REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre : ……

Mémoire

présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : **Intelligence artificielle**

Conception et réalisation d'un modèle de Blockchain intelligent

Par :

MANCER M'HAMED

Soutenu le , devant le jury composé de :

		Président
KAZAR Okba	Professeur	Rapporteur
		Examinateur

الملخص

سلسلة الكتل هي قاعدة بيانات مشتركة تجعل من الممكن إنشاء ثقة بين الأفراد دون أطراف ثالثة. البنية هنا لامركزية، بمعنى آخر يتم توزيع البيانات بين المستخدمين، وبالتالي لا يمكن محو المعلومات أبدًا. و من بين القطاعات الواعدة لهذه التكنولوجيا، نحدد القطاع الصحي، لأنه حساس للغاية فهو يتطلب مشاركة معلومات المرضى وبياناتهم الصحية. لذلك فان الهدف من هذا المشروع هو اقتراح نهج سلسلة الكتل في المجال الطبي، والذي يهدف إلى إدارة البيانات الصحية باستخدام السجلات الطبية الإلكترونية.

الكلمات المفتاحية : سلسلة الكتل، الثقة ، الصحة ، سجل طبي مشترك آمن.

Abstract

Blockchain is a shared database that makes it possible to create trust between individuals without a third parties. The architecture here is decentralized, in other words data is distributed among users, and therefore information can never be erased. Therefore, among the promising sectors of this technology (we mean Blockchain), we specify the health sector, because it is really very sensitive since it recommends sharing patient information and their health data. In this context, the objective of this project is to propose a Blockchain approach in the medical field, which aims to manage health data using electronic medical records.

key-words : Blockchain, Trust, Health, Secure Shared Medical Record, DMPS.

Résumé

Une Blockchain est une base de donné partagée permettant de créer la confiance entre des individus sans faire appel à des intermédiaires. L'architecture ici est décentralisée, autrement dit les donnée sont distribuées entre les utilisateurs, et donc les informations ne peuvent jamais être effacées. Et parmi les secteurs prometteurs de cette technologie (on entend ici la Blockchain), on spécifie le secteur de la santé, car il est vraiment très sensible puisqu'il s'agit de partager les informations des patients et leurs données de santé. Dans ce contexte, l'objectif de ce mémoire consiste à proposer une approche de Blockchain dans le domaine médical qui vise à gérer les données de santé en utilisant des dossiers médicaux électroniques.

Mots-clés : Blockchain, Confiance, Santé, Dossier Médical Partagé Sécurisé, DMPS.

Remerciements

Tout d'abord, je remercie Dieu Tout Puissant de m'avoir donné la force et la patience nécessaire pour achever ce travail de mémoire.

Mes sincères remerciements à mon honorable encadreur Professeur **Kazar Okba** de sa disponibilité, son soutien continu, sa motivation, ainsi que pour ses précieux conseils et la confiance qu'il m'a accordée qui ont fortement contribué à mener à bien ce travail.

Je remercie également les membres de jury, qui vont accepté de lire et d'évaluer ce travail.

Je veux également remercier la Dr **Mancer Soumia** pour m'avoir aidé à rédiger ce mémoire ainsi que pour ses conseils.

Enfin, je tiens à remercier tous ceux qui m'ont aidé et soutenu de près ou de loin pour l'accomplissement de ce mémoire et en particulier ma famille.

Table des matières

Table des figures

Introduction Générale

La Blockchain est l'un des buzzwords dans le monde de la technologie. Cette technologie a fait exploser de nombreux marchés dans une période de crise de confiance et de mécontentement envers les tiers et les médiateurs traditionnels, les institutions, les banques et les États.

La technologie Blockchain, qui porte la promesse de la désintermédiation et de la transparence, est attrayante et intrigante. La Blockchain promet de révolutionner la façon dont nous effectuons les transactions, tout comme l'ordinateur a révolutionné la façon dont nous traitons les données aujourd'hui, et tout comme Internet a révolutionné la façon dont nous partageons les informations à tous les niveaux. Eh bien, la première instanciation de la technologie Blockchain est la ***Cryptomonnaie Bitcoin***, en tant qu'un réseau de paiement innovant et une nouvelle forme d'argent fonctionnant sans autorité centrale, elle est gratuite et ouverte.

Dans un modèle Blockchain, il n'est pas nécessaire de stocker des informations avec des tiers. Les enregistrements sont sur de nombreux ordinateurs avec des informations identiques, de sorte que les violations n'ont aucun sens et si les données de la Blockchain d'un ordinateur sont violées, le système rejette une telle violation. Même si un pirate pénètre dans un réseau et tente de voler de l'argent sur un compte, plusieurs copies redondantes et identiques du même registre sont stockées dans le monde entier. En cas de violation, il y en a beaucoup d'autres sous forme de sauvegardes qui peuvent fournir les fonds du compte piraté. En d'autres termes, les données de la Blockchain sont distribuées autour de nombreux ordinateurs imbriqués. Pour que les efforts de piratage réussissent, plus de 50% des systèmes de réseau doivent être piratés.

la technologie Blockchain, depuis sa création, est en constante évolution et aujourd'hui il existe de nombreuses applications dans de nombreux domaines qui l'adoptent. Ces applications peuvent être classées en deux parties : les applications intelligentes et non intelligentes. Effectivement, la plupart des applications intelligentes utilisent la Blockchain et l'apprentissage automatique. Alors que d'autres applications s'appuient sur la Blockchain et d'autres techniques.

Le secteur de la santé est un secteur particulièrement prometteur de la technologie Blockchain, car il est vraiment très sensible puisqu'il s'agit de partager les informations des patients et leurs données de santé. Un défi qui persiste est l'incapacité de contrôler les données après la transmission, et cela, en fait, comprend deux facteurs importants : la confidentialité et la sécurité. La Blockchain présente

une technologie qui peut éventuellement fournir une solution de sécurité robuste et solide et un niveau élevé de protection de la vie privée.

Dans ce travail, on présente le potentiel de la technologie Blockchain pour faciliter le partage de données de santé privées en toute sécurité. Ainsi que on définit notre proposition : *une contribution d'architecture système qui adopte la Blockchain, où notre système vise à gérer les données de santé en utilisant des dossiers médicaux électroniques*. Une Blockchain consiste en une liste sans cesse croissante d'enregistrements appelés blocs, où chacun d'eux représente une consultation, et donc un document médical. Chaque bloc est lié de manière cryptographique à son bloc précédent formant ainsi une chaîne. La Blockchain est gérée par un réseau peer-to-peer de nœuds. Tous les nœuds de réseau qui sont liés au même patient contiennent la même réplique des données appartenant à un tel patient, ce qui permet d'éliminer le besoin d'une autorité de confiance centrale pour gérer les données.

Ce travail est organisé en deux parties : la première concerne l'état de l'art de notre sujet et la deuxième présente la réalisation d'un système pour un dossier médical électronique en se basant sur la Blockchain.

La première partie : *État de l'art

Le premier chapitre présente les notions générales de la technologie Blockchain, incluant l'historique, les domaines d'application, et l'architecture et le fonctionnement.

Le deuxième chapitre est consacré à décrire Les applications intelligente et non intelligente ainsi que le domaine médical et ses applications. Le chapitre se termine par une étude comparative entre ces différents applications.

La deuxième partie : *Contribution

Le troisième chapitre offre la conception du système proposé et donc les étapes de développement.

Le quatrième chapitre effectivement présente la réalisation et l'implémentation de notre système.

Enfin, on termine notre mémoire par une conclusion générale.

Chapitre 1

Etat de l'art de la technologie Blockchain

1 Introduction

Si vous n'avez pas passé les dernières années dans une grotte, vous connaissez la Blockchain. Blockchain est l'un des buzzwords dans le monde des technologies. Cette technologie a fait exploser de nombreux marchés, à l'heure de la crise de confiance et du mécontentement vis-à-vis des tiers et médiateurs traditionnels, institutions, banques et états. La technologie Blockchain, qui porte la promesse d'une désintermédiation et de la transparence, séduit et intrigue.

La première instanciation de la technologie Blockchain est la cryptomonnaie Bitcoin. Depuis sa création, la technologie a évolué et il existe aujourd'hui de nombreux types de Blockchain, chacune avec ses propres spécificités et usages qui vont bien au-delà des cryptomonnaies. Le potentiel inhérent à cette technologie est bien réel ; la Blockchain promet de révolutionner la manière dont nous effectuons des transactions, au même titre que l'ordinateur révolutionna la manière dont nous traitons aujourd'hui les données, et au même titre qu'internet a révolutionné la manière dont nous partageons l'information au quotidien [1].

