le système **[12].** Ce système est conçu pour fournir une image complète de l'état du patient en tout temps. Ceci est particulièrement bénéfique à mesure que le système de santé devient de plus en plus complexe, puisque les domaines d'expertise en médecine se sont rétrécis et que plus de spécialistes sont impliqués dans le processus thérapeutique. Cela souligne l'importance d'avoir des dossiers médicaux informatisés accessibles à un éventail de professionnels de la santé pour améliorer les soins aux patients. Les DME peuvent également améliorer la productivité des médecins puisqu'ils peuvent

accéder aux renseignements médicaux avant que le patient et le médecin ne se rencontrent et éviter les malentendus causés par l'écriture manuscrite **[14].**

Bien que ce système présente de nombreux avantages, les taux d'adoption sont relativement faibles dans les cliniques communautaires **[15]** qui font face à un certain nombre d'obstacles **[16].** Un facteur majeur est le coût financier du système **[17].** Pour surmonter cet obstacle, le gouvernement américain propose des incitations financières **[18].** Par conséquent, les taux de mise en œuvre sont passés de 18 % en 2001 à 78 % en 2013 aux États-Unis **[19].** La communauté des soins de santé a lentement accepté l'e-santé comme un outil qui peut aider le personnel médical.

Les statistiques de ce domaine on Algérie est presque inexistante ce qui montre un taux d'adoption très faible.

Le DME a aidé les médecins à identifier les maladies en fonction des symptômes et des caractérisations des patients découverts dans les études déclarées. Les hôpitaux ont pu retracer les patients qui répondent aux critères en faisant simplement une recherche dans la base de données des DME. Par exemple, Lin et al. **[20]** ont montré qu'en examinant les caractéristiques structurées et non structurées du système chez les patients souffrant de polyarthrite rhumatoïde, le DME a réussi à déterminer lesquels d'entre eux souffraient également d'une toxicité hépatique induite par le méthotrexate. Les hôpitaux peuvent également effectuer des recherches dans le système pour repérer les patients ayant déjà reçu un diagnostic afin de surveiller leur consommation de Médicaments (en faisant des renvois entre les prescriptions et les fonctions de facturation), **[21]** l'apparition de la maladie à l'étude et les modes de soins. **[22]**

3.4 Dossier médical personnel

Les Dossiers Médicaux Personnels (DMP) sont des dossiers médicaux électroniques contenant des données médicales et des renseignements sur un patient qui sont tenus à jour par les patients eux-mêmes. Les patients peuvent accéder aux DMP en ligne et consulter les résultats des tests, les ordonnances, les allergies, etc. Ces dossiers médicaux peuvent être gérés par les personnes en ajoutant des antécédents médicaux, des renseignements personnels ou simplement pour surveiller leur santé. Les DMP sont un élément vital de l'intervention de transition des soins où les patients plus âgés sont encouragés à participer plus activement à leur processus thérapeutique **[23].** Dans une interaction patient-médecin, les DMP peuvent fournir au patient un langage partagé avec le médecin. Les patients mieux informés peuvent constater que les visites à l'hôpital ou les rendez-vous chez le médecin sont plus positifs. Une autre caractéristique des DMP et de la politique de soins axés sur le patient est que les patients peuvent maximiser leurs bienfaits pour la santé en organisant l'information de façon logique. Le DMP est conçu pour alléger le fardeau de la maladie (en donnant accès à l'information) et est utile pour maintenir le bien-être **[24].**

Les DMP ont été discutés pour la première fois à la fin des années 1970 **[25]** ; cependant, la plupart des études ont été menées et publiées au début des années 2000 depuis que les DMP sont devenus plus répandus dans le secteur des soins de santé à l'époque. L'idée originale découlait de la nécessité d'individualiser les technologies et de rendre les dossiers médicaux plus accessibles au public. Certains DMP offrent des services à valeur ajoutée comme la prise de rendez-vous (avec le même médecin ou un médecin différent), les interactions avec les médicaments, les rappels sur ordonnance, les rendez-vous chez le médecin, etc.

Deux des efforts du DMP les plus notables sont Google Health, qui a été arrêté le 1er janvier 2012, et Microsoft HealthVault, qui est toujours disponible. Comme l'a clairement indiqué la décision de Google d'arrêter Google Santé, son adoption par les individus a été plus lente que prévu. Malheureusement, aucune statistique n'est apparemment dans le domaine public sur le nombre d'utilisateurs de HealthVault (actuellement disponible uniquement aux États-Unis et au Royaume-Uni).

L'utilisation des systèmes électroniques dans le domaine des soins de santé est en hausse pour tous les groupes d'âge en Europe **[26],** un aperçu complet de l'utilisation des DMP **[27]** a montré que les principales raisons de l'adoption des DMP étaient la communication patient-médecin, et le mode de vie et l'autogestion de la santé. Ainsi, les personnes atteintes de maladies chroniques, ou celles qui s'occupent de personnes âgées ont exprimé des attitudes plus favorables à l'utilisation de DMP, bien que cela n'implique pas nécessairement une utilisation réelle. Outre le taux relativement faible d'adoption des DMP, la conclusion concernant les avantages de l'utilisation des DMP n'étaient pas concluantes en ce qui concerne les résultats pour la santé **[28],** à savoir qu'il n'y avait aucune preuve indiquant une amélioration de l'état de santé des utilisateurs. De toute évidence, la principale préoccupation exprimée par les utilisateurs potentiels de DMP était les atteintes à la sécurité et à la confidentialité, comme on pouvait s'y attendre, mais les préoccupations relatives à la convivialité étaient également évidentes, en particulier pour les personnes ayant des déficiences cognitives ou une faible maîtrise de l'informatique **[29]**. D'un autre côté, les médecins craignaient d'avantage l'exactitude de l'information sur la santé contrôlée et gérée par les patients. Le manque d'intérêt des médecins a également

Été considéré comme un obstacle important puisque l'accès à des renseignements médicaux complets et en temps opportun est essentiel à une utilisation satisfaisante et bénéfique des DMP.

3.5 Exigences de sécurité des applications e-santé

Les exigences de sécurité pour les applications e-santé sont difficiles, tels que l'authentification mutuelle, l'utilisateur anonymat, non-traçabilité, perfect-forward-secret, accord de clé de session, et la résistance aux attaques pour assurer la confidentialité et la sécurité des données **[12].**

- Authentification mutuelle : Cela peut être réalisé avec l'utilisation de protocoles d'authentification tels qu'Authentification Kerberos**.[12]**

- Anonymat : Si un attaquant obtient l'identité de l'utilisateur, la confidentialité du patient peut être compromise, Par conséquent, l'anonymat est l'une des exigences de sécurité dans l'e-santé. Le patient et L'identité du médecin doit être prouvée lors de la phase de demande de connexion. Cependant, il est difficile d'obtenir l'identité des patients et des médecins car ils sont cryptés.**[12]**

- Non traçabilité : Si un attaquant retrace les exercices communication de clients spécifiques, alors il / elle peut deviner l'identité réelle des patients avec une probabilité plus élevée. Cela entraîne une violation de la vie privée des utilisateurs. Un attaquant ne peut pas décider des exercices de communication d'un utilisateur spécifique**.[12]**

- Secret de transmission parfait (pfs) : Perfect Forward Secrecy (PFS) est utilisé pour l'accord de clé, qui protège les sessions précédentes contre l'accord futur des mots de passe ou des clés privées en créant une clé de session pour chaque session. Ici, un attaquant ne peut pas accéder aux clés de session, qui ont été créées dans le passé sessions ; même si n'importe qui peut accéder à la clé privée de l'utilisateur, il ne peut pas affecter car la clé de session est chiffrée avec plusieurs algorithmes.

4. Conclusion

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.

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.

La combinaison de la technologie, des données, de l'intelligence artificielle et de l'apprentissage machine dans le secteur des soins de santé permet d'améliorer la façon dont les soins sont dispensés aux patients. Grâce à une réponse aux besoins des patients à la fois plus ciblée et en temps réel, l'Internet des objets peut aider les professionnels de santé à améliorer l'expérience des patients.**[30].**

Dans ce chapitre, nous avons abordé les concepts clé des systèmes d'IoT, ainsi nous avons vu que l'IoT est une nouvelle technologie qui aide à faciliter et améliorer la vie quotidienne des êtres-humains en plusieurs domaines. Notre domaine d'application s'articule autour du domaine de la E-Santé. Nous optons vers le développement d'un système d'IoT pour le suivi médical des patients. Pour ce faire, nous allons utiliser la technologie Blockchaine qui fera l'objet du prochain chapitre.

CHAPITRE 2 : BLOCKCHAIN ET CONTROLE D'ACCESS

1. Introduction

À travers l'humanité, les humains ont fait preuve de créativité dans la communication d'informations et l'échange de valeurs. Il y a plus de 2 000 ans, les délais de transmission des informations par les messagers étaient longs et pouvaient avoir des conséquences désastreuses, les messages étant modifiés en cours de route ou interceptés par quelqu'un d'autre que le destinataire.

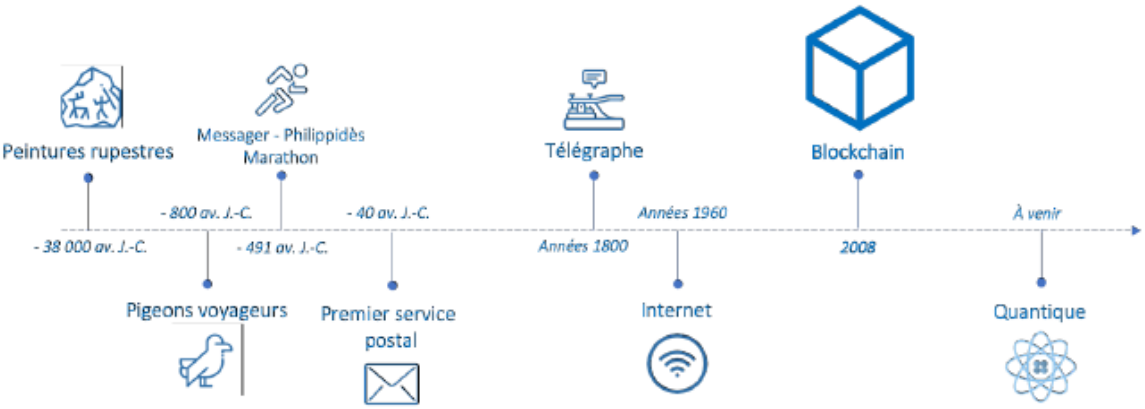


Figure 6 Historique des moyens de transmission d'information [31]

Pour instaurer la confiance entre deux entités et supprimer les intermédiaires afin d'éliminer la fraude et protéger les payeurs et les bénéficiaires contre les faillites bancaires ou les comportements malveillants ;

En 2008, Satoshi Nakamoto a décrit une solution basée sur la crypto-monnaie et un serveur d'horodatage peer-to-peer décentralisé tout en conservant les enregistrements des transactions.**[32]**

Cette solution, appelée blockchain, fournit une sécurité telle que le contrôle d'accès, le chiffrement et la cryptographie.

2. Blockchain

2.1 Définition générale

« L'idée d'un grand cahier informatique, partagé, infalsifiable et indestructible du fait même de sa conception est au cœur d'une nouvelle révolution, celle de la blockchain. » **[33]**

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. **[34]**

Une blockchain (mot anglais) est définie comme une chaîne de blocs de données ordonnées. C'est une nouvelle technologie de stockage et de transmission, techniquement une nouvelle génération de bases de Données distribuées, sécurisées, transparentes et fonctionnant sans autorité centrale, s'appuyant et tirant pleinement profit d'Internet, du protocole libre, de la puissance de calcul et de la cryptographie **[35]**

Il s'agit avant tout d'une technologie basée sur des systèmes de transmission peer-to-peer décentralisés sans intermédiaires, tiers de confiance ou autorités centrales (établissements bancaires, agences gouvernementales, etc.).**[36]**

Cette nouvelle technologie ressemble à un grand registre numérique public partagé contenant des données, des informations et des enregistrements des transactions des utilisateurs, regroupés en blocs et liés de manière irréversible les uns aux autres par un processus cryptographique. Ainsi, chaque membre du réseau dispose d'une copie stockée localement de la blockchain et la met à jour chaque fois qu'un bloc est ajouté.**[36]**

Cette chaîne est visible et accessible par tous les nœuds du réseau, assurant un haut niveau de fiabilité. Par conséquent, vous ne pouvez pas modifier ou supprimer des blocs existants ou modifier l'ordre dans lequel ils sont ajoutés.**[36]**

2.2 Caractéristiques de blockchain

La technologie blockchain se caractérise par six éléments principaux : Décentralisé, transparent, sécurisé et immuable, autonome, open source, anonyme. Comme mentionné ci-dessus :

- **Elle est décentralisée :**

La blockchain contient un système de base de données décentralisé accessible à toute personne connectée au réseau. Les données peuvent être visualisées, surveillées, stockées et mises à jour sur plusieurs systèmes.

Toutes ces données ne sont pas agrégées sur un serveur intermédiaire central, mais à l'inverse elles sont « distribuées », C'est-à-dire qu'il est hébergé par chaque participant. Par conséquent, il n'y a pas d'autorité unique pour approuver une transaction ou établir des règles spécifiques pour accepter une transaction.

Cela signifie que la confiance est très élevée car chaque participant au réseau doit parvenir à un consensus afin d'accepter la transaction. **[37]**

- **Elle est transparente** : C'est l'avantage le plus important. Tous les participants peuvent voir les blocs et les transactions qui y sont stockés. Les données capturées et stockées sur la blockchain sont transparentes pour les utilisateurs potentiels et peuvent être facilement mises à jour. Cependant, cela ne signifie pas que n'importe qui peut voir le contenu réel de la transaction protégée par la clé privée.

Le consensus **:** est un mécanisme qui permet d'ajouter des blocs à la blockchain après que les données téléchargées sur la blockchain ont été vérifiées par la décision d'une majorité de participants et qu'un consensus est atteint. **[37]**

Voici une figure (7) qui montre les mécanismes de la Blockchain « Transaction et Consensus »

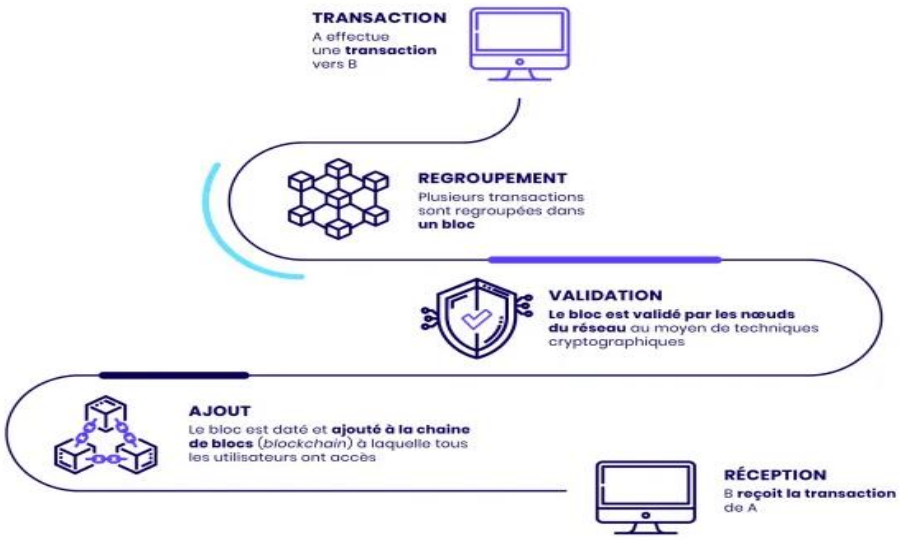


Figure 7 Fonctionnement de la Blockchain (Transaction et Consensus) [38]

- **Elle est sécurisée :** La base de données est uniquement évolutive et ne peut pas modifier les anciens enregistrements (au moins, modifier les anciens enregistrements coûte très cher).
  Ces éléments sont immuables et, une fois stockés, ils sont réservés en permanence et ne peuvent pas être facilement modifiés sans un contrôle simultané de plus De 51 % des nœuds du réseau.
  Le système cryptographique de vérification assure qu'il est pratiquement impossible de réécrire une transaction après qu'un bloc a été vérifié (personne n'a pu le faire depuis la création de Bitcoin) **[37]**
- **Autonome** : Le système blockchain est indépendant et autonome. Cela signifie que chaque nœud du système blockchain peut accéder, transférer, stocker et mettre à jour les données en toute sécurité, ce qui les rend fiables et exemptes d'interférences externes. **[37]**
- **Open source** : La technologie Blockchain est conçue pour fournir un accès open source à toute personne connectée au réseau. Cette polyvalence permet à quiconque non seulement de valider publiquement des enregistrements, mais également de développer une variété d'applications imminentes. **[37]**

- **Anonyme** : Lorsque les données sont transférées entre les nœuds, l'identité de l'individu reste anonyme, ce qui rend le système plus sûr et plus fiable. Quelqu'un qui fait partie de ce réseau a besoin de voir toutes les Nouvelles transactions effectuées. Les transactions de recherche au sein d'un bloc de la blockchain sont validées par tous les nœuds du réseau et deviennent de plus en plus immuables. **[37]**

2.3 Les couches de la blockchain

La blockchain est utilisée dans divers domaines, chacun ayant son propre ensemble d'applications. Contrairement à l'Internet, la structure de la blockchain ne peut pas être généralisée car différents cas d'utilisation nécessiteraient des structures différentes **[39].**

2.3.1 Couche matérielle ou infrastructure

La première couche de la Blockchain est la couche d'infrastructure ou couche matérielle. Le contenu de la Blockchain est maintenu sur des nœuds, qui sont des serveurs ou des ordinateurs à haute performance qui sont situés à distance. Chaque nœud est chargé de valider des transactions, d'organiser des transactions à l'intérieur des blocs, de diffuser les transactions au réseau Blockchain, etc. Ces nœuds sont également chargés de connecter un bloc au réseau. Suite au consensus, ces nœuds sont également chargés d'ajouter un bloc à la chaîne **[39].**

2.3.2 Couche de données

Un bloc individuel dans la Blockchain est une structure de données conteneur qui peut contenir bien plus qu'une liste de transactions. Cette couche est en charge de la structure des blocs dans la Blockchain. Cette couche est responsable de la structure du bloc dans la Blockchain. Les éléments de données d'un seul bloc sont divisés en deux sections, l'en-tête du bloc et le corps du bloc. Le corps du bloc contient la liste des transactions, tandis que l'en-tête de bloc contient des métadonnées sur le bloc en question**. [39]**

En-tête de bloc :

La section d'en-tête de bloc du bloc contient toutes les données concernant les données dans le bloc particulier. L'en-tête de bloc du bloc de bitcoin est en outre subdivisé en six sous-sections, telles que comme **[39]** :

- **Version :** Le numéro de version du logiciel.
- **Last Block :** La valeur de hachage du bloc précédent.
- **Merkle Root :** La racine de l'arbre de Merkle.
- **Time :** Le temps en seconde depuis 1970-01-01 T00:00UTC.
- **Miner :** Informations sur le mineur.
- **Target :** La taille du hachage en bits.
- **The Nonce :** Une variable incrémentée par la preuve de travail.