Ce premier chapitre a pour objectif de présenter les notions générales de la technologie Blockchain. On commence par les définitions les bien connus dans le domaine, avec un peu d'histoire. Ensuite, on définit les caractéristiques principales de la technologie, les modèles pouvant être adopté, l'architecture et le fonctionnement. On met l'accent, par la suite, sur les approches de développement d'une application Blockchain. Finalement, on cite les domaines d'application de la technologie.

2 Définition

La notion de Blockchain a été apparue en 2008 lors de la création du bitcoin, comme son cas d'usage le plus connu, par un inconnu dont le pseudonyme est Satoshi Nakamoto. On trouve à l'heure actuelle plusieurs définitions pour Blockchain ont été proposées, parmi ces définitions on cite les suivantes :

1. une Blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et trans-

fère de la valeur ou des données via Internet, de façon transparente, sécurisée, et autonome sans organe central de contrôle [2].

2. Littéralement, une Blockchain désigne une chaine de blocs, des conteneurs numériques sur lesquels sont stockés des informations de toutes natures : transactions, contrats, titres de propriétés, œuvres d'art, ..., etc. L'ensemble de ces blocs forme une base de données semblable aux pages d'un grand livre de comptes. Ce livre des comptes est décentralisé [4].
3. « technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle » [5].
4. « 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. » [6].

On peut aussi proposer cette définition, comme un résume de ce qui précède : Une Blockchain est une base de donné partagée permettant de créer la confiance entre des individus sans faire appel à des intermédiaires. L'architecture ici est décentralisée, autrement dit les donnée sont distribuées entre les utilisateurs, et donc les informations ne peuvent jamais être effacées.

3 Historique de Blockchain

La technologie de la Blockchain est l'une des plus grandes innovations du 21ème siècle, en raison de son effet d'entraînement sur divers secteurs. L'histoire de la Blockchain remonte au début des années 1990.

En 1991 :
L'architecture derrière la technologie de la Blockchain a été décrite dès 1991 quand les chercheurs Stuart Haber et W. Scott Stornetta ont travaillé sur une chaîne de blocs sécurisée de manière cryptographique, selon laquelle la personne ne pouvait altérer l'horodatage des documents. En 1992, ils ont mis à niveau leur système afin d'incorporer les arborescences Merkle, ce qui permet l'amélioration d'efficacité, et ainsi la permission de collecter des documents sur un seul bloc, cependant cette technologie tomba dans l'oubli [7].

En 1995 :
Le NY Times met en place la première Blockchain dans le journal, cette technologie qui est toujours active, est la plus longue Blockchain de l'histoire [8].

En 2004 :
L'informaticien et l'activiste cryptographique Hal Finney, lance un système appelé RPoW (Reusable Proofs of Work). RPoW a résolu le problème de la double dépense, conçu pour permettre à n'importe quel utilisateur à travers le monde de vérifier son exactitude et son intégrité en temps réel [9].

En 2008 :
La première Blockchain est apparue fin 2008 avec la monnaie numérique bitcoin, développée par un inconnu sous le pseudonyme de Satoshi Nakamoto [10]. Le logiciel Bitcoin original a été mis à la disposition du public en janvier 2009. Il s'agissait d'un logiciel open source, ce qui signifiait que tout le monde pouvait examiner le code et le réutiliser. Il consiste d'un système expérimental

de transfert et de vérification de propriété reposant sur un réseau de peer-to-peer sans aucune autorité centrale [11]. Ce réseau est basé sur l'algorithme de preuve de travail HashCash, mais au lieu d'utiliser une fonction informatique de confiance comme le RPoW, la protection contre la double dépense est assurée par un protocole peer-to-peer décentralisé afin de suivre et de vérifier les transactions [9].

2013 :

En 2013, Vitalik Buterin, programmeur et cofondateur du magazine Bitcoin, a fondé Ethereum, il souhaitait un Blockchain plus volatile, qui n'était pas uniquement utilisé pour les monnaies. En 2015, il a lancé Ethereum comme une deuxième Blockchain publique, qui peut enregistrer des contrats, des emprunts, . . . , etc ; tandis que le Bitcoin ne peut enregistrer que des transactions [9].

Ethereum est un réseau de Blockchain publique distribué qui vise à exécuter le code de programmation de n'importe quelle application décentralisée [12]. il est utilisé pour créer ce qu'on appelle des contrats intelligents. Les contrats intelligents sont des programmes ou des scripts déployés et exécutés sur la Blockchain Ethereum. Ils peuvent par exemple être utilisés pour effectuer une transaction si certaines conditions sont remplies. Ils sont écrits dans des langages de programmation spécifiques et compilés sous forme de bytecode, qui est une machine virtuelle 'Turing-complet' décentralisée, appelée la machine virtuelle Ethereum (ou EVM pour Ethereum Virtual Machine) pouvant ensuite les lire et les exécuter [9].

4 Caractéristiques principales de la technologie Blockchain

Généralement, la technologie Blockchain est caractérisée par :

- **La désintermédiation :** la technologie Blockchain permet d'échanger les informations et les valeurs et peut contrôler et valider les opérations effectuées sans intervenir une autorité centrale (la Blockchain est décentralisé, ainsi la confiance est distribué).
- **La transparence :** la Blockchain est qualifiée d'être transparente car tout le monde peut la télécharger dans son intégralité et vérifier à tout moment son honnêteté [13]. Tout le monde peut voir les transactions et les échanges actuelles et passées ce qui permet à chacun de vérifier la validité de la chaîne.
- **La sécurité :** les données ne sont pas hébergées par un serveur unique mais par une partie des utilisateurs [13], ce qui rend la suppression de toutes les copies des documents impossible.
- **L'autonomie :** la puissance de calcul et l'espace d'hébergement sont fournis par les nœuds du réseau, c'est-à-dire les utilisateurs eux-mêmes. Il n'y a donc pas besoin d'infrastructure centrale [10], car elle est distribuée dans tous les utilisateurs.

5 Les modèles de la Blockchain

Il existe trois types de la Blockchain : des Blockchains publics ouvertes à tous, des Blockchains privées dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs, et des Blockchains consortiums (hybrides).

5.1 Blockchain public

N'importe où, n'importe qui dans le monde à tout moment peut avoir accès à toutes les transactions en cours. De plus, le public peut également participer activement au processus de consensus - ce type de Blockchain est connu pour être totalement décentralisé. Dans ce système, toute personne peut influencer le processus de consensus [14].

En bref, tout le monde peut consulter et utiliser Blockchain publique comme dans les Blockchains Bitcoin et Ethereum.

5.2 Blockchain privé

Ce type de Blockchain est considéré comme un réseau centralisé car il est entièrement contrôlé par une organisation [62]. Dans une Blockchain privée, une autorité régulatrice valide l'introduction de nouveaux membres et accorde les droits en écriture et en lecture. Cette autorité peut être seule aux commandes ou gouvernée collégialement par les différents participants [15]. Donc son accès et son utilisation sont limités à certains acteurs. Personne ne peut y participer sans y être autorisé mais tout le monde peut la consulter [13].

5.3 Blockchain consortium (hybride)

Lorsqu'un nombre spécifique de nœuds sont créés pour contrôler le processus de consensus, nous parlons d'une Blockchain de consortium. Ce type de Blockchain peut être considéré comme partiellement décentralisé, car le droit d'accès au réseau peut être limité à un certain nombre de participants [14]. La Blockchain de consortium, ou hybride, est sous le contrôle d'un ensemble d'organisations au sein desquelles le droit d'accès peut être ouvert à tous ou limité à certains utilisateurs. Ce type de Blockchain est souvent utilisé dans les secteurs très réglementés tels le secteur bancaire [13].

Donc seul un groupe de nœuds présélectionnés participerait au processus de consensus d'une Blockchain du consortium.

5.4 Comparaison entre Blockchain privée et publique

Table 1.1 résume les points de différence entre Blockchain privée et publique, en termes d'accès, la vitesse, l'identité, et la sécurité.

6 Architecture

D'après [16] [17] la technologie de Blockchain présente les caractéristiques essentielles de la décentralisation, de la responsabilité et de la sécurité. La Blockchain est

	Blockchain publique	Blockchain privée
Accès	Accès ouvert	Avec autorisations
Vitesse	Lent	Rapide
Identité	Anonyme/Pseudonyme	Identités connues
Sécurité	Proof-of-Work/Proof-of-Stake	Administrateur prédéfini

TABLE 1.1 – Comparaison entre Blockchain privée et publique [31]

.

une combinaison d'ordinateurs reliés les uns aux autres au lieu d'un serveur central, ce qui signifie que tout le réseau est décentralisé.

L'architecture traditionnelle du World Wide Web utilise un réseau client-serveur. Dans ce cas, le serveur conserve toutes les informations requises au même endroit, ce qui facilite sa mise à jour, car c'est une base de données centralisée contrôlée par un certain nombre d'administrateurs disposant d'autorisations.