Corps du bloc :

Le corps du bloc contient toutes les transactions confirmées du bloc. Lorsqu'une transaction doit être Lorsqu'une transaction doit être vérifiée, les nœuds du réseau vérifient les transactions contenues dans le corps du bloc**. [39]** Voici un schéma récapitulatif de ce que contient un bloc (**Figure 8)**

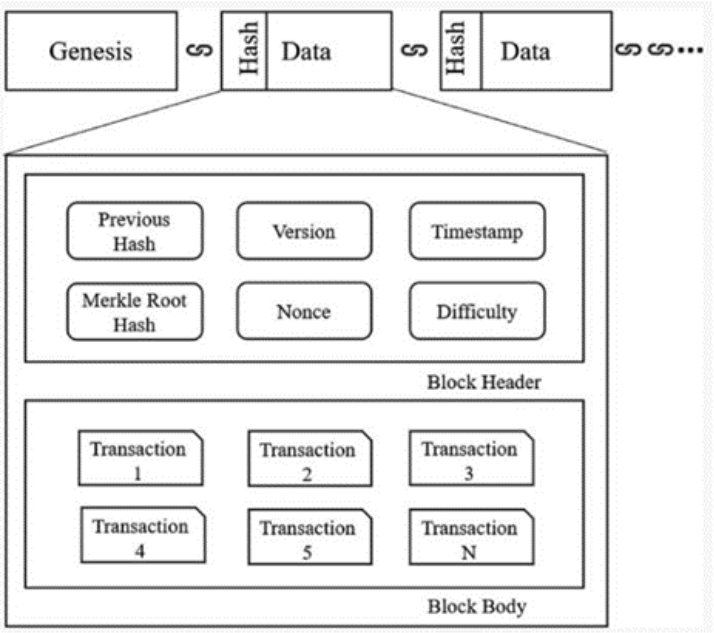


Figure 8 Exemple d'une blockchain contenant trois blocs [40]

2.3.3 Couche réseau

Dans la Blockchain, la couche réseau est également connue sous le nom de couche P2P ou peer-to-peer. Le nœud complet et le nœud léger sont deux types de nœuds différents. Les nœuds complets sont chargés de la vérification et de la confirmation des transactions, du minage et du consensus. Les nœuds légers, quant à eux, se contentent de conserver les en-têtes de la blockchain et de les soumettre au besoin. La couche réseau est responsable de la communication entre les nœuds **[39].**

2.3.4 Couche de consensus

C'est la couche la plus importante et la plus vitale de toute Blockchain. Cette couche est chargée de valider et d'organiser les blocs. Le mécanisme de consensus est la raison pour laquelle les Blockchains sont plus sûres et plus fiables que toute autre méthode conventionnelle **[39].**

2.3.5 Couche d'application

La couche d'application ou la couche de présentation est la couche la plus basse. Cette couche est Cette couche comprend les contrats intelligents, le code de la chaîne et les applications. La couche d'application est en outre divisée en deux sous-couches, à savoir la sous-couche d'application et la sous-couche d'exécution. La sous-couche d'application est un ensemble de logiciels utilisés par les utilisateurs pour interagir avec la Blockchain. La sous-couche d'exécution comprend les contrats intelligents, le code de la chaîne et les règles sous-jacentes. Cette sous-couche contient le code exécutable réel et les règles à suivre. **[39]**

2.4 Les types des systèmes de blockchain

La diversité de la recherche et du développement de la blockchain offre la possibilité de classer la blockchain en catégories selon un ensemble de critères comme la décentralisation, l'immuabilité, processus de consensus...

2.4.1 Blockchain publique :

Dans une blockchain publique, tous les enregistrements sont visibles par le public, et puisque n'importe qui peut participer au processus de consensus (n'importe qui peut devenir un nœud), on peut s'attendre à voir une décentralisation sur une topologie de réseau établie. Étant donné que les transactions sont stockées dans différents nœuds du réseau distribué, il est presque impossible de falsifier la blockchain publique. En termes de rapidité, en raison du grand nombre de nœuds sur un réseau de blockchain public, la propagation des transactions et des blocs prend beaucoup de temps car le processus de consensus prend plus de temps par rapport aux blockchains privées ou de consortium.**[41]**

2.4.2 Blockchain privée :

Considéré comme un réseau centralisé car entièrement contrôlé par une seule organisation, tous les nœuds du système sont identifiés et connus. Étant donné que seuls les utilisateurs autorisés gèrent la blockchain, il est possible de restreindre l'accès en lecture et de limiter qui peut émettre des transactions. Par conséquent, dans un réseau blockchain autorisé, n'importe qui peut lire la blockchain ou restreindre l'accès en lecture aux personnes autorisées. Ils peuvent également permettre à quiconque de soumettre une transaction pour inclusion dans la blockchain, ou encore, ils peuvent restreindre cet accès aux seules personnes autorisées. Les réseaux de blockchain de confiance peuvent être instanciés et maintenus à l'aide de logiciels open source ou fermés. Il est plus efficace d'utiliser moins de validateurs**.[41]**

- **Blockchain de consortium :**

Aussi appelé hybride. Ce type n'est pas contrôlé par une autorité unique, mais par un groupe spécifique créé pour contrôler le processus de consensus. La blockchain du consortium est un système "semi-privé" avec un Ensemble contrôlé d'utilisateurs, mais exploité par différentes organisations. Souvent liés à l'utilisation en entreprise, les groupes d'entreprises travaillent ensemble pour utiliser la technologie blockchain afin D'améliorer les processus métier. Comme la blockchain privée il est plus efficace que la blockchain publique.**[41]**

Une comparaison entre les trois types de blockchain est répertoriée dans la figure

Type de blockchain / Propriété	Blockchain public	Blockchain privé	Blockchain à Consortium
Qui peut la consulter ?	Tout le monde	Seulement les utilisateurs invités	Cela varie
Centralisé	Non	Oui	Partiel
Vitesse de transaction	Lente	Rapide	Rapide
Immutabilité	Presque impossible à falsifier	Pourrait être falsifié	Pourrait être falsifié
Anonymat des utiisateurs	Oui	Non	Non
Détermination du consensus	Tous les noeuds	Une organisation	ensemble de nœuds sélectionné
Permission	Sans autorisation	autorisé	autorisé

Figure 9 Comparaison entre les 3 types de blockchain public, privé, consortium [41]

2.5 Principaux domaines d'utilisation de la blockchain

L'utilisation des blockchains peut être classée en cinq grandes catégories, liées d'une part à la conservation des données et d'autre part à la facilitation des transactions :

2.5.1 Registre statique :

Les blockchains statiques ont tendance à être moins gourmandes en ressources informatiques puisque les enregistrements ne sont pas fréquemment modifiés. L'exportation des données de la blockchain statique vers une plateforme d'analyse vous permet d'examiner diverses caractéristiques de transaction, de segmenter

Les transactions, d'analyser les tendances, de prédire les événements futurs et d'identifier les relations entre la blockchain et d'autres sources de données. Ici, le grand livre se compose d'enregistrements qui sont stockés à des fins de référence. Par exemple, le titre foncier. Il existe de nombreux cas d'ambiguïté dans la propriété des titres. Avec la technologie blockchain, les enregistrements une fois stockés ne peuvent pas être modifiés. Toute modification est horodatée. En cas de

Litige, le titre peut être retracé par le chemin d'origine. Les autres endroits où elle peut être utilisée sont les brevets, les articles de recherche et les registres de sécurité alimentaire et d'origine. **[42]**

- **Identité :**

La gestion des identités est vitale dans l'économie moderne d'aujourd'hui, basée sur l'Internet. Malheureusement, les solutions actuelles de gestion de l'identité ont désespérément besoin d'être améliorées.

Chaque année, le nombre et l'ampleur des vols d'identité augmentent à un rythme alarmant. L'un des principaux problèmes liés à cette tendance est l'incapacité des solutions d'identité actuelles à suivre le rythme des violations de sécurité. Il existe une technologie qui promet à la fois de rendre les solutions logicielles d'identité et leur gestion beaucoup plus sûres et accessibles, cette technologie est Blockchain. **[42]**

- **Contrats intelligents :**

Une base de données distribuée qui contient les conditions enregistrées nécessaires au déclenchement d'une action, telle qu'un paiement ou le transfert d'un actif.

De plus, les contrats intelligents ne se contentent pas de définir les règles et les sanctions relatives à un accord de la même manière qu'un contrat traditionnel, mais ils permettent également d'appliquer automatiquement ces obligations. **[42]**

2.5.2 Registre dynamique :

Base de données distribuée qui se met automatiquement à jour au fur et à mesure que les actifs sont échangés par les membres. La distribution est unique : les enregistrements ne sont pas communiqués aux différents nœuds par une autorité centrale, mais sont au contraire construits et détenus indépendamment par chaque nœud. En d'autres termes, chaque nœud du réseau traite chaque transaction, en tirant ses propres conclusions, puis en votant sur ces conclusions pour s'assurer que la majorité est d'accord avec ces dernières.

L'invention des grands livres distribués représente une révolution dans la façon dont les informations sont recueillies et communiquées. Les transactions dynamiques permettent aux utilisateurs d'aller au-delà de la simple garde d'une base de données et de consacrer leur énergie à la manière dont ils utilisent, manipulent et extraient la valeur des bases de données - il s'agit moins de maintenir une base de données que de gérer un système d'enregistrement. **[42]**

2.5.3 Registre des paiements

La blockchain est reconnue comme la nouvelle technologie qui permettrait de réduire la fraude dans le monde financier où 45% des intermédiaires financiers comme les bourses et les services de transfert d'argent sont sujets à des crimes financiers de façon routinière. Il s'agit d'un registre dynamique qui se met à jour au fur et à mesure que les paiements en espèces ou en crypto-monnaies sont effectués sur le réseau. Cela est avantageux pour les paiements internationaux dans les entreprises.

La plupart des systèmes bancaires dans le monde, construits sur une base de données centralisée, sont plus vulnérables aux cyberattaques car une fois que les pirates attaquent le seul système, ils obtiennent un accès complet. Cette technologie permettrait de se débarrasser de certains des crimes actuels commis en ligne contre nos institutions financières. **[42]**

2.6 défis de la blockchain

- **Un impact environnemental :**

Certaines blockchains sont très gourmandes en énergie. Le réseau Ethereum, principale cryptomonnaie concurrente du Bitcoin, consommerait autant d'électricité qu'un pays comme Chypre, soit environ 4,2 térawatt-heure**.[43]**

- **Des limites de "scalabilité" :**

La puissance de calcul nécessaire pour faire fonctionner la blockchain augmente constamment. Une blockchain comme Bitcoin arrive aujourd'hui difficilement à gérer un nombre très élevé de transactions (le réseau étant vite engorgé) **[44]**

- **Des capacités transactionnelles limitées en fonction de la technologie retenue :**

La blockchain Ethereum enregistre 25 transactions par seconde VS le réseau bancaire Visa qui comptabilise jusqu'à 20 000 transactions par seconde.**[45]**

- **Une utilisation restreinte en santé :**

Une blockchain publique ne peut pas stocker l'ensemble des données de santé d'un patient mais seulement quelques données standardisées.**[44]**

- **L'absence de réglementation en vigueur**

Le droit à l'oubli par exemple, une réglementation fixée par la CNIL, ne peut pas être pris en compte par cette technologie à ce jour car les données ne sont ni modifiables, ni supprimables**.[44]**

2.7 blockchain et contrat intelligent

2.7.1 définition de contrat intelligent

Les contrats intelligents ou (smart contracts), sont des programmes informatiques exécutant un ensemble d'instructions prédéfinies (si telle condition est remplie, telle transaction est faite), garantissant la force obligatoire des contrats non plus par le droit, mais par le code Ces smart contacts sont souvent partie intégrante du fonctionnement de blockchains récentes.**[46]**

2.7.2 Fonctionnement des contrats intelligents

Les contrats intelligents fonctionnent en utilisant de simples instructions if/when…then… écrites dans un code dans une blockchain. L'exécution des actions lorsque des conditions prédéterminées sont remplies et vérifiées se fait à travers un réseau d'ordinateurs. Ces actions peuvent inclure le déblocage de fonds aux parties concernées, L'enregistrement d'un véhicule, l'envoi de notifications ou l'émission d'un ticket. La blockchain est ensuite mise à jour lorsque la transaction est terminée. Cela signifie que la transaction ne peut pas être modifiée et que seules les parties qui ont reçu le droit accordé peuvent voir les résultats.

Dans un contrat intelligent, on trouve plusieurs conditions nécessaires pour convaincre les participants que la tâche sera accomplie de manière satisfaisante. Pour établir les conditions, les participants doivent savoir comment les transactions et leurs données sont représentées dans la blockchain, se mettre d'accord sur les règles « if/when...then… » qui gèrent ces transactions, explorer toutes les exceptions possibles et définir un cadre de résolution des différends.**[46]**

2.7.3 Avantages des contrats intelligents

Rapidité, efficience et exactitude :

Une fois une condition respectée, le contrat est exécuté immédiatement. Les contrats intelligents sont numériques et automatisés, donc aucun traitement de document papier n'a lieu et aucun temps n'est consacré à rectifier les erreurs qui résultent généralement du remplissage manuel des documents**.[46]**

Confiance et transparence :

Il n'est pas possible de modifier les informations pour un usage personnel en l'absence d'un tiers**.[46]**

Sécurité :

Impossible de pirater les enregistrements de transaction dans la blockchain car ils sont cryptés. De plus, comme chaque enregistrement est relié aux enregistrements précédents et suivants dans un grand livre distribué, les pirates devraient modifier toute la chaîne pour changer un seul enregistrement.**[46]**

Économies :

Les contrats intelligents n'ont pas besoin d'intermédiaires pour gérer les transactions, ils évitent donc le temps et les frais associés.**[46]**

2.7.4 Applications des contrats intelligents

- **Préserver l'efficacité des médicaments :**

Sonoco et IBM travaillent dur pour améliorer la transparence de la chaîne d'approvisionnement en réduisant les tracas liés au transport de médicaments vitaux. Les produits pharmaceutiques nécessitant un contrôle de la température sont suivis tout au long de la chaîne d'approvisionnement afin de fournir des données fiables et précises à plusieurs parties et cela est optimisée par IBM Blockchain Transparent Supply, Pharma Portal, une plateforme basée sur la blockchain.**[46]**

- **Renforcer la confiance dans les relations entre distributeurs et fournisseurs :**

The Home Depot utilise des contrats intelligents dans la blockchain pour résoudre rapidement les différends avec les fournisseurs. Ils établissent des relations plus solides avec les fournisseurs, leur permettant de consacrer plus de temps aux tâches essentielles et à l'innovation grâce à une communication en temps réel et à une visibilité accrue des canaux.**[46]**

- **Accélérer le commerce international et le rendre plus efficace :**

En rejoignant we.trade, le réseau de financement du commerce organisé par IBM Blockchain, les entreprises créent un écosystème de confiance pour le commerce mondial. En tant que plateforme basée sur la blockchain, pour réduire les frictions et les risques tout en facilitant le processus de négociation et en élargissant les opportunités commerciales pour les entreprises et les banques participantes, we.trade utilise des règles standardisées et des options de négociation simplifiées.**[46]**

2.8 Blockchain et les jetons non-fongible (NFT)

2.8.1 Définition de NFT

Depuis peu, NFT est devenu le sujet de nombreuses discussions, surtout dans le domaine de l'art. Mais c'est quoi un NFT ?

NFT signifie en anglais *non-fungible token*, soit jeton non fongible en français. Un objet non fongible est un objet unique non modifiable. Par exemple, l'argent est fongible, on peut échanger des euros ou des cryptomonnaies, mais une œuvre d'art est non fongible, car unique.

Un NFT c'est un fichier numérique authentifié par un certificat numérique. Plus exactement, le NFT est un jeton cryptographique stocké sur une blockchain. Le fichier numérique seul est fongible, qu'il s'agisse d'une photo, d'une vidéo ou données, le NFT associé est non fongible. **[47]**

2.8.2 Utilisations de NFT dans le domaine médical

Les jetons non fongibles (NFT) peuvent-ils servir dans le domaine médical ? Généralement, oui ! Après il est devenu un événement important dans le domaine de l'art et a occupé les premières pages des journaux et des médias sur Internet .C'est dans le secteur de la santé qu'ils reviennent sur le devant de la scène.

Désormais, les NFT, permettre de suivre les informations relatives au consentement des patients dans le cadre des essais cliniques, C'est l'idée avancée par des chercheurs en éthique médicale qui voient dans cette technologie un moyen pour les patients de reprendre la main sur leurs données**.[48]**

3. LE CONTROLE D'ACCES

3.1 Définition du contrôle d'accès

Il est utile de rappeler que l'une des premières mesures en sécurité informatique consiste à contrôler les différents accès possibles à un système d'information et à autoriser ou non un certain nombre d'actions en fonction de l'utilisateur.