Dans le cas de l'architecture distribuée du réseau en chaîne, chaque participant du réseau gère, approuve et met à jour les nouvelles entrées. Le système est contrôlé non seulement par des individus distincts, mais également par tous les membres du réseau de la Blockchain.

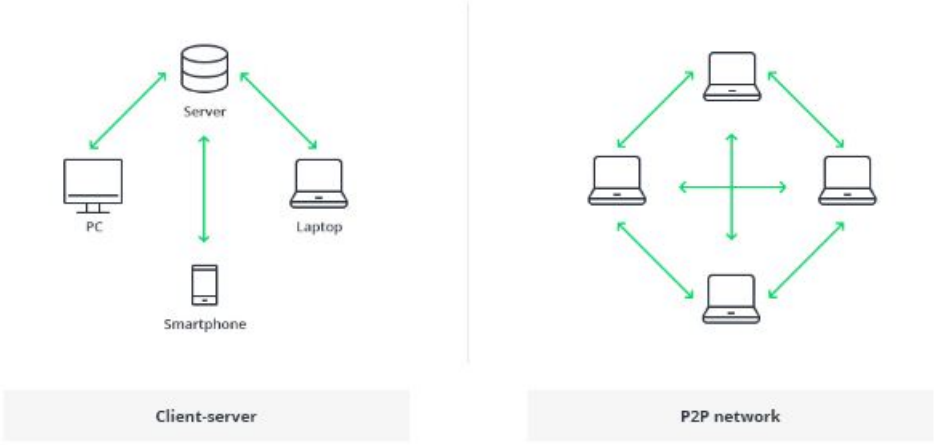

FIGURE 1.1 – Client-serveur vs Réseau P2P [16]

.

La structure de la technologie Blockchain est représentée par une liste de blocs avec des transactions dans un ordre particulier. Les données de transaction sont stockées en blocs, qui sont reliés entre eux pour former une chaîne. À mesure que

le nombre de transactions augmente, la taille de la Blockchain augmente également. Les composants architecturaux ont été généralisés puis modifiés par diverses entreprises, menant à différents projets de Blockchain tels que Bitcoin, Ethereum, Hyperledger, ..., etc. Voici les principaux composants de l'architecture Blockchain (revenant à [18] [17] [19]).

6.1 Transaction

Les transactions sont les choses qui donnent un but à la Blockchain. Ils sont les plus petits blocs de construction d'un système de Blockchain. Les transactions consistent généralement en une addresse de destinataire, une adresse d'expéditeur et une valeur. Les transactions contiennent une ou plusieurs entrées et une ou plusieurs sorties. Une entrée est une référence à une sortie d'une transaction précédente.

6.2 Blocs

Les blocs sont des structures de données ayant pour but de regrouper des ensembles de transactions et d'être distribués à tous les nœuds du réseau. Chaque bloc contient un en-tête, qui est la métadonnée permettant de vérifier sa validité, tandis que le reste contient des transactions que le mineur a choisi d'inclure dans le bloc qu'il a créé. Le nombre maximum de transactions qu'un bloc peut contenir dépend de la taille du bloc et de la taille de chaque transaction.

6.3 Consensus

Les mécanismes consensuels sont des protocoles garantissant que tous les nœuds (le périphérique de la chaîne qui gère la chaîne et (parfois) traite les transactions) sont synchronisés les uns avec les autres et conviennent des transactions légitimes à ajouter à la chaîne. Ces mécanismes de consensus sont cruciaux pour une Blockchain afin de fonctionner correctement. Ils s'assurent que tout le monde utilise la même Blockchain. Tout le monde peut soumettre des éléments à ajouter à la Blockchain. Il est donc nécessaire que toutes les transactions soient constamment vérifiées et que la Blockchain soit constamment auditée par tous les nœuds. Sans un bon mécanisme de consensus, les Blockchains sont exposées à diverses attaques.

6.4 Exploitation minière (mining)

Le minage est la validation d'un bloc par l'un des membres du réseau. Un bloc est un groupe d'opérations, qui vont être groupés entre eux, et qui sont ensuite montés dans la suite de Blockchain. C'est donc l'opération fondamentale dans les blocs, quelle est celle qui se présente, centralisée classique.

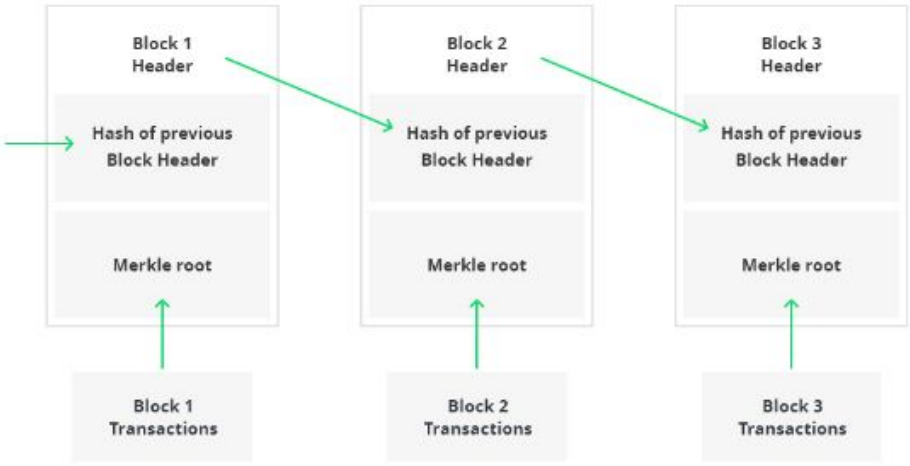

FIGURE 1.2 – Bloc [16]

.

7 Fonctionnement

D'après [8], le protocole Blockchain est essentiellement un grand livre numérique distribué, composé de transactions numériques et partagé sur un réseau. Ce protocole est basé sur une architecture peer-to-peer, chaque participant constituant un nœud dans le réseau. Ces participants stockent une copie identique du grand livre puis travaillent ensemble dans le processus de valider et certifier les transactions numériques, en ajoutant de nouvelles transactions au grand livre.

Le processus d'ajout de transactions consiste à évaluer la transaction proposée et à la soumettre à un vote. Si la majorité des participants estiment que la transaction est valide, elle est ajoutée au grand livre, ce qui la lie à la transaction précédente, formant une chaîne qui ne peut être modifiée sans en briser l'intégrité. Chaque transaction qui passe par le processus de liaison est regroupée dans un bloc, qui contient en outre un hachage cryptographique du bloc précédent, puis est ajouté linéairement au grand livre dans l'ordre chronologique.

Les modifications apportées au grand livre sont répliquées sur l'ensemble du réseau et, de ce fait, chaque participant dispose d'une copie complète du grand livre mis à jour. Cela signifie également qu'aucun participant n'a la capacité d'attaquer facilement l'ensemble du réseau distribué. Bien qu'il reste la notion de transaction, les données associées à l'un peuvent être de n'importe quel type, car la Blockchain relie simplement les données qui y sont stockées.

Le format des transactions est défini par le réseau sous-jacent prenant en charge la Blockchain, tandis que les données présentes dans celles-ci sont définies par les participants qui les créent. Ces données peuvent être cryptées et signées numériquement afin d'apporter au système des avantages supplémentaires tels que l'authenticité, l'intégrité et la non-répudiation. Les transactions sont ajoutés à la chaîne lorsqu'un mécanisme de consensus spécifique est vérifié.