Il s'agit de limiter l'accès aux ressources du système d'information uniquement aux utilisateurs, programmes, procédés ou systèmes autorisés.

Le contrôle d'accès est défini comme n'importe quel mécanisme par lequel un système autorise ou interdit le droit à des entités actives d'accéder à des entités passives (objets), ou d'effectuer des opérations.

Il consiste à vérifier si une entité (une personne, un ordinateur, etc.) désireuse d'accéder à une ressource possède les droits nécessaires pour le faire.**[49]**

3.2 Objectifs du contrôle d'accès

Préserver la confidentialité, l'intégrité et la disponibilité des données.

- **La confidentialité** permet d'empêcher la divulgation non-autorisée de données.
- **L'intégrité** permet d'empêcher la modification non-autorisée de données.
- **La disponibilité** est la propriété d'une information d'être accessible lorsqu'un utilisateur autorisé en a besoin. **[49]**

3.3 Politique de contrôle d'accès

Dans un système informatique, l'autorisation a pour but de ne permettre que les actions légitimes, c'est-à-dire empêcher qu'un utilisateur puisse exécuter des opérations qui ne lui sont pas permises. Pour définir quelles sont les opérations autorisées et celles qui sont interdites, il faut établir une politique de contrôle d'accès.

3.4 Concepts fondamentaux d'une politique de contrôle d'accès

- **Sujet** : entité active qui accède aux données du système. Le sujet peut être un utilisateur, une application, une adresse IP…
- **Objet :** entité passive qui représente les données à protéger. L'objet peut être : un fichier, une table relationnelle, une classe …
- **Action :** représente l'action à traiter par le sujet sur l'objet.
  L'action peut être : lire, écrire, exécuter … **[49]**

3.5. Axes de la politique de contrôle d'accès

Une politique de contrôle d'accès peut se développer dans trois directions distinctes : les politiques de sécurité physique, administrative et logique**.[50]** illustrées dans la figure (10) ci-dessous.

Type	Description	*Exemples*
Physique	restrictions d'accès physiques aux ressources	*barrières* *coffres* *passes et clefs*
Administrative	règlements et procédures pour renforcer la sécurité	*enquêtes, audits* *reponsabilisation* *bonnes pratiques*
Logique	restrictions d'accès logiques aux ressources informatisées, mises en œuvre par des logiciels et matériels	*authentification* *identification* *cryptage* *cloisonnement* *organisation des droits*

Figure 10 Figure 10 Spécialisations des politiques de sécurité [50]

3.6 Modèles de contrôle d'accès

On distingue principalement trois grandes catégories de modèles de contrôle d'accès : les modèles de contrôle d'accès discrétionnaires DAC (Discretionary Access Control) et le modèle de contrôle d'accès obligatoires MAC (Mandatory Access Control). Afin de mieux s'adapter à des organisations particulières, d'autres modèles ont été définis, en particulier, le modèle de contrôle d'accès basé sur la notion de rôle RBAC (RoleBased Access Control).**[51]**

- **Modèles de contrôle d'accès discrétionnaires (DAC)**

Le contrôle d'accès discrétionnaire (DAC) a été défini à l'origine par Trusted Computer System Evaluation Criteria (TCSEC) comme « un moyen de restreindre l'accès aux objets en fonction de l'identité des sujets et/ou des groupes auxquels ils appartiennent. Les contrôles sont discrétionnaires en ce sens qu'un sujet ayant une certaine permission d'accès peut transmettre cette permission (peut-être indirectement) à tout autre sujet (à moins qu'elle ne soit restreinte par un contrôle d'accès obligatoire). »

En pratique, l'utilisation de cette terminologie n'est pas aussi claire. Dans l'interprétation la plus stricte, chaque objet contrôlé par un DAC doit avoir un propriétaire qui contrôle les permissions permettant l'accès à l'objet (figure 11). Bien que de nombreux systèmes d'exploitation modernes prennent en charge le concept de propriétaire, cela n'est pas toujours mis en œuvre. En particulier, la norme ne couvre pas les « propriétaires », ce qui laisse une définition problématique lorsque la propriété de groupe se produit**.[52]**

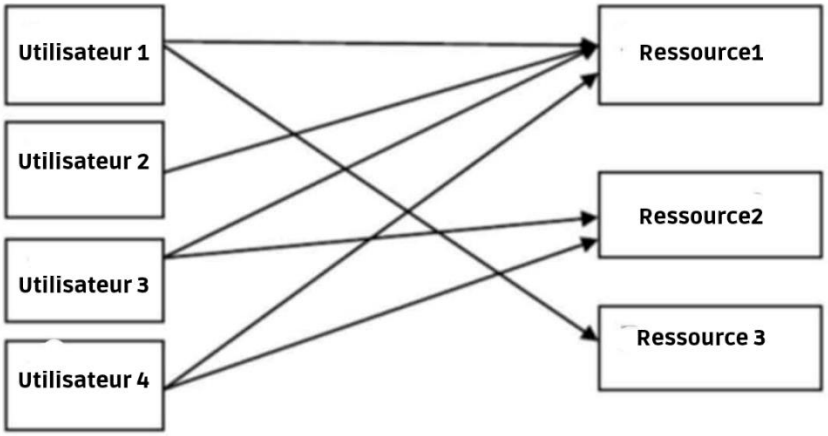


Figure 11 Modèle de contrôle d'acces DAC [53]

- **Modèles de contrôle d'accès obligatoires (MAC)**

Le Mandatory Access Control imposent le contrôle d'accès sur la base de la réglementation mandatée par une autorité centrale. La forme la plus courante de cette politique est la politique de sécurité à plusieurs niveaux, basée sur la classification des sujets et des objets dans le système (figure 12). Les objets sont des entités passives stockant des informations. Les sujets sont des entités actives qui demandent l'accès aux objets. Notez qu'il y a

une distinction entre les sujets de la politique obligatoires(mandatory) et les sujets d'autorisation politiques discrétionnaires. Bien que l'autorisation correspondent aux utilisateurs (ou groupes de ceux-ci), les politiques obligatoires(mandatory) font une distinction entre les utilisateurs et les sujets. Les utilisateurs sont des êtres humains qui peuvent accéder au système, tandis que les sujets sont des processus (c.-à-d. des programmes en cours d'exécution) fonctionnant pour le compte de utilisateurs. Cette distinction permet à la politique de contrôler les accès indirects (fuites ou modifications) causées par l'exécution de processus**.[54]**

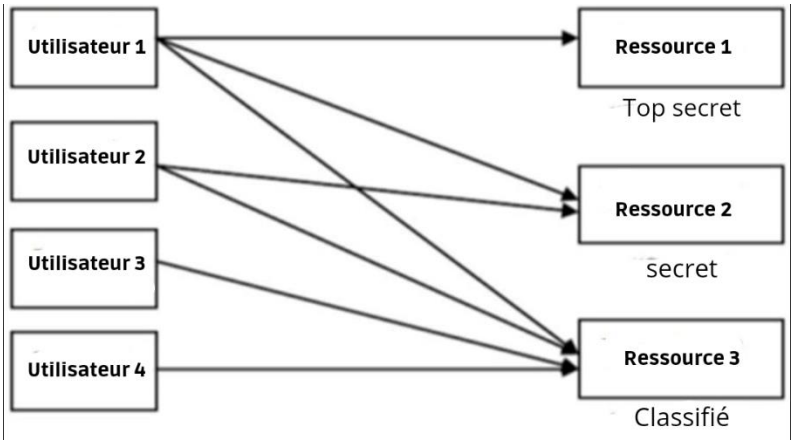


Figure 12 Modèle de contrôle d'acces MAC [53]

- **Modèles de contrôle d'accès à base de rôles (RBAC)**

Les modèles DAC et MAC ne sont pas bien adaptés aux besoins des organisations commerciales. Dans ce type d'organisation les privilèges conférés aux utilisateurs dépendent du rôle des utilisateurs au sein de l'organisation. De ce fait les modèles RBAC sont apparus et se sont imposés comme une alternative aux modèles DAC et MAC traditionnels. En 2004, l'International Committee for Information Technology Standards de l'American National Standards Institute (ANSI/INCITS) a officiellement élevé au statut de standard la proposition de Sandhu, Ferraiolo and Khun **[55].**

Les principes de base du modèle RBAC sont les suivants :

- Alors que dans les modèles DAC, les permissions ont trait à des opérations de bas niveau telles que les opérations de lecture/écriture, dans les modèles RBAC elles concernent des tâches de nature organisationnelle telles que « transférer de l'argent », « acheter un billet d'avion » etc. voir (figure 13).
- Dans les modèles RBAC, le concept de rôle correspond à une fonction professionnelle. Les permissions sont accordées à des rôles et non pas à des utilisateurs. Les rôles sont ensuite distribués aux utilisateurs en fonction de leurs responsabilités au sein de l'organisation. Une même permission peut être affectée à différents rôles et différents rôles peuvent être attribués à un même utilisateur.
- Les modèles RBAC offrent une solution pour implanter des mesures de type séparation des tâches. Le principe de la séparation des tâches prévoit qu'un même utilisateur ne peut effectuer des tâches qui pourraient être orchestrées pour mettre œuvre des opérations frauduleuses, comme par exemple « autoriser un paiement » et « effectuer un paiement ».

Ce principe peut aisément être garanti avec les modèles RBAC dans la mesure où deux rôles peuvent être déclarés comme étant mutuellement exclusifs. Deux rôles mutuellement exclusifs ne peuvent alors être affectés à un même utilisateur.

Le standard RBAC ne dit rien au sujet de l'administration du règlement de sécurité. Il suppose de manière implicite que la définition des rôles, l'affectation des permissions aux rôles et la distribution des rôles aux utilisateurs sont effectuées par une autorité centrale. Le modèle ARBAC (Administrative Role-Based Access Control est un modèle à base de rôles prévoyant des rôles correspondant aux fonctions d'administration du règlement de sécurité. Les modèles à base de rôles ont été implantés dans de nombreux systèmes et applications tels que Microsoft Active Directory, la plupart des SGBD commerciaux, FreeBSD et Wikipédia **[56].**

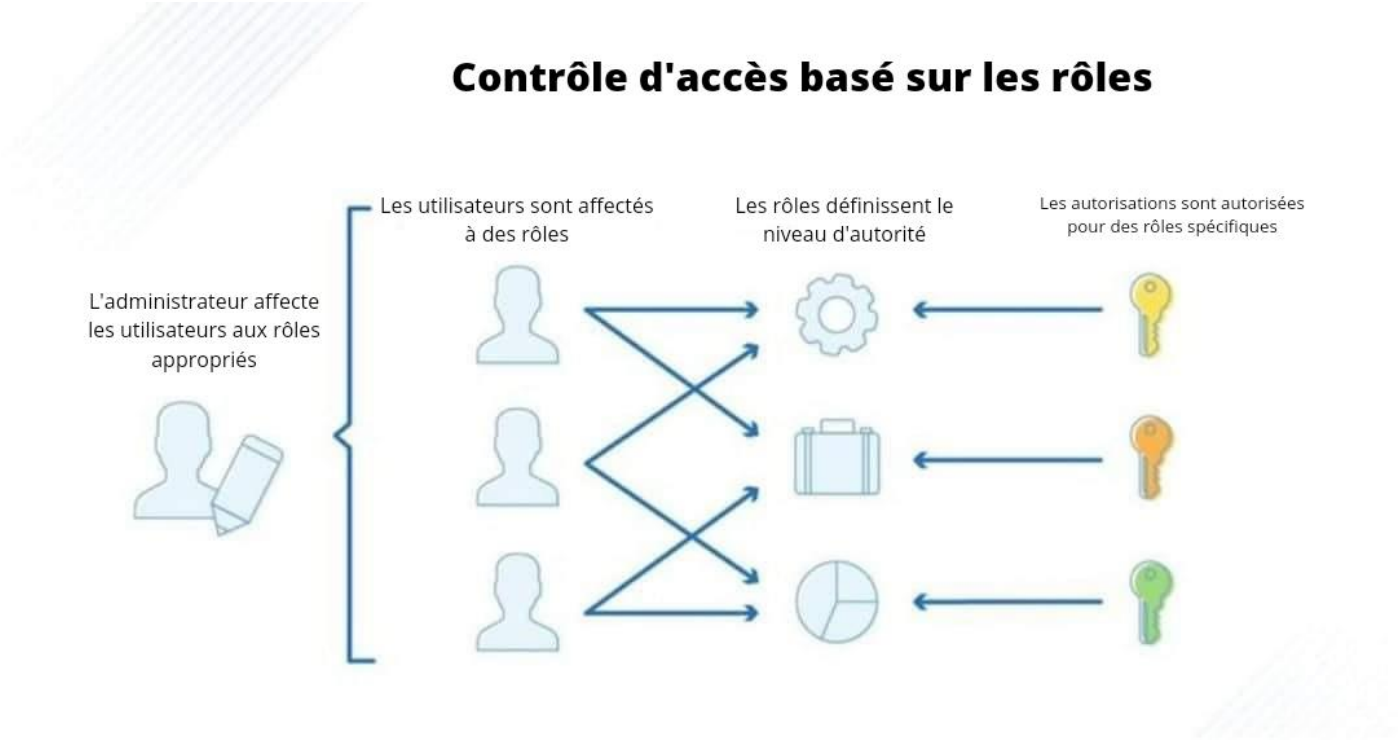


Figure 13 Modèle de contrôle d'acces RBAC [57]

- **Modèles de contrôle d'accès à base d'attribut (ABAC)**

Le modèle ABAC a été développé par Eric Yuan et Jin Tong dans le but de pallier aux difficultés que rencontrent les architectures web services en termes de sécurité. En effet, les accès à l'information au niveau de ces architectures web services se font non seulement sur les systèmes distribués mais très dynamiquement. Les modèles classiques sont généralement destinés à un fonctionnement statique, ils ne permettent guère une évolution dynamique. De part sa définition, le modèle ABAC peut être le plus adapté pour les architectures fonctionnant dans un environnement ouvert « in the cloud » où différentes organisations peuvent assurer à la fois les accès aux informations et la protection de leurs ressources.**[58]**

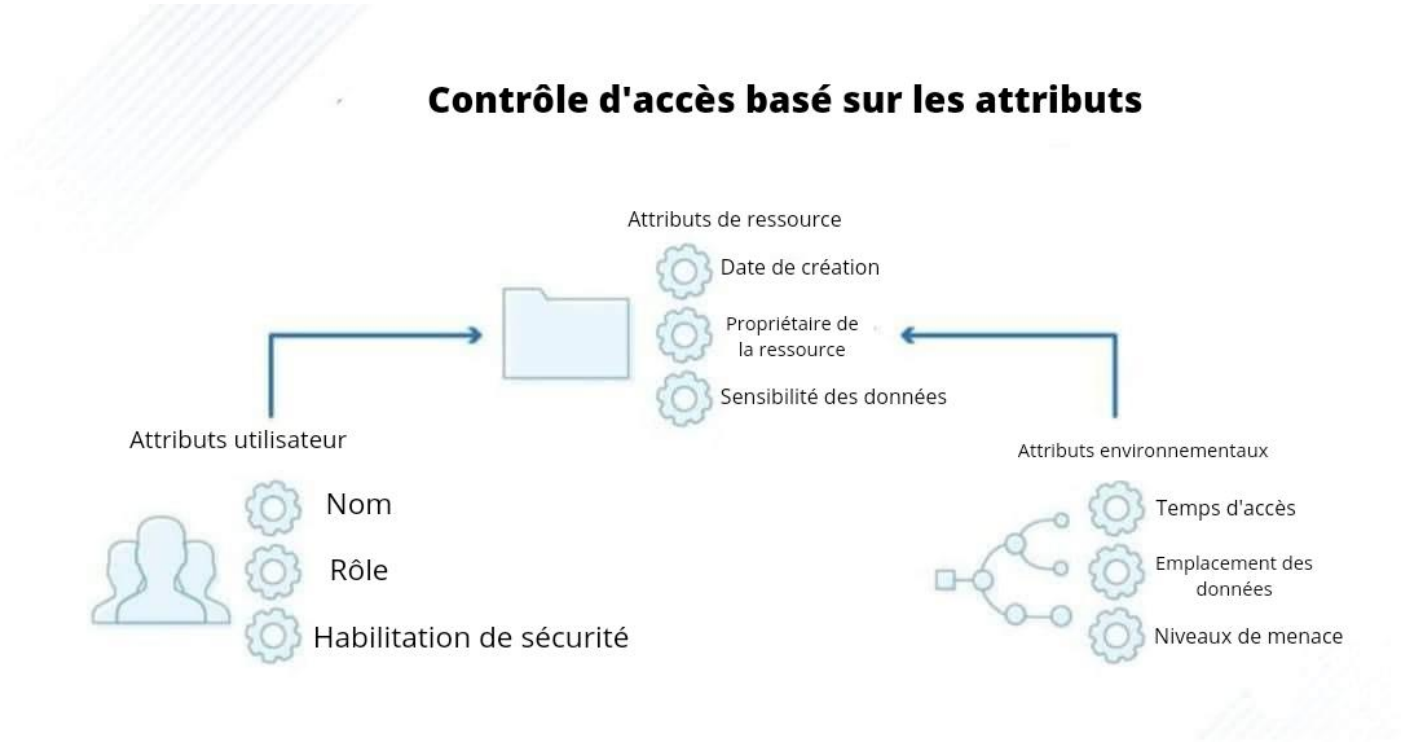


Figure 14 Modèle de contrôle d'acces ABAC [57]

Comme son nom l'indique, le modèle ABAC définit les autorisations d'accès en se basant sur des caractéristiques de chaque entité, appelés attributs (figure 14). Trois groupes d'attributs se distinguent selon le type de l'entité à laquelle ils s'appliquent :

- Les attributs des sujets : un sujet est une entité qui peut agir sur une ressource. A chaque sujet on associe des attributs qui définissent son identité et ses caractéristiques. Par exemple le rôle du sujet peut aussi être considéré comme un attribut, tout comme le nom, le prénom, ou le titre, etc.
- Les attributs des ressources : C'est un objet du système sur lequel un sujet peut agir. Autrement dit, c'est une entité qui peut être accéder accessible à un sujet. Une ressource peut être un fichier, un service, etc. A chaque ressource est associée des attributs, variables selon sa nature, mais qui peuvent être : son type, le nom de son auteur, son propriétaire, la date de modification, etc.
- Les attributs d'environnement : l'environnement peut être décrit par des informations opérationnelles, techniques, liées à la situation ou encore au contexte dans lequel l'accès à l'information se produit. La particularité du modèle, ABAC est la prise en compte du contexte d'exécution du système, en définissant des attributs d'environnement, comme par exemple : la date, le niveau de sécurité du réseau, le débit de la connexion, etc.