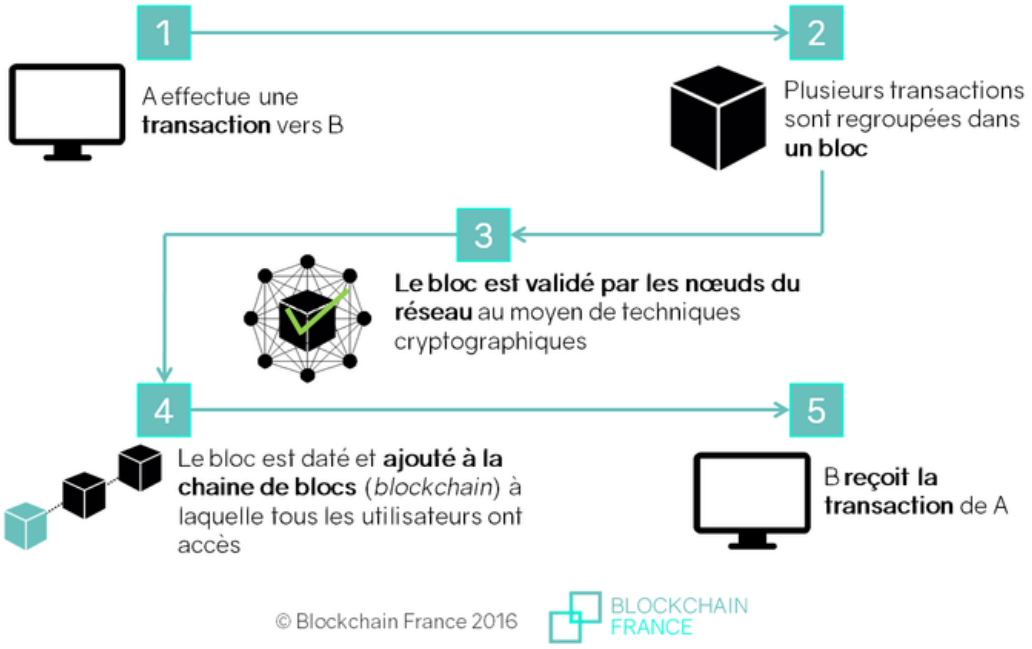

FIGURE 1.3 – Fonctionnement de la Blockchain [5]

8 Les approches de développement d'une application Blockchain

Comme tout autre processus de développement, le développement d'applications Blockchain nous oblige également à délimiter la portée et le but de l'application, mais avant de creuser le processus de développement d'applications Blockchain nous devons découvrir ses types en fonction du type de réseau. D'après [20] il existe deux types :

1. **Une Blockchain sans autorisation :** est accessible à tous les membres du réseau et elle est disponible sur n'importe quel appareil. Chaque utilisateur peut accéder au code, vérifier les transactions, interagir avec les autres et rester anonyme. Par exemple, Bitcoin est sans autorisation.
2. **Une Blockchain autorisée :** n'autorise que les participants autorisés. Tous les utilisateurs ont des rôles et des autorisations. Une Blockchain autorisée a des règles qui régissent les transactions entre les membres du réseau. Ce type de Blockchain est idéal pour gérer les opérations au sein des organisations.

Passant maintenant à présenter les étapes de développement d'applications Blockchain. Ils sont répartis comme suit :

clarifiez votre idée :
Comme pour toute entreprise ou produit, l'idée est la première chose à laquelle vous devez penser avant de commencer à développer une application Blockchain. Et parmi les questions auxquelles vous devez répondre : Pourquoi j'utilise Blockchain ? Est-il besoin d'utiliser Blockchain ? Vous devez aussi identifier les cas d'utilisation de votre application et assurer que votre idée nécessite ou non une Blockchain [21].

identifiez le problème et l'objectif :
La deuxième étape consiste à définir l'énoncé du problème. À ce stade, vous devez définir le problème à résoudre et la façon dont vous vous attendez à ce que l'application le résout [22].

Identifiez les acteurs du système :
La troisième étape consiste à définit les acteurs de la Blockchain. D'après [25], il y a dans la Blockchain, comme dans tout système encadrant des transactions, deux types d'acteurs : les utilisateurs du système d'une part ; et ceux qui l'organisent et mettent en place l'infrastructure d'autre part.

- *Les utilisateurs :* sont les mêmes que dans un système classique. D'une côté, il y a l'initiateur de la transaction : le débiteur qui paye une somme d'argent. Et de l'autre il y a le bénéficiaire de la transaction qui, corrélativement, est le créancier qui reçoit une somme d'argent.
- *Les organisateurs :* ce sont les organisateurs qui diffèrent fondamentalement du système classique, du moins dans la Blockchain publique.

identifiez le mécanisme de consensus le plus approprié :
Étant donné que la Blockchain est un système décentralisé, tous les membres du réseau doivent authentifier une transaction, ce processus est appelé consensus [22]. Il existe de nombreux mécanismes de consensus disponibles en fonction des besoins individuels. Et d'après [23] les mécanismes suivants sont les plus populaires :

- preuve de travail : (utiliser par Bitcoin)
- Preuve d'enjeu
- Preuve de temps écoulé
- Tolérance aux pannes byzantine
- Fédérée
- Round Robin
- Preuve déléguée de pieu

Vous pouvez choisir la méthode idéale en fonction de votre cas d'utilisation individuel.

Et la dernière étape consiste à présenter l'architecture globale du système. Figure 1.4 bien définit le processus de déroulement de Blockchain pour un système financier.

9 Domaines d'application

Aujourd'hui, de nombreux domaines s'intéressent au développement des produits et des solutions techniques basées sur la technologie Blockchain.

En raison de l'enthousiasme et des promesses de la Blockchain en termes de ra-

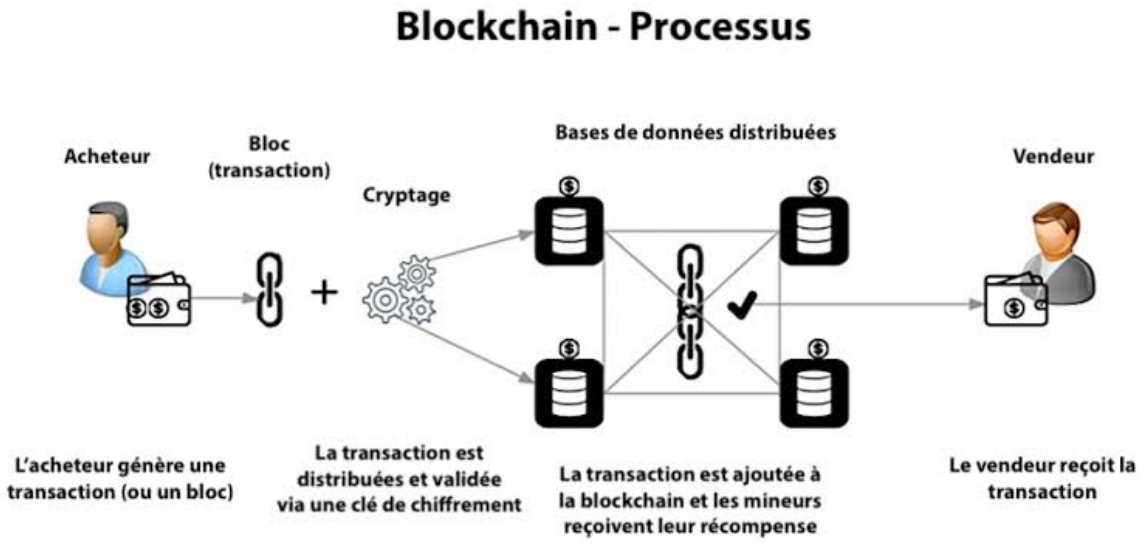

FIGURE 1.4 – Processus de Blockchain [63]

.

pidité et de sécurité des transactions, elle a été adoptée dans de nombreux domaines d'application. Dans ce qui suit, nous mentionnons les plus connus.

9.1 La banque

Le secteur de la banque et de la finance est largement impliqué dans cette technologie. Différents prestataires et acteurs du domaine proposent des solutions de portefeuilles électroniques, permettent des transactions financières rapides et sécurisées entre particuliers et professionnels, et entre organismes bancaires [8].

Les clients peuvent voir leurs transactions traitées en moins de 10 minutes, tandis qu'une opération semblable prend 1 à 3 jours à vérifier en raison du volume considérable de transactions que les banques doivent régler, quel que soit le moment ou le jour de la semaine. Grâce à la Blockchain, les banques ont également la possibilité d'échanger des fonds entre institutions plus rapidement et en toute sécurité. Capgemini, un cabinet de conseil français, estime que les consommateurs peuvent économiser chaque année jusqu'à 16 milliards de dollars en frais bancaires et en frais d'assurance via des applications basées sur la Blockchain.

En avril 2016, BNP Paribas Securities Services a annoncé travailler à la mise au point d'un registre utilisant le protocole Blockchain [27].

9.2 Les soins de santé

Dans le secteur des soins de santé, la technologie Blockchain a la capacité d'agir sur le partage de données cliniques, en stockant les données elles-mêmes ou en indiquant les personnes qui peuvent accéder à ces données , en sécurisant l'identité et les informations des patients et des prestataires, en optimisant la gestion des données. Chaîne d'approvisionnement en soins de santé, partage de données et consentement

pour la recherche et les essais cliniques, et traitement des assurances et des réclamations et détection/réduction des activités frauduleuses [28].

Les prestataires de soins de santé peuvent utiliser la Blockchain pour stocker en toute sécurité les dossiers médicaux de leurs patients. Ce qui fournit aux patients la preuve et la certitude que le dossier ne peut pas être modifié, et ainsi assurer la confidentialité.