Cette particularité de prise en compte du contexte est très importante dans notre problématique où nous sommes appelés à gérer des tiers sujets n'appartenant à aucune organisation et qui souhaitent obtenir un service auprès de tierces organisations. Un des avantages de ce modèle est d'exploiter les opportunités offertes par les autres modèles, par exemple avec l'attribut du sujet « rôle » on peut appliquer le modèle RBAC.

3.7 Comparaison entre les différents modèles de contrôle d'accès

Le tableau 6 présente les avantages et les inconvénients des modèles de contrôle d'accès décrits précédemment. Notons ici que

-Le contrôle d'accès discrétionnaire et obligatoire offre deux extrémités opposées du spectre. Bien qu'un modèle de DAC puisse convenir aux petites entreprises, il ne favorise certainement pas l'expansion ni la sécurité de l'environnement à mesure que l'entreprise se développe.

- Un modèle MAC pourrait être assez sûr, mais il vient avec un coût opérationnel élevé, et en tant que tel est la méthode la moins efficace. Il ne faut pas oublier que la sécurité est une question d'équilibre. D'un côté, on veut donner aux gens le moyen de faire leur travail, sans sacrifier la sécurité. D'un autre côté, on ne veut pas verrouiller les choses jusqu'à ce que personne ne puisse faire son travail.

-Une distinction clé entre RBAC et ABAC est leur nature statique par rapport à dynamique, comme implicite dans leurs modèles respectifs. RBAC permet l'accès basé sur des rôles, qui sont généralement assez statiques au sein d'une organisation. Par ailleurs, ABAC s'appuie sur des attributs, qui peuvent être dynamiques - changeants, par exemple, lorsqu'un utilisateur tente d'accéder à une ressource à partir d'un périphérique ou d'une adresse IP différent.

- ABAC peut être automatisé pour mettre à jour les autorisations et, une fois que tout est configuré, nécessite moins d'administration globale. Il est également sécurisé lorsqu'il est correctement configuré. Toutefois, ABAC peut être assez complexe et spécifique à l'environnement, et les ensembles d'attributs compliqués peuvent être difficiles à mettre à l'échelle. Il est également difficile d'effectuer un audit à des fins de conformité - on doit vérifier chaque objet individuel par rapport à notre politique d'accès, au lieu de simplement vérifier l'accès d'un utilisateur particulier.

- RBAC, d'autre part, est très efficace et peut rationaliser le processus de conformité. Bien que toute forme de contrôle d'accès s'accompagne d'un certain degré de complexité, le RBAC est suffisamment transparent pour qu'on puisse voir comment les individus interagissent avec les ressources en fonction de leurs rôles. Et, conformément à l'adage :

« La complexité est l'ennemi de la sécurité », parce que sa configuration est relativement simple, on peut contrôler plus facilement l'accès aux données sensibles, ce qui peut entraîner moins de violations. Cependant, la gestion des rôles de RBAC peut devenir difficile et complexe dans un environnement qui a une multitude de rôles différents, chacun avec son propre ensemble complexe d'autorisations.

Dans notre projet, MAC et DAC ne sont pas des choix judicieux que l'on pourrait utiliser dans une application e-santé basé sur la blockchain. Par ailleurs, les modèles ABAC et RBAC semblent plus réalisables et sont les plus utilisés dans ce domaine. De plus, ABAC avec son utilisation de multiple et différent type d'attributs (environnement, ressources, sujets) qui définisse l'utilisateur et avec la possibilité d'utilisation du chiffrement par attribut (ABE), semble beaucoup plus adapté pour les applications e-santé.

Contrôle d'acces	Les avantages	Les inconvénients
DAC	**Convivial :** Les utilisateurs peuvent gérer leurs données et accéder rapidement aux données d'autres utilisateurs. **Flexible** : Les utilisateurs peuvent configurer les paramètres d'accès aux données sans administrateur. **Facile à entretenir :** L'ajout de nouveaux objets et d'utilisateurs ne prend pasbeaucoup de temps pour l'administrateur. **Granulaire :** Les utilisateurs peuvent configurer les paramètres d'accès pourchaque élément de données.	**Faible niveau de protection des données** : LeDAC ne peut garantir une sécurité fiable car les utilisateurs peuvent partager leurs données comme ils le souhaitent. **Obscur :** Il n'y a pas de gestion centralisée des accès, donc pour connaître les paramètres d'accès, on doit vérifier chaque ACL.
MAC	**Niveau élevé de protection des données :** Un administrateur définit l'accès auxobjets, et les utilisateurs ne peuvent pas modifier cet accès. **Granulaire** : Un administrateur définit manuellement les droits d'accès des utilisateurs et les paramètres d'accès aux objets. **Immunisé contre les attaques de chevaux de Troie :** Les utilisateurs ne peuventdéclassifier les données ou partager l'accès aux données classifiées.	**Maintenabilité :** La configuration manuelle des niveaux de sécuritéet des habilitations nécessite une attention constante de la part des administrateurs. **Évolutivité :** MAC ne s'adapte pas automatiquement. **Non convivial :** Les utilisateurs doivent demander l'accès à chaque nouvelle donnée ; ils ne peuvent pas configurer les paramètres d'accès pour leurs propres données.
RBAC	**Contrôle précis :** plus besoin d'autoriser ou de révoquer l'accès sur une baseindividuelle, rassemblant les utilisateurs en fonction de leurs rôles à la place **Facile à implémenter :** L'établissement d'un ensemble de rôles dans une petiteou moyenne entreprise n'est pas difficile	**Statique :** Les permissions ne peuvent être attribuées qu'aux rôles des utilisateurs et non aux objets et aux opération
ABAC	**Dynamique :** accorde l'accès en fonction non pas du rôle de l'utilisateur, mais des attributs de chaque composante du système. De cette façon, on peut décrire une règle d'affaires de toute complexité. Même si on doit rendre certaines données accessibles uniquement pendant les heures de travail	Ce type de système est difficile à configurer enraison de la façon dont les politiques doivent être spécifiées et maintenues

4. Blockchain et E-santé

Le secteur de la santé fait face à de nombreux problèmes que certaines entreprises tentent désormais de résoudre. Les principaux problèmes concernent la fragmentation des données médicales, les faux médicaments et le manque de transparence. **[59]**

Sécurisation des données des patients :

Garder nos données médicales sûres et sécurisées est très important. La sécurité est un enjeu majeur dans le secteur de la santé. Entre 2009 et 2017, plus de 176 millions de dossiers de patients **[60]** ont été exposés à des violations de données. Les auteurs ont volé des informations de carte de crédit et bancaires, ainsi que des dossiers de santé et de tests génomiques

La capacité de Blockchain à conserver un journal incorruptible, décentralisé et transparent de toutes les données des patients en fait une technologie répandue pour les applications de sécurité. De plus, bien que la blockchain soit transparente, elle est également privée, cachant l'identité de tout individu avec des codes complexes et sécurisés qui peuvent protéger la sensibilité des données médicales. La nature décentralisée de la technologie permet également aux patients, aux médecins et aux prestataires de soins de partager les mêmes informations rapidement et en toute sécurité**.[61]**

- **Les dossiers médicaux de la blockchain peuvent rationaliser les soins et éviter des erreurs coûteuses :**

Une mauvaise communication entre les professionnels de la santé coûte au secteur de la santé la somme colossale de 11 milliards de dollars par an **[62].** Le long processus d'obtention de l'accès aux dossiers médicaux d'un patient épuise les ressources du personnel et retarde les soins des patients. Les dossiers médicaux basés sur la blockchain offrent un remède à ces maux. La nature décentralisée de la technologie crée un écosystème de données sur les patients qui peut être référencé rapidement et efficacement par les médecins, les hôpitaux, les pharmaciens et toute autre personne impliquée dans le traitement. De cette manière, la blockchain peut conduire à des diagnostics plus rapides et à des plans de soins personnalisés.**[63]**

- **Gestion de la chaîne d'approvisionnement médicale et traçabilité/sécurité des médicaments :**

Que savons-nous vraiment de nos médicaments ? Vient-il d'un fournisseur légitime ? Pouvons-nous être sûrs qu'il n'a pas été falsifié ? Ces questions sont les principales préoccupations du lien entre le laboratoire et le marché (pharmacie). [**64]**

Blockchain a des effets positifs sur la gestion de la chaîne d'approvisionnement pharmaceutique, tel que sa décentralisation garantit pratiquement une transparence totale dans le processus d'expédition. Une fois qu'un registre pour un médicament est créé, il marquera le point d'origine (c'est-à-dire un laboratoire). Le grand livre continuera ensuite d'enregistrer des données à chaque étape du processus, y compris qui les a manipulées et où elles se sont rendues, jusqu'à ce qu'elles atteignent le consommateur. Le processus peut même surveiller les coûts de main-d'œuvre et les émissions de déchets**.[65]**

5. Conclusion

En conclusion, la blockchain présente certains avantages tels que la sécurité, l'anonymat et l'intégrité des données sans intervention de tiers. Ces avantages en font un choix logique pour stocker les dossiers médicaux des patients, Mais la protection des données n'est pas le seul défi auquel est confronté le secteur de la santé. Pour que la blockchain soit efficace à 100%, il faut des données médicales entièrement numérisées, ainsi que des logiciels interopérables entre l'assurance maladie, l'hôpital et les dossiers médicaux.

CHAPITRE 3 : CONTRIBUTION ET RESULTATS

1. Introduction

Dans ce chapitre, nous parlerons des ajouts que nous avons faits dans notre application, ainsi qu'un scénario sur la façon de l'utiliser. Nous parlerons également de la conception et de l'environnement matériel et logiciel pour construire notre application

2. Contribution

Pour la création d'un mécanisme de contrôle d'accès via la blockchain privé, on le fera dans deux étapes essentielles sont créer un NFT unique pour chaque Subject pour accéder au profil des patients et ensuite la demande d'accès aux données médicales qui est autorisé par le contrôle d'Access

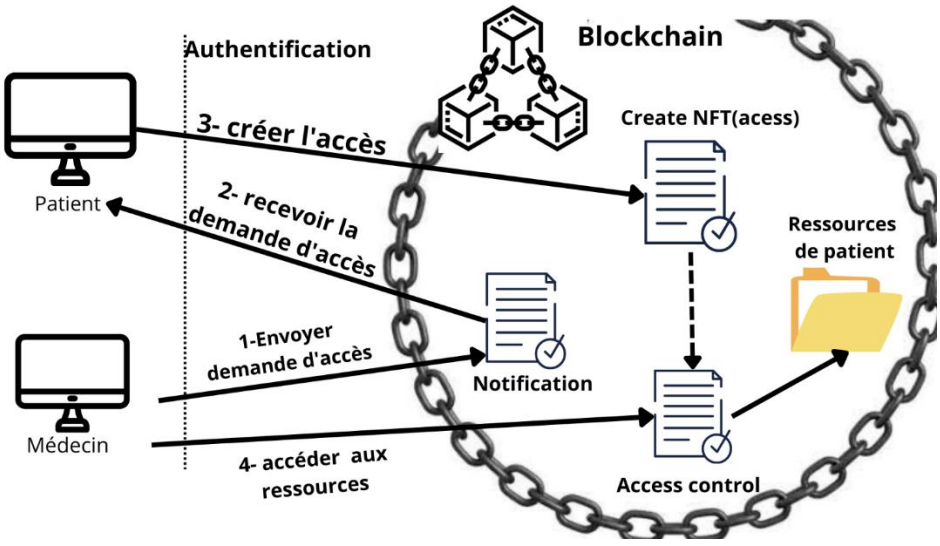
Nous avons choisi d'utiliser la blockchain par ce que c'est la technologie qui assure la gestion de contrôle d'access. Ainsi nous avons utilisé le NFT pour garantir la confidentialité et aussi pour assurer que sauf les utilisateurs qui ont le NFT peut accéder aux données et ressources de patient .

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

3. Scénario

Notre travail consiste à la création d'un NFT entre le patient et le médecin, ce NFT va être créé par le patient pour chaque médecin pour contrôler l'accès à ses données. Seul le patient qui peut gérer les politiques d'accès à ses ressources via le NFT. Ainsi que chaque ressource a sa propre contract intelligent

La figure montre le contrôle d'accès lorsqu'un médecin veut accéder à la ressource d'un patient avec un contrat déployé sur la Blockchain, vu que les comptes patient et médecin sont déjà créés dans notre blockchain dans différents nœuds.



Scénario pour accéder aux ressources du patient

4. Conception système

4.1 Les acteurs

- **Le patient :** c'est l'acteur qui va créer le contrat pour le sujet afin de permettre ce dernier d'accéder à leurs données.
- **Le médecin :** c'est l'acteur qui demande l'autorisation pour accéder aux données de patient

4.2 Les besoins fonctionnels et Besoins non fonctionnels :

4.2.1 Besoins fonctionnels

- Le patient crée un NFT pour le médecin
- Le patient definir les droits d'access aux appareils pour le médecin
- Le patient modifier les droits d'access aux appareils donner au médecin
- Le patient supprime les droits d'access aux appareils qui sont déjà donner au médecin
- Le médecin demande un NFT pour accéder au profil de patient
- Le médecin accède aux appareils disponibles

4.2.2 Besoins non-fonctionnels

Les besoins non fonctionnels sont importants car ils agissent de façon indirecte sur le résultat et sur le rendement de l'utilisateur, ce qui fait qu'ils ne doivent pas être négligés, pour cela il faut répondre aux exigences suivantes :

- **Fiabilité :** Bon fonctionnement de site sans erreurs.
- **Sécurité :**

  Les comptes des utilisateurs sont sécurisés par mot de passe.

  Seul le médecin qui a le NFT qui peut accéder aux données de patient

  Le patient c'est le seul qui gère les droits d'accès a ses ressources

  Le médecin est bloqué s'il essaye d'acceder a une ressource 3 fois avec 30 secondes entre chaque essaye.
- **Performance :** Le site répond à toutes les exigences des utilisateurs d'une manière optimale.
- **Rapidité :** Le déplacement entre les profils doit être facile et rapide.
- **Convivialité (ergonomie et bonne interface) :**

  Un design clair.

  Une bonne interface qui donne aux utilisateurs l'envie de l'utiliser.

  Des notions faciles à comprendre.

  Respect de l'ergonomie.
- **Portabilité (responsive) :**

  Le site est multiplateforme : il fonction sur tout système d'exploitation.

  Il fonction sur tout type de terminal (Pc/Smartphone/Tablette).