9.3 Les enregistrements de propriété

Le processus d'enregistrement des droits de propriété est fastidieux, inefficace et prend beaucoup de temps, mais il est plein d'erreurs humaines car il rend chaque inexactitude de suivi de la propriété moins efficace. Si la propriété est stockée et vérifiée sur une Blockchain, les propriétaires peuvent avoir la certitude que leurs activités sont exactes et durables [27].

9.4 Le vote

L'un des domaines les plus valides pour une Blockchain est celui de voter. Blockchain distribue des informations de vote individuelles sur des milliers d'ordinateurs à travers le monde, rendant impossible la modification ou la suppression des votes une fois qu'ils ont été exprimés. Cette approche favorise une plus grande confiance entre les électeurs et les gouvernements en protégeant leurs données et leur vie privée [29]. Et donc éliminer la fraude électorale et augmenter la participation électorale. Le protocole de Blockchain maintiendrait également la transparence du processus électoral, en réduisant le personnel nécessaire à la conduite des élections et en fournissant aux fonctionnaires des résultats immédiats [29]. Le vote a été testé lors des élections de mi-mandat de novembre 2018 en Virginie-Occidentale. Chaque vote serait stocké sous forme de bloc sur la Blockchain, les rendant quasiment impossibles à altérer.

9.5 L'éducation

De nos jours, certaines universités et instituts ont appliqué la technologie Blockchain à l'éducation, et la plupart d'entre elles l'utilisent pour soutenir la gestion et la récapitulation de diplômes universitaires. De plus, la technologie Blockchain contribue à réduire le nombre de fraudes [30].

Dans le passé, il y avait de nombreux cas de fraude de degré. Cependant, il est possible d'éviter cela en utilisant maintenant la Blockchain pour accorder et gérer les diplômes des étudiants. Ainsi, la fiabilité et l'autorité sont les deux assurées, ce qui réduira considérablement le degré de fraude [30].

9.6 La certification de documents

Comme un autre grand domaine concerné par cette technologie, en considère la certification de documents. Du fait de la capacité à rendre l'information irrépudiable et publiquement certifiée, différentes mises en œuvre à base de Blockchain ont été réalisées. On peut citer par exemple, l'état civil et le permis de conduire à base de Blockchain développé par le gouvernement Australien, la certification de diplômes ou différents documents notariés [8].

9.7 L'assurance

La compagnie d'assurance française Axa a récemment lancé une police intitulée Fizzy via la Blockchain Ethereum. Le but de l'assurance voyage est d'assurer les passagers contre les retards. Les passagers qui souhaitent utiliser le service n'ont qu'à s'inscrire. L'objectif est de rendre la conclusion des contrats et le règlement des sinistres plus transparents sur la base de la Blockchain [31].

9.8 L'énergie

Dans le domaine de l'énergie, la Blockchain permet de revendre directement l'énergie propre fournie par panneaux solaires ("smart grids") à son voisin sans passer par de grands fournisseurs. Le promoteur Bouygues Immobilier a pour projet de lancer un mini-smart grid décentralisé à Lyon, via une Blockchain privée [32].

9.9 L'économie collaborative

La Blockchain se prête particulièrement à l'économie collaborative et en particulier au covoiturage en faisant "sauter" tout intermédiaire. Lazooz.net ou encore Arcade City proposent leurs services via une application reposant sur la technologie Blockchain [32].

10 Avantages & inconvénients de la technologie Blockchain

D'après [9] [33] [34], la création de la technologie Blockchain a apporté de nombreux avantages dans de nombreux secteurs, offrant une sécurité accure dans des environnements sans confiance. Cependant, sa nature décentralisée présente également certains inconvénients.

* Parmi ses avantages, on cite :
  La distribution : les données de la Blockchain sont souvent stockées dans des milliers de périphériques sur un réseau de nœuds distribué, le système et les données résistent très bien aux défaillances techniques et aux attaques malveillantes.
  La stabilité : une fois que les données ont été enregistrées dans la Blockchain, il est extrêmement difficile de les supprimer ou de les modifier. Cela fait de Blockchain une technologie de choix pour stocker des enregistrements financiers ou toute autre donnée.
  Système sans tiers de confiance : un système de Blockchain élimine le risque de faire confiance à une seule organisation et réduit également les coûts globaux et les frais de transaction en éliminant les intermédiaires et les tiers.

* Bien que ses inconvénients peuvent être résumé dans ce qui suit :
  Modification de données : un inconvénient des systèmes Blockchain est qu'une fois que des données ont été ajoutées à la Blockchain, il est très

difficile de les modifier, ce n'est pas toujours bon. Changer les données ou le code d'une Blockchain est généralement très exigeant.

Clés privées : Blockchain utilise une clé publique, chaque adresse de Blockchain a une clé privée correspondante. Les utilisateurs ont besoin de leur clé privée pour accéder à leurs fonds. Si un utilisateur perd sa clé privée, l'argent est effectivement perdu et il ne peut rien y faire.

Stockage : les registres de Blockchain peuvent devenir très volumineux avec le temps. La croissance de la taille de la Blockchain devient supérieure à celle des disques durs, le réseau risque de perdre des nœuds si le registre devient trop volumineux pour être téléchargé et stocké par les utilisateurs.

11 Conclusion

Il semble évident que la Blockchain s'impose naturellement dans les domaines où les avantages de son utilisation sont considérables. Puis progressivement, s'imposer à d'autres secteurs. Mais seul l'avenir nous dira comment nos sociétés utiliseront cette technologie dans le futur. Dans le chapitre suivant, on met l'accent sur des applications utilisant la Blockchain. Ces applications sont classées comme intelligentes, non-intelligentes et appartenant également au domaine médical.

Chapitre 2

Les applications intelligentes et non intelligentes du Blockchain

1 Introduction

L'intelligence artificielle comme la Blockchain sont des technologies qui participent au changement du monde, améliorant presque toutes les industries dans lesquelles elles sont mises en œuvre [35].

La Blockchain et l'intelligence artificielle se combinent pour tout mettre à niveau, de la logistique de la chaîne d'approvisionnement alimentaire et du partage de dossiers de santé aux redevances médias et à la sécurité financière. Mais leurs applications restent actuellement très techniques et peu connues du grand public, même si l'intelligence artificielle devient de plus en plus connue. Pourtant très distinctes, ces technologies pourraient collaborer ensemble afin d'offrir un panel d'applications plus vaste. En combinant les avantages de chaque technologie [35].

Dans ce deuxième chapitre, on présente l'adoption de la technologie Blockchain dans des applications intelligentes et non intelligentes, ainsi que dans le domaine médical. Enfin, une étude comparative entre ces différents travaux est fournie.

2 Les applications intelligentes

Dans cette section on présente les applications du Blockchain intelligentes.

2.1 FINALZE

Emplacement : Golden, Colo.
Utilisation de la Blockchain ? Finalze est une plate-forme logicielle qui utilise la Blockchain et l'apprentissage automatique pour créer des applications visant à améliorer les infrastructures civiles. Les outils de la société automatisent et accélèrent les flux de travail, les processus de gestion et de vérification de l'industrie de la construction, et sa technologie s'intègre également aux appareils portables pour répondre aux réglementations de sécurité [36].
Impact sur l'industrie : Finalze vise à rendre les processus cruciaux plus efficaces

tout en maximisant le retour sur investissement dans une industrie dont les revenus devraient atteindre 15,5 billions de dollars d'ici 2028 [36].

2.2 BEXT360

Emplacement : Denver.
Comment il utilise la Blockchain ? Bext360 utilise l'IA et la Blockchain pour améliorer la transparence et l'efficacité de la chaîne d'approvisionnement dans les industries du café, du bois, des fruits de mer et des minéraux. L'intelligence artificielle de la société analyse les cultures et prédit les schémas de croissance, tandis que la Blockchain assure l'enregistrement de la chaîne d'approvisionnement d'un produit, de la semence au produit fini [36].
Impact sur l'industrie : Bext360 a appliqué des applications mobiles, des robots et des chaînes de blocs à la chaîne d'approvisionnement du café pour créer un parcours plus transparent et éthique du grain à la tasse. L'IA de l'entreprise mesure la qualité des grains de café et prédit les conditions météorologiques et les tendances de croissance, tandis que la Blockchain enregistre immuablement la ferme d'où proviennent les grains et les spécifications exactes d'une livraison de café. Il sert même de registre de paiement pour garantir que toutes les parties sont payées rapidement et équitablement [36].

L'application et le logiciel cloud de la startup Bext360 basée à Denver utilisent la chaîne de blocs Stellar pour enregistrer les horodatages et la valeur des transactions en temps réel. Les parties à la transaction telles que les entreprises, les agriculteurs et les coopératives rendent les données transparentes. Il crée des enregistrements de l'origine des grains de café. Le système crée également un enregistrement de qui a payé combien. De cette façon, il devrait apporter une transparence totale dans la chaîne d'approvisionnement du café. Le système devrait être utilisé dans d'autres produits tels que le cacao [37].

La première entreprise de Bext360 sera un kiosque où les agriculteurs pourront vendre des haricots. Le système utilise une technologie de reconnaissance d'image intelligente qui évalue les cultures qui sont soumises dans les installations de production. Le système s'appuie sur l'apprentissage automatique pour classer la note et attribuer un prix. Un robot mobile permet aux acheteurs de café d'évaluer la qualité et le poids du produit d'un agriculteur sur le terrain [37].

2.3 BURSTIQ

Emplacement : Denver.
Comment il utilise la Blockchain ? BurstIQ a créé un «portefeuille santé», qui combine l'IA, la Blockchain et le big data pour gérer de manière holistique les données d'un patient. Le portefeuille Burst IQ permet à l'équipe de professionnels de la santé d'un patient d'accéder à son dossier de santé et à ses plans de bien-être. Les professionnels de santé peuvent alors choisir d'acheter, de vendre ou d'échanger des données sur les patients pour différentes études scientifiques ou pour en savoir plus sur une maladie spécifique. Cependant, la Blockchain permet aux patients de garder privées leurs informations d'identification personnelle tout en ne partageant

que des données de santé générales [36].
Impact sur l'industrie : BurstIQ utilise sa technologie pour lutter contre la crise des opioïdes. En enregistrant les antécédents de consommation de drogues d'un patient, BurstIQ peut suggérer différents traitements, médecins ou services qui peuvent aider à réduire la dépendance aux opioïdes [36].

La plate-forme propriétaire Big Data basée sur la Blockchain de BurstIQ permet à Empiric de gérer en toute sécurité les données des clients à grande échelle et d'effectuer des analyses avancées à l'aide des capacités d'apprentissage automatique et d'intelligence collaborative de la plate-forme. De plus, cela marque la première fois que les données et les enregistrements de soins de santé ont été stockés et gérés sur la Blockchain, faisant de la plate-forme de Blockchain propriétaire de BurstIQ la plate-forme de données sécurisée conforme HIPAA leader de l'industrie. La plateforme BurstIQ et l'écosystème travaillent ensemble pour améliorer la sécurité avancée des mégadonnées, augmenter l'accès à la santé et l'autonomisation personnelle, réduire les coûts des soins de santé et permettre de nouvelles perspectives et de nouveaux modèles de soins [38].

Une récente start-up de la santé appelée BurstIQ a exploré les soins de santé et Blockchain en détail. BurstIQ, basé sur la Blockchain propriétaire. La plateforme Big Data permet à un fournisseur de santé connu de gérer en toute sécurité les données des clients à grande échelle et d'effectuer des analyses avancées à l'aide de la plateforme, l'apprentissage automatique et les capacités d'intelligence collaborative. De plus, cela marque les premières données et enregistrements de soins de santé ont été stockés et gérés sur Blockchain, faisant de la plate-forme Blockchain propriétaire de BurstIQ le leader de la loi sur la transférabilité et la responsabilité en matière d'assurance maladie conforme à la loi HIPAA plate-forme de données sécurisée [39].

2.4 NETOBJEX

Emplacement : Irvine, Californie.
Comment il utilise la Blockchain ? NetObjex est une plate-forme d'infrastructure de ville intelligente qui utilise l'IA, la Blockchain et l'IoT pour tout alimenter, des appareils connectés aux produits basés sur le cloud. La combinaison de ces technologies aurait amélioré le suivi logistique, la détection des pannes en temps réel et l'authentification des données et des appareils [36].
Impact sur l'industrie : la bibliothèque de Brooklyn a utilisé la technologie de collecte de données de NetObjex pour accroître sa clientèle et stimuler son engagement positif. Pour utiliser la station de recharge téléphonique gratuite de la bibliothèque, les utilisateurs doivent d'abord regarder un clip vidéo de 15 à 30 secondes sur un appareil IoT compatible avec la Blockchain qui enregistre les réponses au sondage ultérieures [36].

L'infrastructure IoT actuelle manque de composants essentiels, avec des lacunes majeures dans les fondements de l'écosystème qui empêchent la réalisation du plein potentiel de l'IoT. Et NetObjex a développé les technologies pour combler ces lacunes. Chez NetObjex, nous imaginons un monde dans lequel toutes choses, de nos voitures et de nos maisons à nos actifs numériques comme un média ou un contrat juridique, interagissent dans un écosystème composé d'une pluralité d'enti-

tés de confiance et de propriété -sans intervention humaine. Nous fournissons une plate-forme sécurisée de bout en bout combinant les technologies de pointe de la Blockchain, de l'IoT et de l'intelligence artificielle (IA) pour permettre aux entreprises de développer et de gérer des produits intelligents capables de fonctionner de manière indépendante et, de manière critique, d'interagir ou «interopérer» avec d'autres appareils intelligents. La plate-forme phare de gestion des actifs numériques de la société utilisant l'IoT et la Blockchain est en production depuis juin 2016. La société continue d'investir dans la recherche et le développement pour améliorer cette gamme de produits. Alors que la demande pour la solution Blockchain augmente considérablement à l'échelle mondiale, la société se positionne comme une plate-forme Blockchain Middleware agnostique en ce qui concerne les réseaux décentralisés. À cette fin, la société prévoit un écosystème technologique comprenant de nombreuses chaînes de blocs publiques différentes contenant des silos d'informations. Pour se préparer à cette éventualité et en prévision de ce paysage technologique fragmenté [40].

2.5 SYSTÈMES HANNAH

Emplacement : San Francisco.
Utilisation de la Blockchain : Hannah Systems apporte l'IA et la Blockchain aux véhicules autonomes. Le portefeuille de la société comprend une plate-forme d'échange de données basée sur l'IA, un outil de cartographie en temps réel, un tableau de bord d'informations et une chaîne de blocs afin qu'un véhicule autonome puisse rapidement absorber, interpréter et stocker en toute sécurité les données [36].
Impact sur l'industrie : le deep learning propriétaire d'Hannan System prédit les informations routières en fonction du comportement humain, comme la marche sur piste et la vitesse. Il prend également en compte les notifications météorologiques et les encombrements à jour [36].

2.6 NEUREAL

Emplacement : Salt Lake City.
Comment il utilise la Blockchain ? Neureal est un moteur de prédiction qui combine l'IA, la Blockchain et les technologies cloud pour tout prévoir, de la bourse aux recherches Google. L'IA de l'entreprise analyse les prédictions passées pour prédire les événements futurs. De plus, son registre Blockchain enregistre chaque résultat afin que les réseaux informatiques puissent identifier les tendances des prévisions correctes [36].
Impact sur l'industrie : Neureal travaille sur sa combinaison IA/Blockchain pour une variété de secteurs. Plus récemment, la société a déclaré qu'elle travaillait sur une méthode basée sur l'IA pour prédire la trajectoire exacte des ouragans [36].

Neureal est un projet combinant la Blockchain et la technologie d'IA prédictive pour faire quelque chose de vraiment bénéfique pour l'humanité, plutôt que d'essayer de casser un hachage inutile. Neureal cherche à donner à l'humanité le pouvoir de voir l'avenir et de devenir illimité en mettant à disposition les outils actuellement utilisés par les entreprises les plus puissantes du monde entre les principaux de

tous. La conception de Neureal signifie qu'il a un grand potentiel pour devenir le prédicteur le plus précis du monde. Oubliez la précision fiable, nous partons à la chasse au cygne noir !

Neureal est une plaque-forme, qui permet à quiconque d'approcher la plaque-forme avec quelque chose qu'il veut prédire, des données qui, selon lui, sont pertinentes pour cette prédiction, et une récompense pour les prédicteurs les plus précis (dans notre devise des neurones). À partir de là, les algorithmes prédictifs, les réseaux de neurones, les marchés de prédiction alimentés / augmentés par l'homme se font concurrence pour fournir la prédiction la plus précise. Cette compétition présente un nombre incroyable d'avantages par rapport aux modèles existants. Par exemple, il garantit que le prédicteur le plus précis disponible est utilisé pour faire la prédiction à chaque fois, encourager le développement de nouveaux algorithmes / techniques prédictifs et le raffinement des algorithmes existants. Cela crée également un excellent marché pour les projets qui tentent actuellement de permettre aux individus de reprendre le contrôle de leurs données et de monétiser pour eux-mêmes, car nos prédicteurs tentent toujours recherché plus de données qui, selon eux, leur permettraient de prédire avec plus de précision.