4.3 Diagrammes

4.3.1 Diagramme de cas d'utilisation

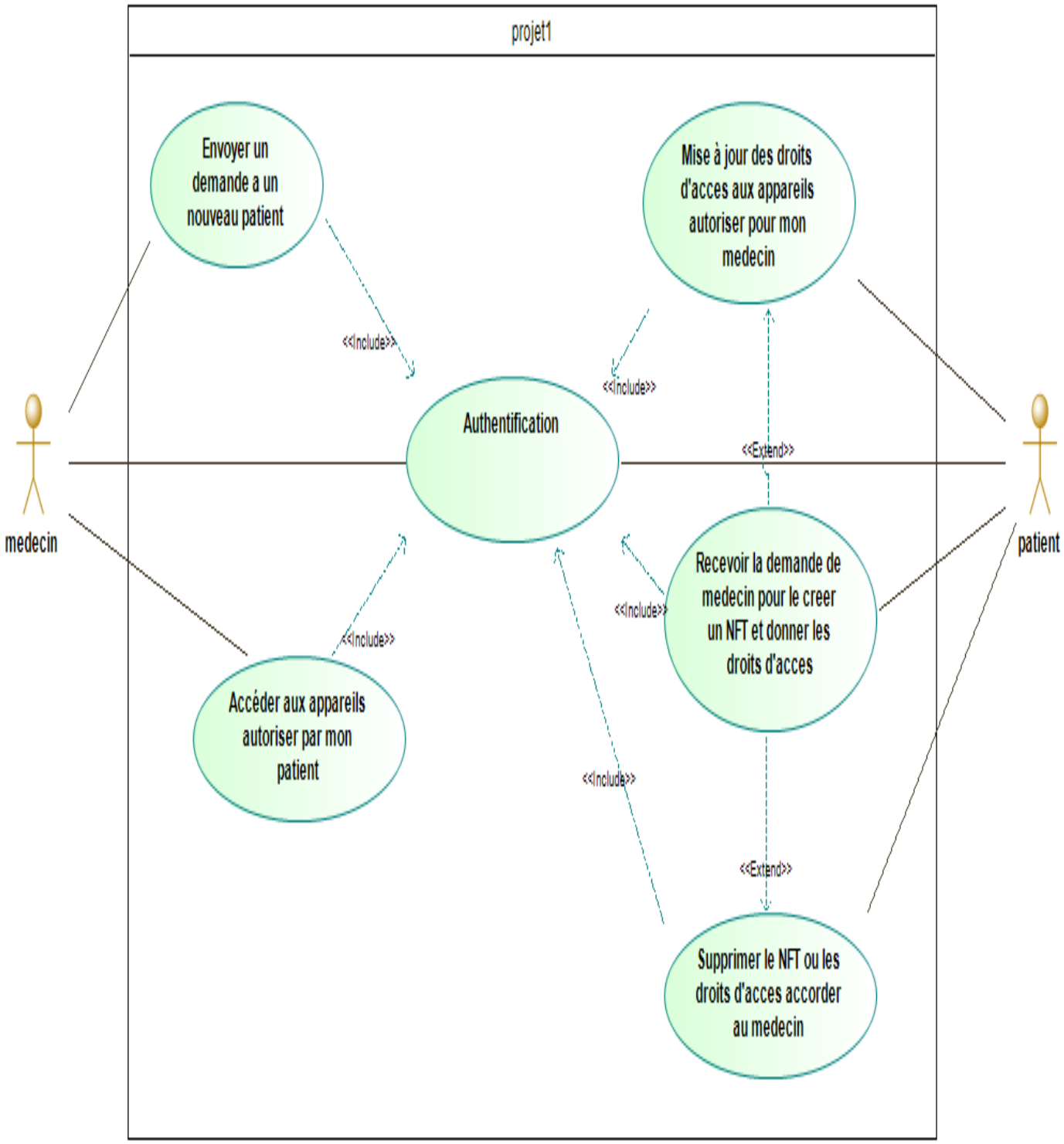


Diagramme de cas d'utilisation

4.3.2 Diagramme de séquence

- **Diagramme d'authentification**

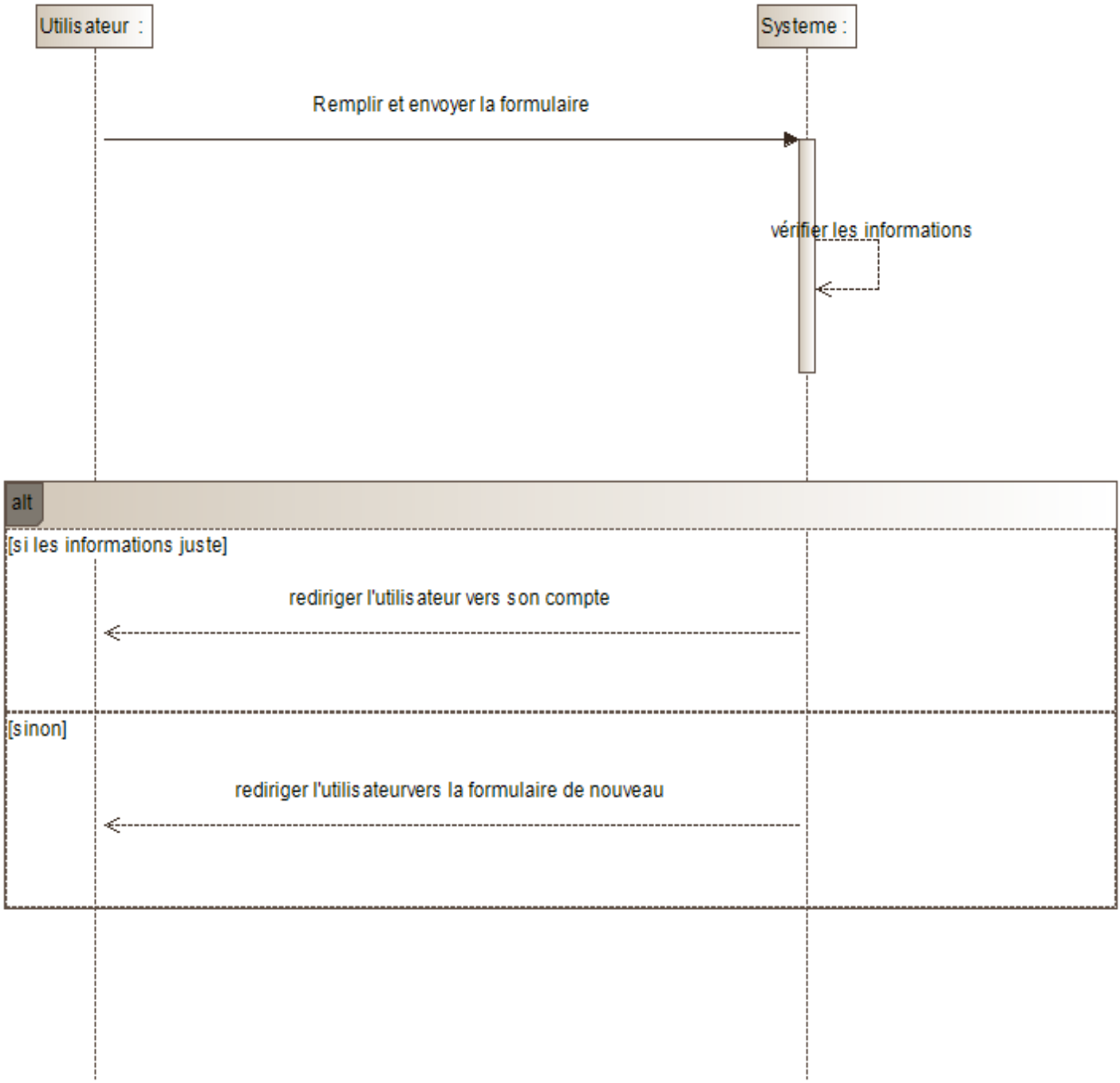


Diagramme de séquence d'authentification

- **médecin demander NFT**

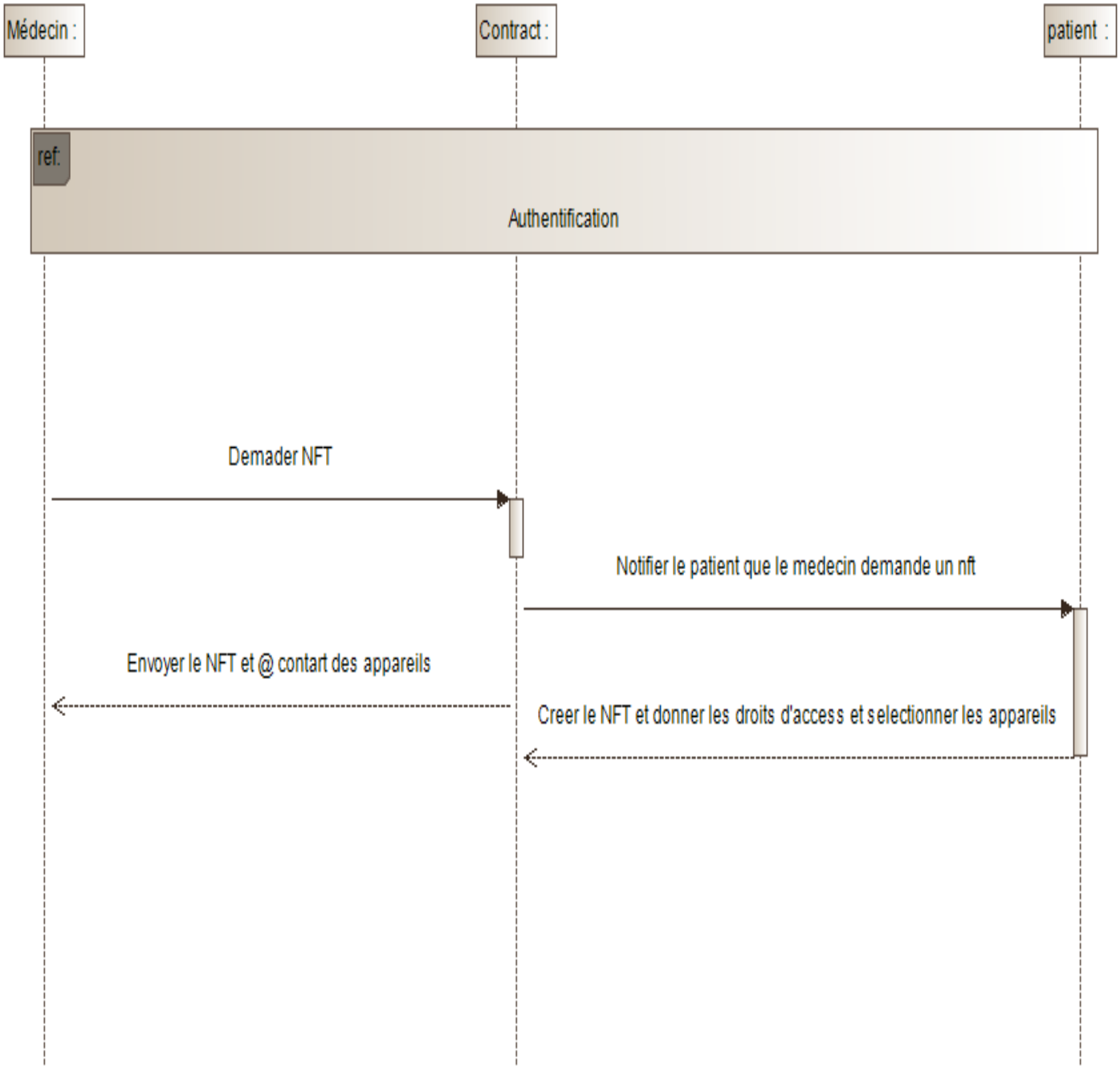


Diagramme de séquence médecin demande NFT

- **Access aux ressources de patient**

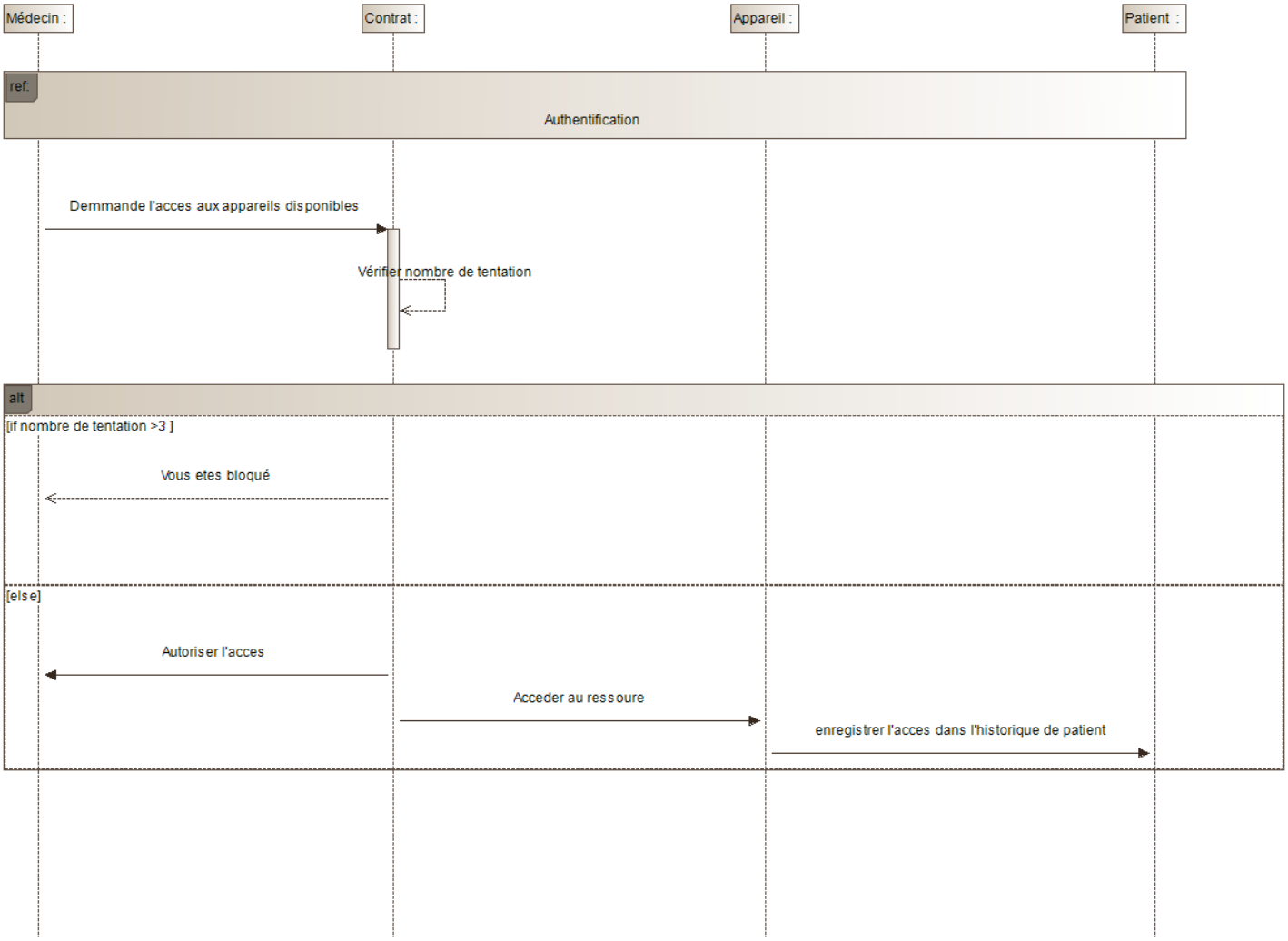


Diagramme de séquence Access aux ressources

- **Mise à jour de la liste des appareils donner à un médecin**

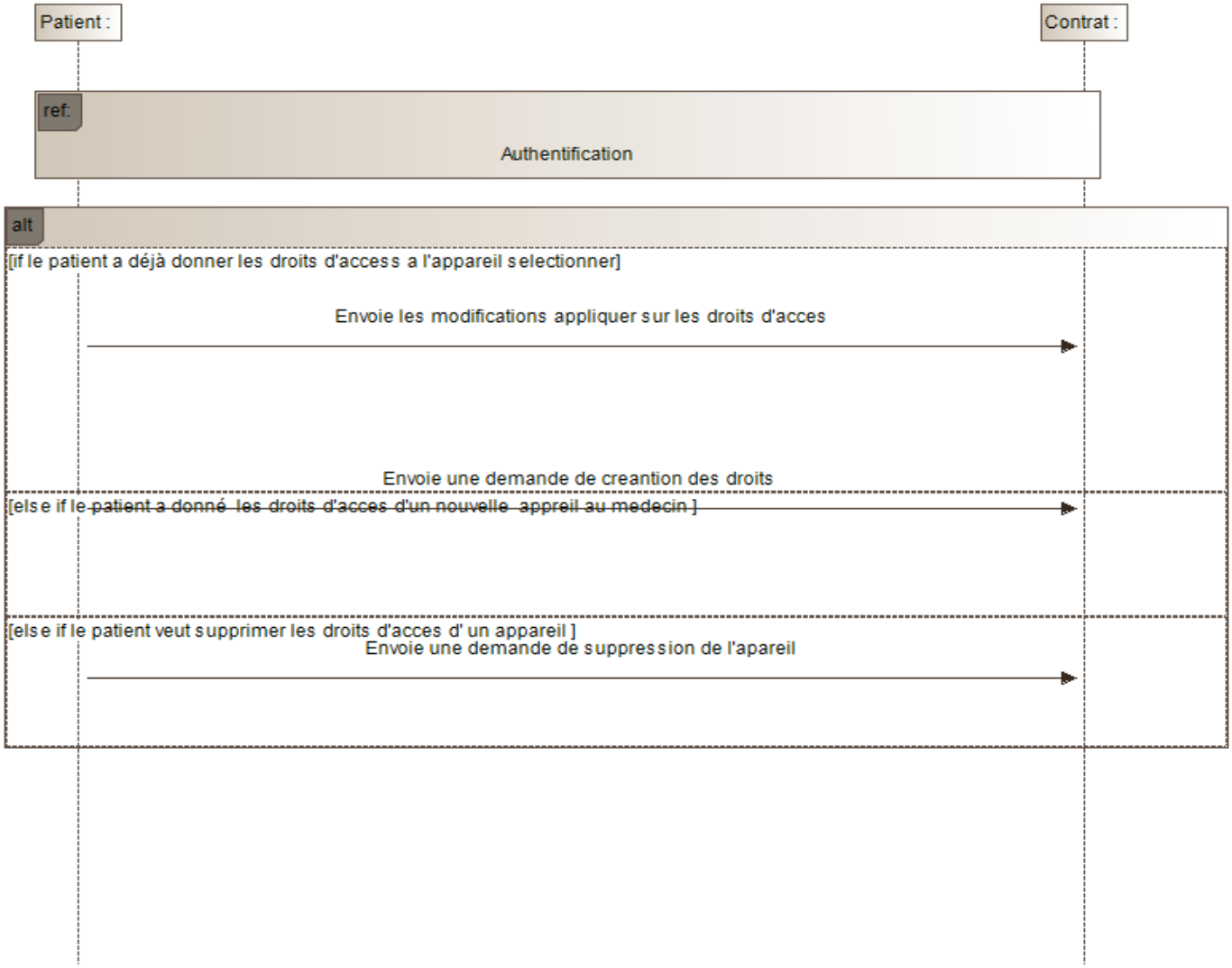


Diagramme de séquence Mise à jour des droits d'accès

- **Supprimer médecin**

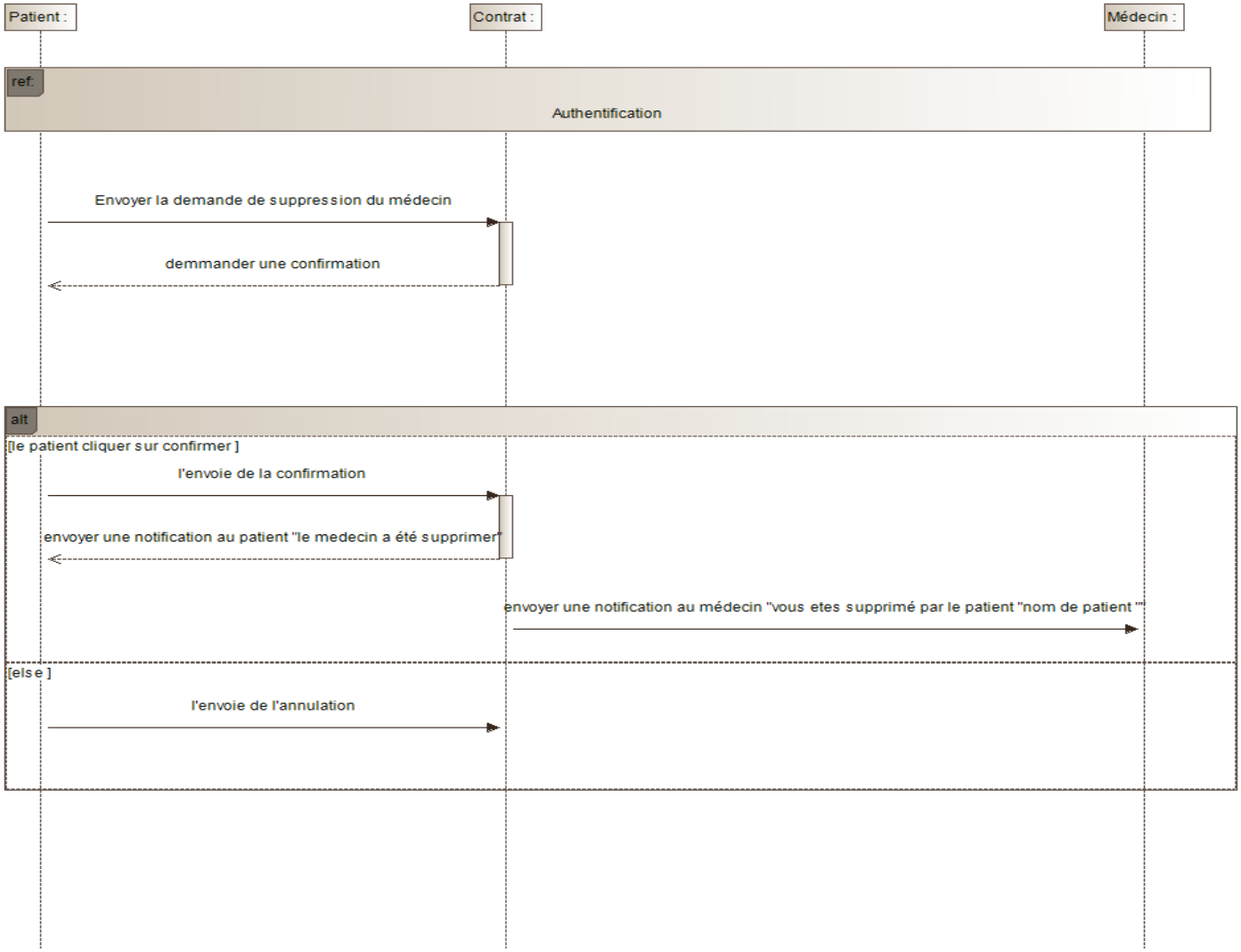


Diagramme de séquence Suppression de médecin

5. Implémentation

5.1 Outils utilisés

5.1.1 Front-end

Pour implémenter notre application, nous avons utilisé les langages web tels que HTML, CSS et JavaScript, web3.js, node.js, et pour rendre notre site responsif et qu'il puisse s'afficher à tous les types des équipements, nous avons utilisé aussi la bibliothèque Bootstrap.

- **HTML :** signifie « *HyperText Markup Language* » qu'on peut traduire par « langage de balises pour l'hypertexte ». Il est utilisé afin de créer et de représenter le contenu d'une page web et sa structure
- **CSS :** Les feuilles de styles (en anglais "*Cascading Style Sheets*", abrégé CSS) sont un langage qui permet de gérer la présentation d'une page Web.

- **JavaScript :** langage de script, oriente objet principalement connu comme langage de script des pages web.
- **Web3.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 :** 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
- **Go Ethereum :** Go-ethereum, également connu sous le nom de geth, est le client Ethereum le plus populaire et, comme il se trouve dans Go, il fournit tout ce dont nous aurons besoin pour lire et écrire dans la blockchain lors du développement d'applications.
- **Canva :** est une plate-forme de conception graphique qui permet aux utilisateurs de créer des graphiques, des présentations, des affiches, des documents et d'autres contenus visuels

5.1.2 Back-end :

Pour la création de notre contrat intelligent, nous avons besoin de :

- Une Blockchain de développement.
- Langage utiliser Solidity.
- Un IDE pour tester les contracts.

Blockchain de développement : Nous avons utilisé l'Ethereum est une plate-forme décentralisée qui exécute des contrats intelligents, des applications qui fonctionnent exactement comme programmé sans possibilité de temps d'arrêt. Etant donné que publier un contrat intelligent sur la Blockchain Ethereum coûte de l'argent, on va commencer par le publier sur une Blockchain gratuite (privée) où on peut tester directement notre contrat.

Solidity : Langage de programmation oriente objet, il a été développé par les principaux contributeurs de la plateforme Ethereum. Il est utilisé pour concevoir et mettre en œuvre des contrats intelligents au sein de la plate-forme virtuelle Ethereum et de plusieurs autres plates-formes blockchain.

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

5.2 Matériel utilisé

• acer Intel(R) Core (TM) i3 RAM 4Go CPU 250 ssd

• hp Intel (R) Core (TM) i3 RAM 4Go CPU 520 hdd

5.3 Implémentation d'algorithme

Dans cette étape on va étudier notre algorithme d'accès quand nous avons utilisé pour contrôler l'accès aux ressources

- **Algorithme de contrôle d'accès**

Algorithm 1 Access control

```
Input: addSubject, idNft, action, time
Output: result, penalty
Require: penalty ← 0,result ← true,s, SubjectMisconductList List
P ← Policy [idNft][action]
M ← List [idNft]
if M == addSubject then
    if M.timeOfUnblock ≤ time then
        M.timeOfUnblock ← 0
        if P.permission == 'allow' then
            s ← time - P.ToLR
            if s ≤ P.MinInt then
                P.NoFR ← P.NoFR ++
                if P.NoFR ≥ P.Limit then
                    Detect a Misconduct MSC
                    S ← M.length+1
                    penalty ← base*S
                    result ← false
                    M.timeofUnblock ← time+penalty
                    push MSC into the SubjectMisconductList
            else
                P.NoFR ← 0
else
    P.ToLR ← time
ReturnAccessResult(result, panalty)
```

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

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

- **Étape 1 (création des contrats intelligents) :** le propriétaire de la ressource crée un contrat intelligent et envoie une transaction pour le déployer sur la blockchain.
- **Étape 2 (Soumettre la demande) :** le sujet soumet une demande d'accès à un objet et demande à récupérer le contrat de contrôle d'accès.
- **Étape 3 (récupération du contrat) :** (si le sujet n'a pas de jeton d'accès) le Prop de l'objet redirige le sujet vers l'adresse du contrat qu'il a déployé, (et si le sujet a déjà un jeton on passe à l'étape 6)

- **Étape 4 (génération du jeton) :** le contrat intelligent génère le jeton d'accès (le NFT) avec les arguments spécifiés à la demande
- **Étape 5 :** le jeton émis est transmis au sujet.
- **Étape 6 (Les transactions sont enregistrées dans le nouveau bloc) :** Le sujet envoie une transaction qui contient les informations nécessaires au contrôle d'accès. La transaction va être miné et encapsulé dans un nouveau bloc, ensuite les méthodes de contrôle d'accès peuvent être exécutées.
- **Étape 7 (Nouvelle chaîne légale la plus longue) :** dès que le processus de contrôle d'accès est fini, le résultat est envoyé au sujet et l'objet.

Dans la première étape, le patient devra définir les politiques d'accès à sa ressource en remplissant le type de ressource à laquelle le sujet veut accéder comme un enregistrement, ou un champ, l'action que le sujet peut effectuer sur son objet comme lire la donnée ou la modifier, et enfin la permission d'accès qui peut être soit autoriser ou refuser.

Le tableau représente un exemple d'une liste de politique d'accès remplis par un propriétaire d'objet.

Type de ressource	**Action**	**Permission**
Tensiomètre	Lire	Autoriser
Glucomètre	Lire	Refuser
Electrocardioscope	Lire	Autoriser

On prend en considération que dans notre exemple n'a 3 actions :

Lire : sauf la lecture des données

Ecrire : possibilité de lecture et écriture

Exécution : possibilité de lecture, écriture et exécution des données

- **La liste des politiques d'accès**

Notre contrat de contrôle d'accès passe par 3 étapes, la vérification d'enregistrement du sujet, la vérification des droits d'accès, et la vérification de la mauvaise conduite.

Pour aider à caractériser la mauvaise conduite, nous avons ajouté les champs suivants aux lignes (c'est-à-dire, les politiques)

MinInt : le temps minimum autorisé entre 3 demandes successives.

NoFR : Nombre de demandes fréquentes.

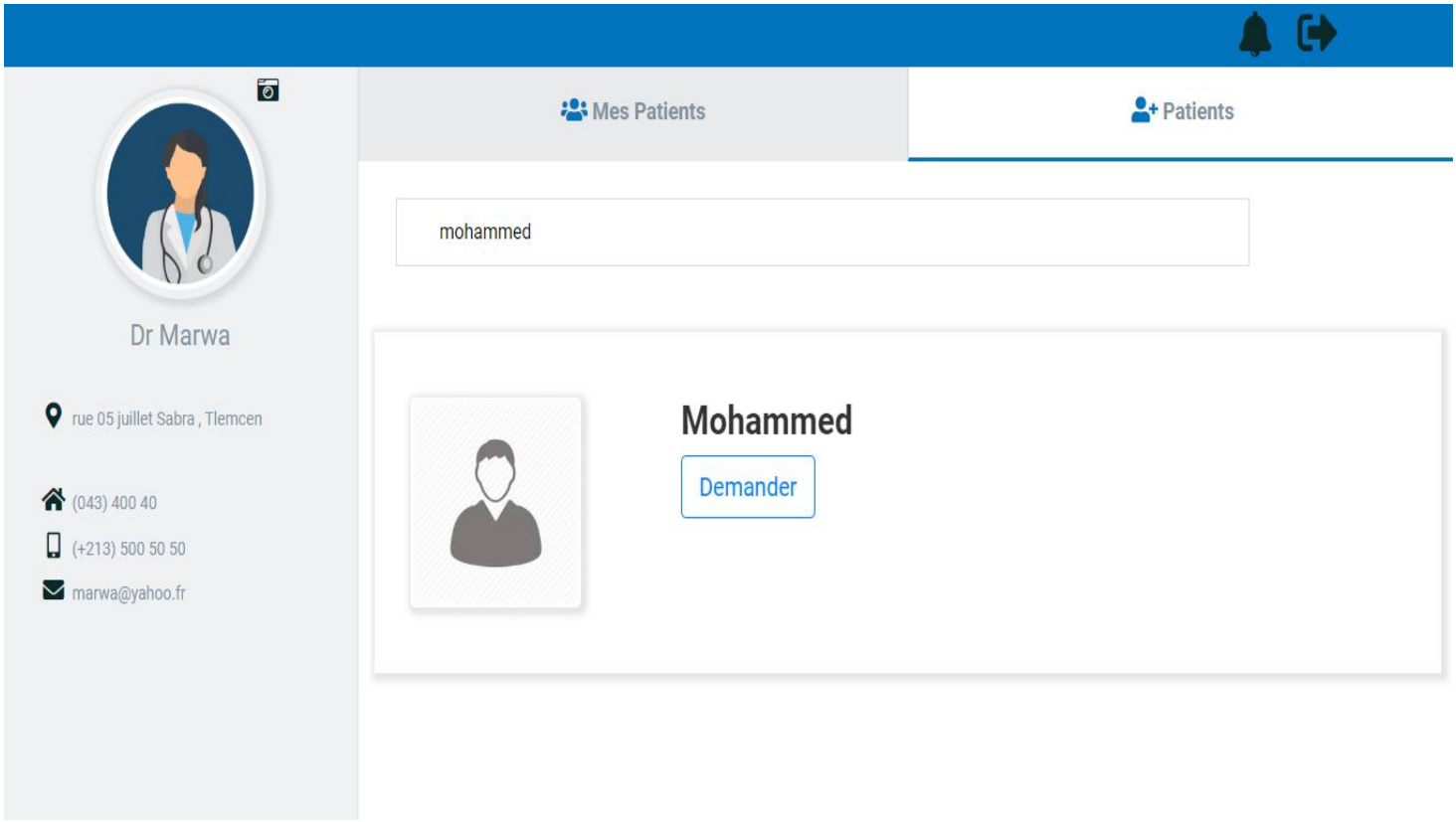
Limit : Limite de demandes fréquentes.

- **La structure de NFT**

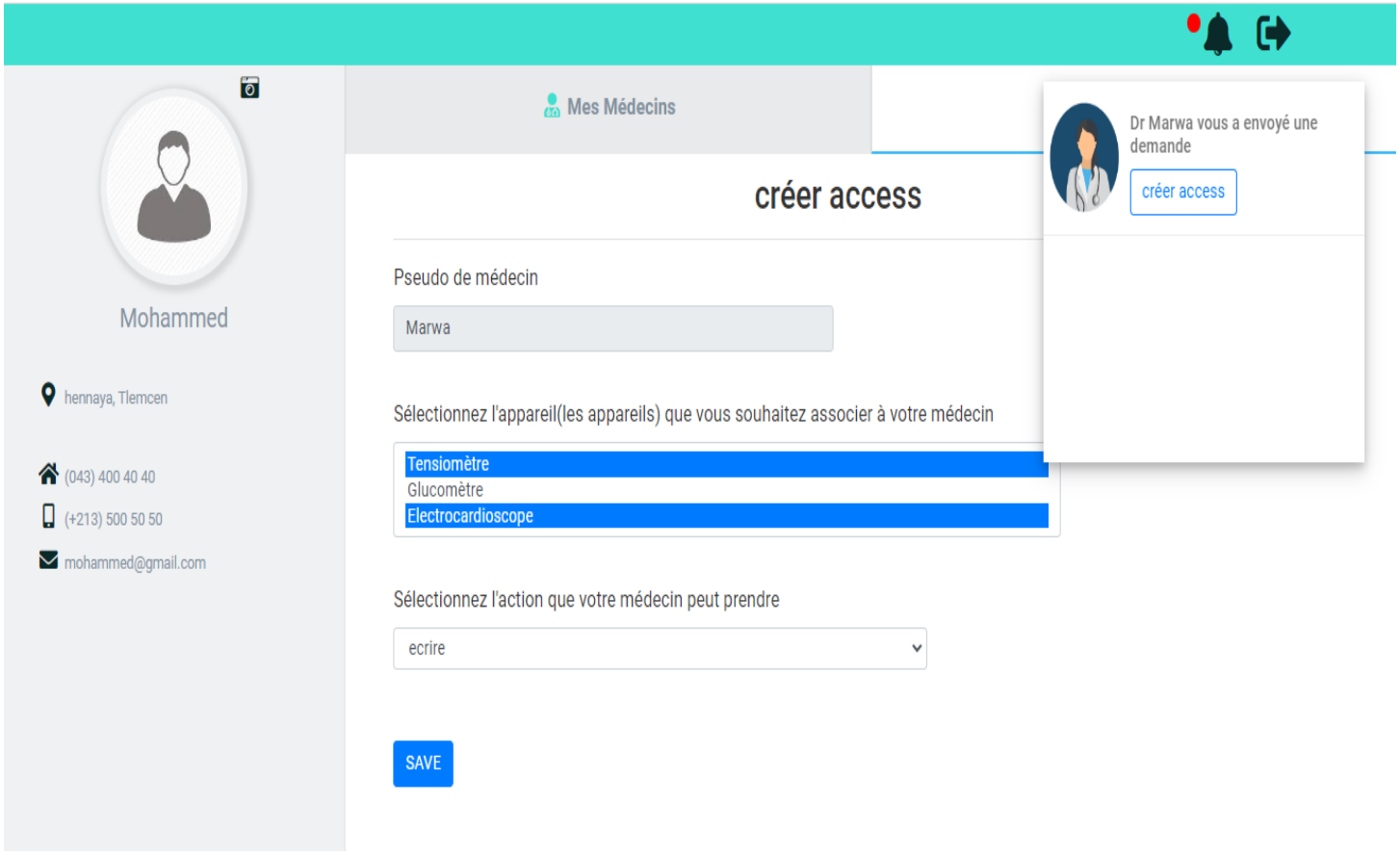
TokenId (20 bytes)
AddSubject (20 bytes)
Permission (20 bytes)
OwnerId (20 bytes)