Le projet est également, une solution très éloquente à la question : «Que fait-on de tout ce gaz gaspillage d'énergie dans la cryptographie ?» Avec Neureal, le pouvoir est utilisé pour faire des prédictions utiles pour les particuliers et les entreprises plutôt que d'essayer de casser un inutile hacher. La plupart des experts que j'ai écoutés dans l'espace disent depuis des années que toute cette puissance de hachage sera finalement utilisée pour l'IA [42].

3 Les applications non intelligentes

3.1 Bitcoin

Bitcoin est un réseau de paiement novateur et une nouvelle forme d'argent [43]. C'est une technologie pair à pair fonctionnant sans autorité centrale. La gestion des transactions et la création de bitcoins est prise en charge collectivement par le réseau. Bitcoin est libre et ouvert, sa conception est publique, personne ne le possède ni ne le contrôle, et tous peuvent s'y joindre. Grâce à plusieurs de ses propriétés uniques, cette application rend possible des usages prometteurs qui ne pourraient pas être couverts par les systèmes de paiement précédents [43].

D'après [44], Bitcoin peut souvent faire référence à deux choses. Premièrement, le réseau Bitcoin qui assure le suivi de nos transactions et soldes, et deuxièmement, la devise que nous utilisons comme unité de valeur lors de nos transactions. Le réseau de paiement de Bitcoin est ce qui nous permet de traiter entre nous. Le réseau utilise un consensus distribué pour vérifier et confirmer les transactions, et un consensus est atteint via un vaste réseau mondial d'ordinateurs hautes performances exécutant le logiciel Bitcoin. Chaque fois que quelqu'un envoie une transaction, elle est diffusée instantanément sur le réseau et vérifiée par les mineurs. Les mineurs travaillent constamment pour confirmer les transactions individuelles et les inclure dans le prochain bloc de transactions de la chaîne. Une fois qu'un nouveau bloc est vérifié, toutes les transactions qu'il contient sont enregistrées en permanence sur la Blockchain. Les récompenses sont versées en Bitcoin aux mineurs qui confirment

les transactions et vérifient le bloc suivant comme moyen d'inciter à la productivité sur le réseau. Chaque partie qui participe au processus d'exploration de données possède une copie à jour identique de la Blockchain ou du grand livre public, qui est un enregistrement de toutes les transactions dans l'historique des bitcoins. La copie du livre de chaque partie est mise à jour chaque fois qu'un nouveau bloc est trouvé.

La devise l'unité de valeur que nous envoyons et recevons sur le réseau Bitcoin est également appelée bitcoin ou bitcoins. Le Bitcoin est complètement numérique, ce qui signifie que nous ne pouvons pas le tenir physiquement dans notre main. Il est également portable, divisible, fongible et irréversible [44].

3.2 Ethereum

En 2013, Vitalik Buterin, programmeur et cofondateur du magazine Bitcoin, a fondé Ethereum, il souhaitait un Blockchain plus volatile, qui n'était pas uniquement utilisé pour les monnaies. En 2015, il a lancé Ethereum comme une deuxième Blockchain publique, qui peut enregistrer des contrats, des emprunts, ..., etc [45]. Ethereum est un réseau de Blockchain publique distribué qui vise à exécuter le code de programmation de n'importe quelle application décentralisée.

Ethereum permet aux développeurs de créer et de déployer des contrats intelligents, ainsi que d'émettre leur propre crypto-monnaie directement sur la Blockchain de l'Ethereum, évitant ainsi aux développeurs de devoir créer une nouvelle Blockchain pour les services qu'ils proposent. Cela ne fait pas seulement économiser le temps nécessaire aux développeurs pour créer une Blockchain, mais il les permet également de profiter de la sécurité et de la décentralisation de l'Ethereum qui ne sont pas inhérentes à toutes les blockchains [46].

Ethereum peut être considéré comme une Blockchain avec un langage de programmation intégré, ou comme un ordinateur globalisé, basé sur le consensus, sur lequel les applications s'exécutent parce qu'elles valorisent les avantages offerts par Ethereum par rapport à ceux proposés par un serveur normal [47].

3.3 smart contract

Un contrat intelligent est un logiciel auto-imposé géré par un réseau d'ordinateurs P2P. Les contrats intelligents sont des outils de gestion des droits qui fournissent un cadre de coordination et d'application pour les accords entre les participants au réseau, sans avoir besoin de contrats juridiques traditionnels. Ils peuvent être utilisés pour formaliser des accords simples entre deux parties, les statuts d'une organisation, ou pour créer des jetons [48].

Un contrat intelligent est un accord auto-exécutoire intégré dans un code informatique géré par une Blockchain. Le code contient un ensemble de règles selon lesquelles les parties à ce contrat intelligent conviennent d'interagir entre elles. Si et quand les règles prédéfinies sont respectées, l'accord est automatiquement appliqué. Les contrats intelligents fournissent des mécanismes pour gérer efficacement les actifs à jetons et les droits d'accès entre deux ou plusieurs parties. Les valeurs sous-jacentes et les droits d'accès qu'ils gèrent sont stockés sur une Blockchain, qui est un grand livre transparent et partagé, où ils sont protégés contre la suppression, la falsification et la révision. Les contrats intelligents offrent donc un moyen public

et vérifiable d'intégrer les règles de gouvernance et la logique métier dans quelques lignes de code, qui peuvent être auditées et appliquées par le consensus majoritaire d'un réseau P2P [48].

3.4 CHAIN

Emplacement : San Francisco, Californie
Comment il utilise la Blockchain ? Chain construit des infrastructures de Blockchain cloud pour les services financiers. Les registres cryptographiques de la société de San Francisco aident les institutions financières à gérer de manière sûre et efficace le transfert de crypto-monnaies [49].
Chain Financial résout le problème des fiat via notre consortium Fiat Exchange Blockchain (FEB). Le FEB intègre la conformité, l'identité et la traçabilité à un niveau fondamental et peut évoluer pour prendre en charge des milliers de transactions par seconde. Le FEB permet aux capitaux détenus dans les banques traditionnelles de circuler vers et depuis les services basés sur la Blockchain sans que chaque service ne doive " réinventer la roue " - le FEB fournit l'infrastructure, les processus de conformité et les interfaces bancaires hors du boîte. Les relations réglementaires et bancaires multi-juridictionnelles permettent aux services financiers fondés sur notre technologie de fonctionner à l'échelle mondiale dès le premier jour. Le protocole FEB permet de créer efficacement des instruments financiers, puis de les négocier à l'aide de monnaies fiduciaires, dans la Blockchain. L'identité, la traçabilité et la lutte contre le blanchiment d'argent sont des caractéristiques essentielles, et non une réflexion après coup [50].

3.5 OCULAR

Emplacement : Los Angeles, Californie.
Utilisation de la Blockchain : la plate-forme de conformité anti-blanchiment d'Ocular exploite la sécurité activée par la Blockchain pour garantir que les données ne peuvent pas être manipulées. La technologie utilise des systèmes biométriques pour scanner le visage des personnes qui demandent un passeport, un permis de conduire et d'autres pièces d'identité délivrées par le gouvernement. En consultant les systèmes biométriques sur les chaînes de blocs, les gouvernements peuvent plus facilement attraper des voleurs d'identité à la recherche de faux passeports, certificats et pièces d'identité d'autres pays [49].

3.6 VOATZ

Emplacement : Boston, Massachusetts.
Comment il utilise la Blockchain ? Voatz est une plateforme de vote mobile qui fonctionne sur la Blockchain. Le système de sécurité biométrique crypté permet de voter en toute sécurité sur un appareil mobile de n'importe où dans le monde sans crainte de piratage ou de corruption de données. La Virginie-Occidentale est l'un

des premiers États à utiliser la plate-forme de l'entreprise pour recueillir les votes des militaires et des voyageurs éligibles à l'étranger lors des élections [49].

la startup basée à Boston, qu'il a cofondée et dirigée, a fourni une plateforme de vote mobile. En mars 2018, avait testé avec succès la nouvelle technologie pour permettre aux militaires américains en poste à l'étranger de voter en toute sécurité aux élections primaires de Virginie-Occidentale. Deux comtés de Virginie-Occidentale avaient participé au premier test. Treize personnes ont voté à partir de leur téléphone portable, une alternative beaucoup plus pratique que les autres options disponibles pour les membres du service à l'étranger. Le tout premier électeur de Virginie-Occidentale à utiliser l'application l'a appelée «lisse». Deux douzaines de comtés de Virginie-Occidentale se préparaient à faire du vote mobile via Voatz une option pour leurs citoyens vivant à l'étranger lors des élections générales prévues en novembre [51].