5.4 Présentation de l'application

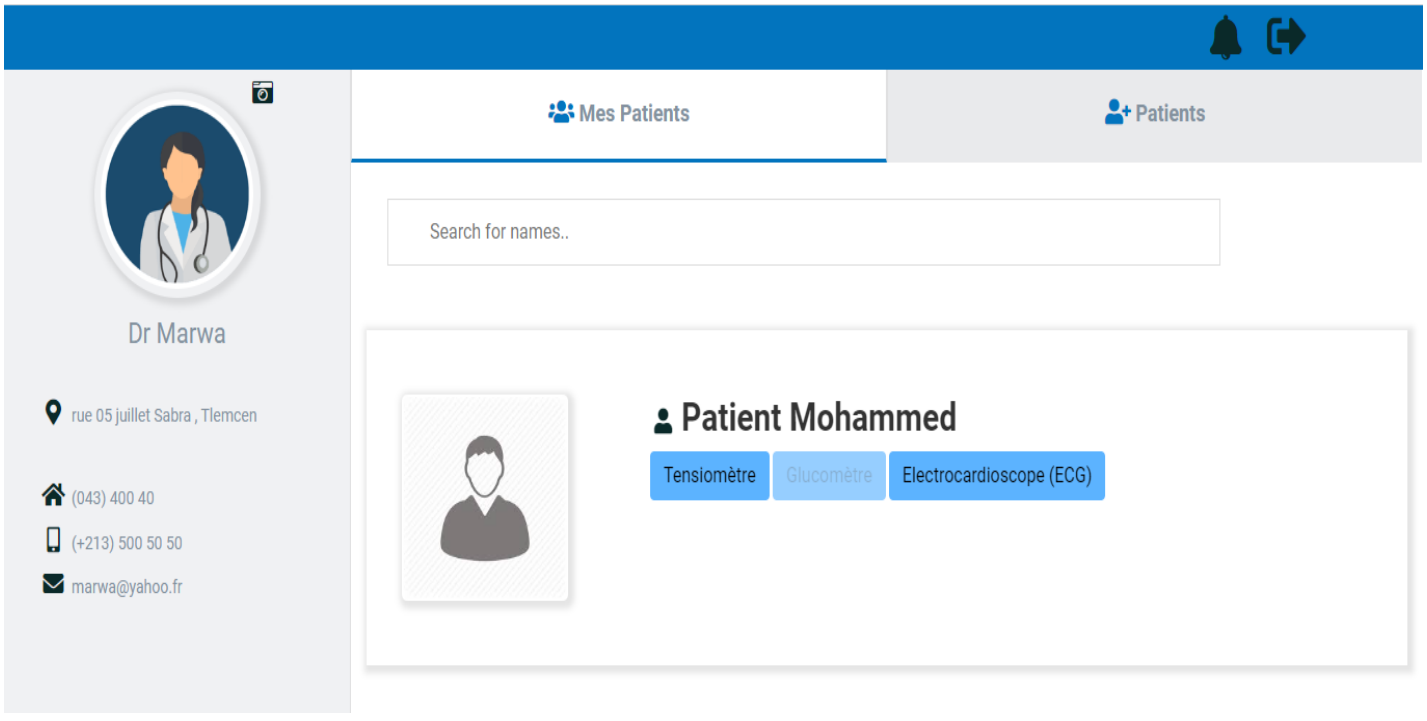
La figure montre que le médecin peut chercher d'un patient et l'envoyer une demande d'accès



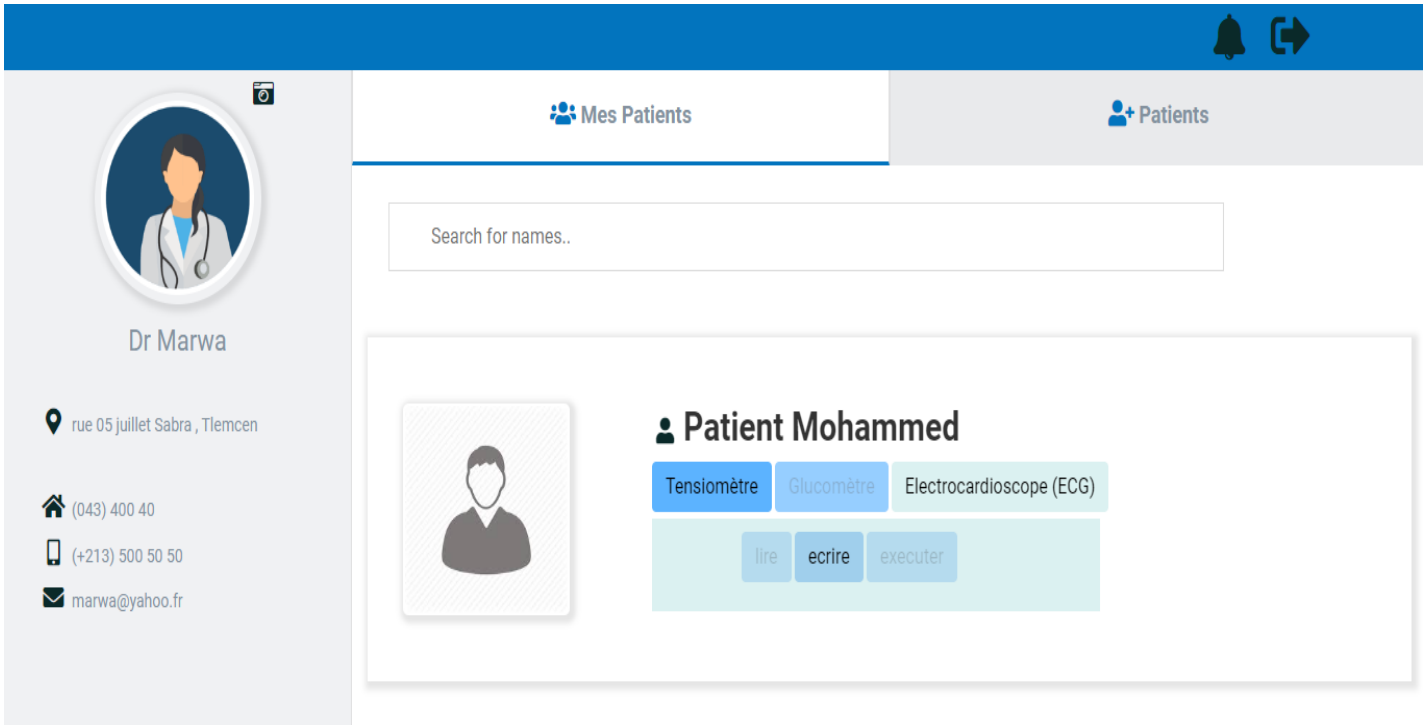
La figure montre comment le patient donne le NFT et les droits d'access au médecin après la réception de la notification de la demande



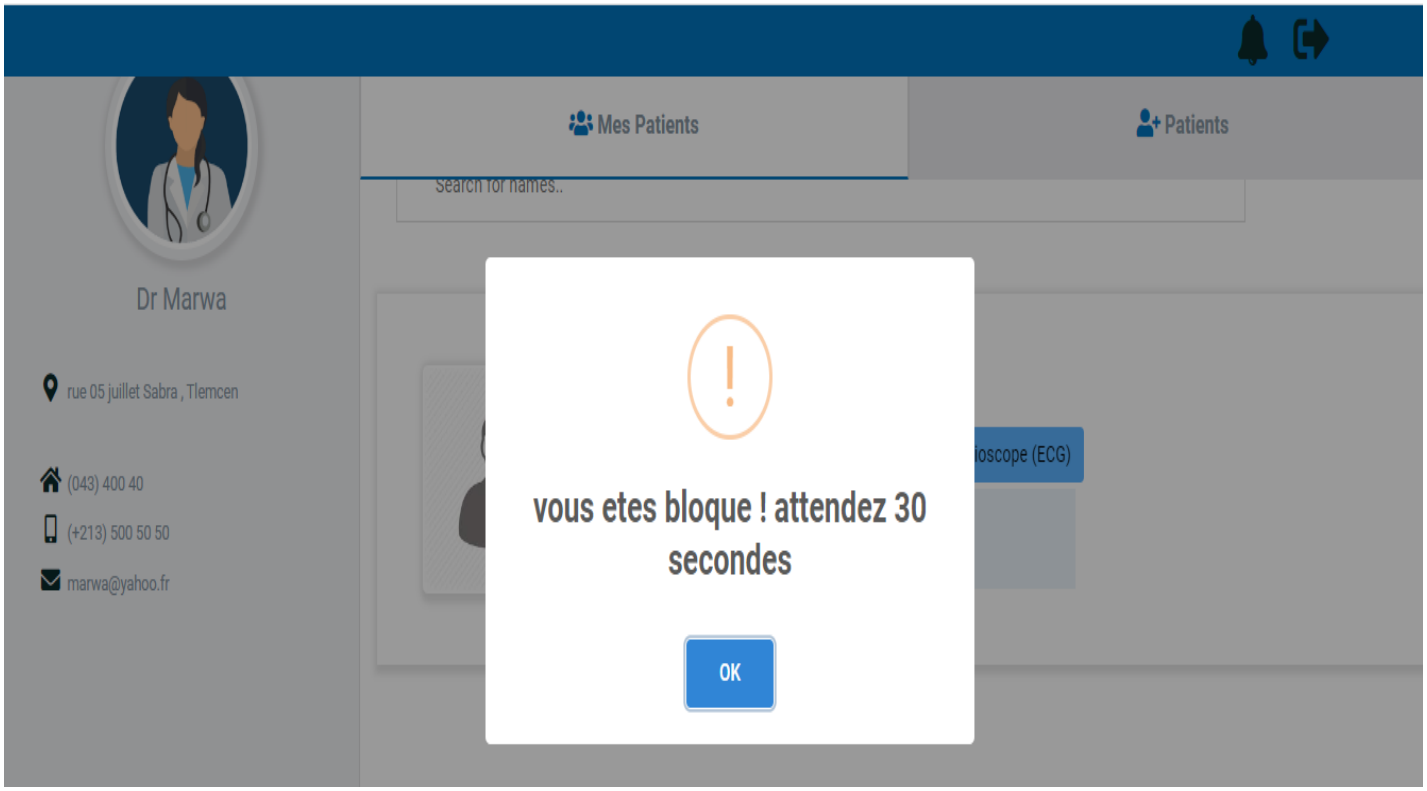
La figure montre que le patient Mohammed devient dans la liste des patients de Dr Marwa



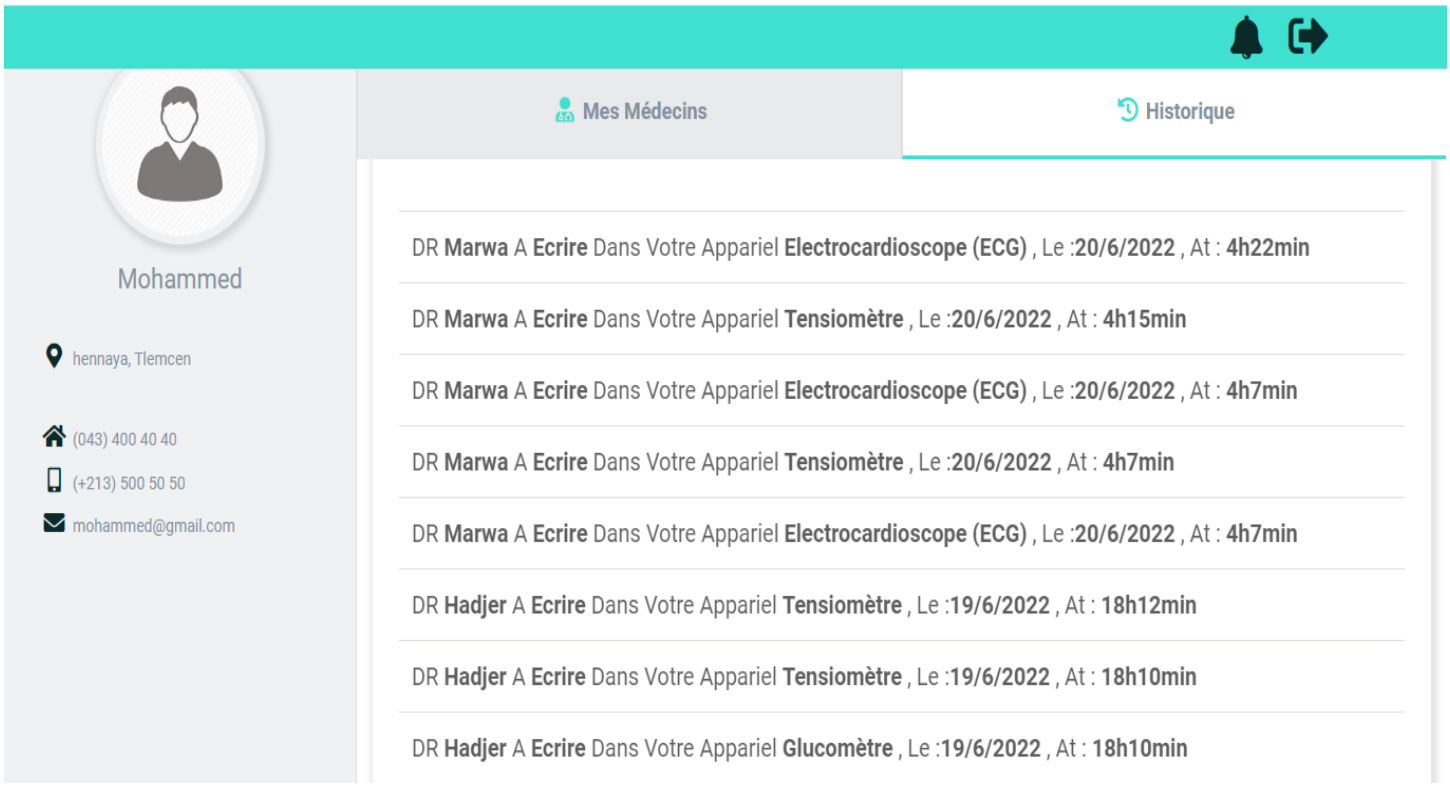
La figure montre les droits donnés au médecin par le patient



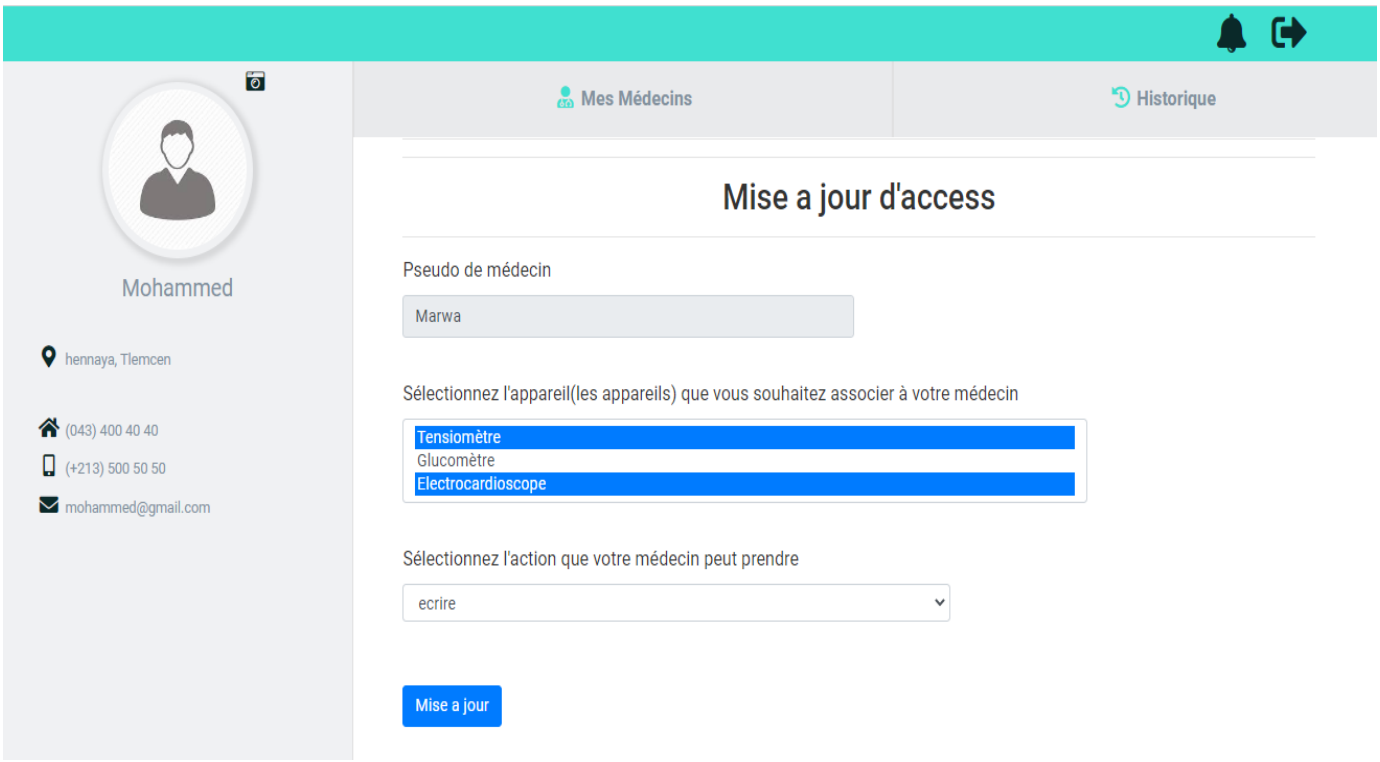
La figure montre une mauvaise conduite de médecin (3 essaye d'access dans une durée moins de 30 secondes)

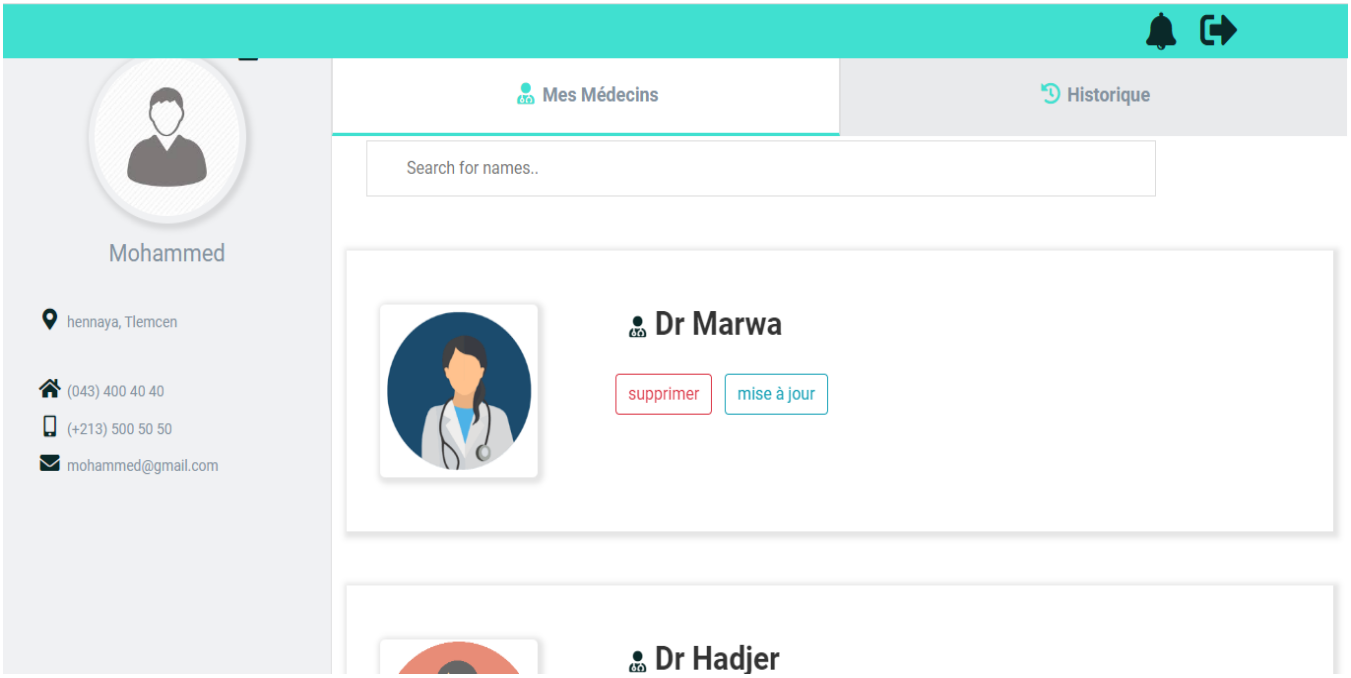


La figure montre l'historique de médecin dans le profil du patient



La figure montre qu'un patient peut mettre à jour les droits d'access données ou supprimer un médecin





5.5 Résultats

1. Le médecin peut accéder seulement aux données des patients qui a son NFT
2. Le médecin peut accéder seulement aux ressources qui a son droit d'accès
3. Le patient c'est lui qui contrôle les droits d'access à ses ressources
4. Chaque médecin a un contract
5. Un système sécurisé et décentralisé pour stocker les données

Cout de transaction pour chaque fonction dans notre contrat :

La fonction	Le cout de transaction (Gas)
Create NFT(Access)	**257770**
Access Control	**52371**
Update NFT(Access)	**26723**
Delete NFT (Access)	**104856**
Set Notification	**44641**
Delete Notification	**14767**
Historique	**161000**

6.Conclusion

Dans ce chapitre, nous avons décrit notre solution pour sécuriser aux mieux notre application e-santé. L'approche utilisée repose sur l'utilisation de la technologie blockchain privée qui garantit l'immutabilité et la traçabilité, un NFT qui assure que l'accès aux données est possible seulement pour les gens qui ont la clé NFT, et avec l'algorithme de contrôle d'access qui assure l'accès aux données, la confidentialité et l'intégrité des données.

Conclusion générale

- **Conclusion**

La blockchain a dépassé largement son application classique de monnaie électronique sans autorité centrale. Cette technologie a apporté des nouveaux concepts qui assure l'immutabilité et renforce la sécurité. Ces caractéristiques rendent la technologie de blockchain appropriée pour plusieurs domaines, tels que : les systèmes de E-santé

Dans ce mémoire, nous avons exploré la blockchain et proposé des solutions basées sur cette technologie. Nos propositions concernent une application pour le contrôle d'accès aux ressources de patient.

Dans ce contexte, notre travail consiste à étudier la Blockchain, le contrat intelligent et la technologie des NFT ainsi que la plateforme Ethereum pour la réalisation d'un système de contrôle d'accès pour protéger les informations médicales de patient. Notre application est une application décentralisée où les données sont partagées entre tous les nœuds et protégés avec un smart contrat dans un réseau présenté en P2P. Nous avons déployé un smart contrat dans la plateforme ethereum qui met les données des patients en sécurité, et établir les règles pour accéder à une ressource à savoir l'identité de l'acteur dans des conditions prédéfinies par le patient (par exemple médecin)

Ce projet nous a été très bénéfique, car il nous a permis d'enrichir nos connaissances concernant la blockchain sur les deux plans : théorique et pratique. Il nous a aussi permis de découvrir et d'acquérir de nouvelles connaissances en matière de programmation et de d´développement dans le domaine des applications décentralisées.

La technologie blockchain est encore très complexe à appréhender et le d´développement d'un système décentralisé nécessite énormément du temps, de ressources, de recherches et aussi de grands efforts de programmation.

Bibliographies

[1] M. Han and H. Zhang, "Business intelligence architecture based on internet of things " Journal of Theoretical & Applied Information Technology, vol. 50, no. 1, pp. 90-95, 2013.

[2] P.J. Benghozi, S. Bureau, F. Massit-Folléa, C. Waroquiers, and S. Davidson, L'internet des objets : quels enjeux pour l'Europe, Éd. De la Maison des sciences de l'homme éd., 2009, 66 p.

[3] https://www.geeksforgeeks.org/characteristics-of-internet-of-things/

[4] Etude de cas : J. Simard, La ville intelligente comme vecteur pour le développement durable : le cas de la ville de Montréal, 2015.

[5] Citintelly, « Citintelly - Smart Street Lighting System | Motion sensor street lighting, » [En ligne]. Available : https://www.citintelly.com/intelligent-street-lighting-products/motionsensor-street-lighting/. [Accès le 27 févr. 2022].

[6] smarthome, « August AUG-SL04-M01-S04 Smart Lock, Silver, » [En ligne]. Available : https://www.smarthome.com/august-aug-sl04-m01-s04-smart-lock-silver.html. [Accès le 27 févr. 2022].

[7] Cooking Hacks, «Barcelona Park Smart Irrigation System project with Waspmote Agriculture Sensors Kit, » [En ligne]. Available : https://www.cookinghacks.com/blog/barcelona-park-smart-irrigation-system-project-with-waspmoteagriculture-sensors-kit/. [Accès le 27 févr. 2022].

[8] Y. CHALLAL, “Sécurité de l’Internet des Objets : vers une approche cognitive et systémique”, HDR, Juin 2012, UTC.

[9] https://www.openscience.fr/IMG/pdf/iste_ido18v2n1_1.pdf

[10] SETHI, Pallavi et SARANGI, Smruti R. Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017, vol. 2017

[11] ATOUMI.M Y, BENSADI. S, « Approche évolutionnaire pour la composition de services sensible à la QoS dans l’Internet des Objets à large échelle », Mémoire de master, Université de Bejaia, Algérie, 2018.

[12] Jigna J. Hathaliya, Sudeep Tanwar, An exhaustive survey on security and privacy issues in Healthcare 4.0, Computer Communications, Volume 153,2020, Pages 311-335, ISSN 0140- 3664.

[13] K. Hayrinen, K. Saranto, P. Nykanen, Definition, structure, content, use and impacts of electronic health records: a review of the research literature Int J Med Inform, 77 (5) (2008), pp. 291-304.

[14] Sánchez JL, Savin S, Vasileva V. Key success factors in implementing electronic medical records in University Hospital of Rennes: Rennes: ENSP; 2005. p. 1–59

[15] F. Lau, M. Price, J. Boyd, C. Partridge, H. Bell, R. Raworth Impact of electronic medical record on physician practice in office settings: a systematic review BMC Med Inform Decis Mak, 12 (1) (2012), pp. 1-10

[16] R.H. Miller, I. Sim Physicians' use of electronic medical records: barriers and solutions Health Aff, 23 (2) (2004), pp. 116-126

[17] A. Boonstra, M. Broekhuis Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions BMC health Serv Res, 10 (1) (2010), pp. 231-247

[18] D. Blumenthal, M. Tavenner The "meaningful use" regulation for electronic health records New Engl J Med, 363 (6) (2010), pp. 501-504

[19] Hsiao CJ, Hing E. Use and characteristics of electronic health record systems among office-based physician practices: United States, 2001–2013. In: Services USDoHaH, editor. Hyattsville, Maryland: National Center for Health Statistics; 2014.

[20] C. Lin, E.W. Karlson, D. Dligach, M.P. Ramirez, T.A. Miller, H. Mo, et al. Automatic identification of methotrexate-induced liver toxicity in patients with rheumatoid arthritis from the electronic medical record J Am Med Inform Assoc, 22 (e1) (2014), pp. 151-161

[21] K.M. Krysko, N.M. Ivers, J. Young, P. O'Connor, K. Tu Identifying individuals with multiple sclerosis in an electronic medical record Mult Scler J, 21 (2) (2015), pp. 217-224

[22] Tsipi Heart, Ofir Ben-Assuli, Itamar Shabtai, A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy, Health Policy and Technology, Volume 6, Issue 1, 2017, Pages 20-25, ISSN 2211-8837, https://doi.org/10.1016/j.hlpt.2016.08.002.

[23] E.A. Coleman, J.D. Smith, J.C. Frank, S.J. Min, C. Parry, A.M. Kramer Preparing patients and caregivers to participate in care delivered across settings: the care transitions intervention J Am Geriatr Soc, 52 (11) (2004), pp. 1817-1825

[24] P.C. Tang, J.S. Ash, D.W. Bates, J.M. Overhage, D.Z. Sands Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption J Am Med Inform Assoc, 13 (2) (2006), pp. 121-126

[25] T. McKeown the role of medicine. Dream, mirage or nemesis? Basil Blackwell Publisher Ltd., Oxford, England (1979)

[26] P.E. Kummervold, C.E. Chronaki, B. Lausen, H.U. Prokosch, J. Rasmussen, S. Santana, et al. eHealth trends in Europe 2005-2007: a population-based survey J Med Internet Res, 10 (2008), p. 4

[27] N. Archer, U. Fevrier-Thomas, C. Lokker, K.A. McKibbon, S.E. Straus Personal health records: a scoping review J Am Med Inform Assoc, 18 (4) (2011), pp. 515-522

[28] C.L. Goldzweig, G. Orshansky, N.M. Paige, A.A. Towfigh, D.A. Haggstrom, I. MiakeLye, et al. electronic patient portals: evidence on health outcomes, satisfaction, efficiency, and attitudesa systematic review Ann Intern Med, 159 (10) (2013), pp. 677-687

[29] S.J. Czaja, C. Zarcadoolas, W.L. Vaughon, C.C. Lee, M.L. Rockoff, J. Levy The usability of electronic personal health record systems for an underserved adult population Hum Factors: J Hum Factors Ergon Soc, 57 (3) (2014), pp. 491-506.

[30] https://www.blackberry.com/fr/fr/solutions/iot-internet-of-things/iot-healthcare

[31] (PDF) Contribution de la Blockchain au management des données de santé - Thèse d' Exercice Cedric Strub - final (researchgate.net)

[32] bitcoin.pdf

[33] JEAN-PAUL DELAHAYE, mars 2015, POUR LA SCIENCE N° 449

[34] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[35] LELOUP, Laurent. Blockchain : La révolution de la confiance. Editions Eyrolles, 2017.

[36] PIGNEL, Marion et STOKKINK, Denis. LA TECHNOLOGIE BLOCKCHAIN Une opportunité pour l'économie sociale ?
https://www.pourlasolidarite.eu/fr/publication/la-technologie-blockchain-une-opportunite-pour-leconomie-sociale

[37] https://www.mdpi.com/388844

[38] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[39] Samanta, Sidharth & Mohanta, Bhabendu & Patnaik, Deepti & Patnaik, Srikanta. (2021). Introduction to Blockchain Evolution, Architecture and Application with Use Cases. 10.1007/978-981-33-6470-7_1.

[40] Mukherjee, P. and C. Pradhan, Blockchain 1.0 to Blockchain4.0—The Evolutionary Transformation of Blockchain Technology, in Blockchain Technology: Applications and Challenges, S.K. Panda, et al., Editors. 2021, Springer International Publishing: Cham. p. 29-49.

[41] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and HuaiminWang. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (Bigdata congress), pages 557–564. IEEE, 2017.

[42] https://www.codleo.com/blockchain-development-service

[43] https://www.vice.com/en/article/d3zn9a/ethereum-mining-transaction-electricity-consumption-bitcoin

[44] https://blockchainpartner.fr/sante-industrie-pharmaceutique-et-blockchain-notre-etude/

[45] https://siecledigital.fr/2017/03/20/blockchain-pas-si-simple-pour-les-grands-groupes/

[46] https://journalducoin.com/lexique/smart-contract/

[47]https://www.futura-sciences.com/tech/definitions/tech-non-fungible-token-19205/

[48]https://www.cointribune.com/analyses/institutions-entreprises/blockchain-et-nft-rightshash-loutil-qui-protege-le-consentement-des-patients/

[49] A. Haddad, Modélisation et vérification de politique de sécurité, Formation Européenne de 3ème Cycle en Systèmes d'Information : MATIS Université de Joseph Fourier, Genève, 2005.

[50] https://liris.cnrs.fr/Documents/Liris-3523.pdf

[51] (PDF) Modèle de sécurité pour le secteur de la santé (researchgate.net)

[52]Craig Wright, in The IT Regulatory and Standards Compliance Handbook, 2008

[53]Chirag Langaliya , Rajanikanth Aluvalu , Enhancing Cloud Security through Access Control Models: A Survey ,International Journal of Computer Applications (0975 – 8887)Volume 112 – No. 7, February 2015

[54]Samarati P., de Vimercati S.C. (2001) Access Control: Policies, Models, and Mechanisms. In: Focardi R., Gorrieri R. (eds) Foundations of Security Analysis and Design. FOSAD 2000. Lecture Notes in Computer Science, vol 2171. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45608-2_3

[55]Ferraiolo, Sandhu, Gravila, Kuhn and Chandramouli, "Proposed NIST Standard for Role- Based Access Control," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 222- 274, 2001.

[56]Alban Gabillon. Contrôler les accès aux données numériques. La Revue de l'Electricité et de l'Electronique, Société de l'Électricité, de l'Électronique et des Technologies de l'Information et de la Communication, 2013, 12 p. ffhal-02108021f

[57]RBAC vs. ABAC: What's the Difference? https://www.dnsstuff.com/rbac-vs-abac-access- control consulter le 28/06/2022

[58] ABAKAR Mahamat Ahmat, « Étude et mise en œuvre d'une architecture pour L'authentification et la gestion de documents numériques certifiés », université Jean Monnet de Saint-Étienne, 22 novembre 2012.

[59] Blockchain et santé : présentation et cas d'usage • BitConseil

[60] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[61] https://medium.com/@josiahoyahaya/using-blockchain-to-build-a-decentralized-health-record-system-dhrs-bc07ec309ee3

[62] https://www.beckershospitalreview.com/quality/top-5-inefficiencies-in-hospital-operations.html

[63]https://medium.com/datadriveninvestor/digital-health-records-challenges-and-opportunities-51fc3256bc50

[64] https://www.pwc.com/gx/en/industries/pharmaceuticals-life-sciences/publications/pharma-2020/pharma-2020-supplying-the-future.html

[65] https://medium.com/@sukantkhurana/will-healthcare-supply-chain-to-be-more-transparent-with-this-blockchain-technology-4d71b2921ed

Résumé

La technologie Blockchain a le potentiel de transformer le secteur de la santé, en plaçant le patient au centre de système de la santé et en augmentant la sécurité, la confidentialité et l'interopérabilité des données. Cette technologie pourrait fournir un nouveau modèle pour les échanges d'informations sur la santé en rendant les dossiers médicaux électroniques plus efficaces et sécurisés. Bien qu'il ne s'agisse pas d'une panacée, ce nouveau domaine en évolution rapide offre un terrain fertile pour l'expérimentation, l'investissement et les tests. Étant donné que les antécédents médicaux d'un patient sont la première pierre angulaire d'une bonne médecine, la recherche dans ce domaine est relativement nouvelle mais en croissance rapide. Ainsi, les chercheurs et praticiens en informatique de la santé ont toujours du mal à suivre le rythme des progrès de la recherche dans ce domaine... Dans ce modeste travail nous appliquerons le concept de la technologie blockchain et le NFT pour réaliser un système de contrôle d'accès aux données de patient en utilisant les contrats intelligents qui permet aux patients d'être les véritables propriétaires de leurs données sensibles et de les partager en toute sécurité.
Mots clés : blockchain, NFT, contrôle d’accès, contrat intelligent.

Abstract

Blockchain technology has the potential to transform the healthcare industry, placing the patient at the center of the healthcare system and increasing data security, privacy and interoperability. This technology could provide a new model for the exchange of health information by making electronic medical records more efficient and secure. While not a panacea, this new and rapidly evolving field provides fertile ground for experimentation, investment and testing. Since a patient's medical history is the first cornerstone of good medicine, research in this area is relatively new but growing rapidly. Thus, health informatics researchers and practitioners continue to struggle to keep pace with advances in research in this domain. In this modest work we will apply the concept of blockchain technology and NFT to realize a patient data access control system using smart contracts that allows patients to be the true owners of their sensitive data and to share it securely.
Keywords: blockchain, NFT, access control, smart contract

ملخص

تتمتع تقنية blockchain بالقدرة على تحويل صناعة الرعاية الصحية، ووضع المريض في مركز نظام الرعاية الصحية وزيادة أمن البيانات والخصوصية وقابلية التشغيل البيني. يمكن أن توفر هذه التكنولوجيا نموذجًا جديدًا لتبادل المعلومات الصحية من خلال جعل السجلات الطبية الإلكترونية أكثر كفاءة وأمانًا. على الرغم من أنه ليس حلاً سحريًا، إلا أن هذا المجال الجديد سريع التطور يوفر أرضًا خصبة للتجريب والاستثمار والاختبار. نظرًا لأن التاريخ الطبي للمريض هو حجر الزاوية الأول للطب الجيد، فإن البحث في هذا المجال جديد نسبيًا ولكنه ينمو بسرعة. وبالتالي، لا يزال الباحثون والممارسون في مجال المعلوماتية الصحية يكافحون لمواكبة تقدم البحث في هذا المجال ... في هذا العمل المتواضع، سنطبق مفهوم تقنية blockchain و NFTلتحقيق نظام للتحكم في الوصول إلى بيانات المريض باستخدام عقود ذكية تسمح للمرضى بأن يكونوا المالكين الحقيقيين لبياناتهم الحساسة ومشاركتها.
الكلمات الرئيسية: blockchain,NFT، التحكم في الوصول، العقد الذكي