La platforme Voatz utilise deux blockchains privées autorisées construites à l'aide d'HyperLedger, une collection d'outils de Blockchain open source développés par Linux Foundation. Le premier est une «chaîne d'identité» et le second est la «chaîne de vote». Sur la base d'une liste électorale vérifiée créée par les organisateurs des élections, les électeurs doivent d'abord confirmer leur identité et obtenir un «jeton d'identité». Avec des jetons d'identité, les électeurs peuvent effectuer des transactions sur la «chaîne de vote». Chaque bulletin de vote le choix agit comme un destinataire sur la chaîne de vote, et chaque «vote» est la transaction d'un jeton allant de l'électeur à un destinataire, représentant ainsi un vote émis pour cette option. Tous les appareils mobiles et les tablettes anonymisent l'identité des utilisateurs avant de soumettre des votes. Une fois les votes exprimés, la transaction (vote) est immuable et stocké en toute sécurité sur le registre de la Blockchain [52].

3.7 STEEM

Emplacement : Austin, Texas.
Comment il utilise la Blockchain ? Steem est une plate-forme de médias sociaux soutenue par la Blockchain. Sa communauté «Proof-of-Brain» utilise des jetons comme incitations, encourageant les gens à créer du contenu original. Le nombre de jetons distribués est basé sur le nombre de votes positifs que chaque article reçoit. Steem a payé plus de 40 millions de dollars en jetons aux créateurs [49].

Steemit est une plaque-forme qui permet aux éditeurs de monétiser leur contenu qui fonctionne de la même manière que de nombreux autres réseaux sociaux. La communauté construite permet aux utilisateurs de récompenser les autres utilisateurs pour le contenu qu'ils publient en utilisant la Blockchain et la crypto-monnaie de Steem. Publier du contenu sur Steemit.com reste gratuit. La monnaie est ensuite distribuée aux producteurs de contenu en fonction du nombre de votes qu'ils obtiennent pour les messages qu'ils publient. En construisant une communauté en ligne qui est récompensée en crypto-monnaie pour avoir partagé leur contenu, Steemit redéfinit le monde des médias sociaux et construit une économie sociale en pleine croissance car ce sont les utilisateurs qui tirent des avantages [54].

Comment ça fonctionne ? Chaque jour, le réseau Steemit crée de nouvelles unités Steem et les distribue à ses utilisateurs. Les utilisateurs peuvent ensuite échan-

ger ses unités sur le marché libre contre le Bitcoin, d'autres crypto-monnaie, ou contre des Fiats. Steemit permet virtuellement à n'importe qui d'écrire sur des sujets intéressants et de gagner de l'argent [53] [54].

4 Le domaine médical

Le secteur de la santé est un secteur particulièrement prometteur pour la technologie Blockchain. Celle-ci permettrait de nombreuses applications sur la gestion, la sécurité, et l'usage des données patients.

4.1 La Blockchain comme registre patient distribué

Plusieurs acteurs de la santé s'intéressent de près à la création d'un registre patient distribué s'appuyer sur une architecture Blockchain. De nos jours, il est difficile de visualiser de manière claire toutes les données liées à un patient et accumulées au cours de son parcours de soins. Ces informations proviennent habituellement de sources très variées, comme les médecins de ville, l'hôpital, les assurances, les pharmaciens ou les laboratoires d'analyses médicales. Lors de l'admission d'un patient à l'hôpital, les professionnels de santé n'ont en effet pas toujours accès à son historique et n'ont pas une visibilité complète sur les traitements qu'il prend, sur l'historique de sa maladie ou sur ses antécédents familiaux [55].

L'idéal serait donc d'avoir une liste qui répertorie tous les lieux où se trouvent les données médicales du même patient afin de pouvoir rapidement les récupérer. Cette liste serait accessible, avec l'accord du patient, à tout professionnel de santé qui en ferait la demande. Ainsi, plutôt que de n'avoir accès qu'à la base de données de l'établissement où l'on se trouve, on pourrait avoir accès à toutes les sources d'informations dispersées dans toutes les bases de données du réseau. La technologie Blockchain apporte justement cette solution sous la forme d'un registre distribué et sécurisé qui permet au patient non seulement d'avoir une visibilité sur ses données, mais aussi d'en contrôler les accès et donc le patient est le point central d'un réseau [55]. Et d'après [1] le dossier patient devrait ainsi :

- Etre entièrement digital.
- Etre partagé, avec l'accord du patient, avec les acteurs de son choix.
- Permettre de retracer rapidement l'historique des conditions et traitements du patient.
- Etre mis à jour en temps réel par les professionnels de la santé travaillant sur le dossier du patient ou par les smart devices que le patient porte (exemple : smart Watch).

Un système reposant sur une Blockchain pourrait par exemple cocher certaines de ces conditions. Les bénéfices seraient alors nombreux :

- Les données du patient ne seraient pas systématiquement demandées lors de la prise en charge du patient pour un traitement.
- Les différents acteurs de la santé (docteurs, hôpitaux, recherche, ..., etc.) travailleraient sur une même plateforme, réduisant les problèmes liés à l'interopérabilité de leurs systèmes,
- Les assurances pourraient déclencher le remboursement des frais de santé dès l'inscription d'actes remboursables dans le dossier du patient.

- Les pharmaciens et compagnies pharmaceutiques pourraient optimiser leurs stocks de médicaments en temps réel, voire anticiper une livraison à domicile dès une prescription créée.
- Les services d'interventions (exemple : urgences) pourraient avoir accès à des informations vitales des patients lorsque ceux-ci ne sont plus en capacité de leur répondre.

PassCare (passeport numérique)

Lancé en 2018, PassCare est un passeport numérique de santé personnel développé par la start-up InnovHealth pour "permettre aux patients de récupérer et maîtriser toutes leurs informations de santé et les partager avec les professionnels de santé de leur choix", a expliqué à TICsanté le fondateur de la jeune pousse, le Dr Adnan El Bakri [56]. Le patient remet son PassCare au professionnel de santé qui, après avoir entré le numéro de clé unique du patient sur la plateforme web PassCare, peut accéder à sa fiche médicale via l'application web dédiée et y ajouter les informations relatives à sa consultation [56].

Le patient peut ainsi accéder à ses informations de santé, les enregistrer dans un coffre-numérique dont il est le seul à détenir la clé (via son numéro de clé unique) et les partager avec des professionnels de son choix, qui peuvent donc enrichir le PassCare sans installer d'outils supplémentaires ou installer un logiciel [56]. Les données sont chiffrées et anonymisées pour être ensuite stockées sur la plateforme PassCare et sécurisées par la Blockchain privée [56].

Concrètement, grâce à l'IA, le PassCare propose aux patients des programmes de prévention, des campagnes de dépistage ciblées, une gestion de sa vaccination, un suivi de sa maladie chronique ou encore des entretiens nutritionnels, via des notifications par SMS ou push sur l'application web [56].

FIGURE 2.1 – passcare [56]

4.2 La Blockchain dans la supply chain pharmaceutique

Problématique d'envergure dans l'industrie pharmaceutique et la logistique santé, la fraude de médicaments concerne tous les acteurs de la supply chain pharma. Selon l'OMS, près de 15% de médicaments falsifiés sont en circulation dans le monde. Ce fléau mondial entraîne des conséquences graves voire dramatiques sur la santé des patients. En effet, ils ne répondent à aucune des exigences de qualité, d'efficacité et de sécurité, entraînant ainsi près de 800 000 décès chaque année. Parallèlement à l'impact catastrophique sur la santé publique, la contrefaçon engendre des coûts

conséquents. Le marché de la contrefaçon de médicaments génère en effet 200 milliards de dollars par an et représente un manque à gagner de 10,2 milliards d'euros pour le secteur pharmaceutique européen [56].

«la Blockchain, grâce à sa transparence et son inaltérabilité, peut également être utilisée en tant qu'outil de traçabilité et de vérification d'authenticité pour les médicaments, les ordonnances médicales ou encore les brevets. L'utilisation d'une Blockchain pourrait aider à lutter contre ce fléau, en enregistrant les empreintes de chaque action liée à un médicament, lors des différentes phases du processus de fabrication et distribution », explique l'entreprise Blockchain Partner dans son étude « Blockchain et Santé » [57].

La technologie Blockchain apporte donc un réel avantage en termes de traçabilité des médicaments : elle permet un suivi des produits dans la chaîne de distribution, créant un circuit hermétique, imperméable aux produits contrefaits [55].

Il permettra également aux patients de contrôler l'origine de leurs médicaments :

- Les laboratoires pharmaceutiques pourraient créer un registre de médicaments issus de leurs laboratoires, chaque boîte de médicament étant enregistrée dans la chaîne [1].
- Les magasins revendant les médicaments ou pharmaciens pourraient vérifier à réception de stocks de médicaments que ceux-ci proviennent bien de laboratoires valides ; les informations liées à chaque médicament sont mises à jour dans la chaîne pour indiquer que le médicament a changé d'endroit [1].
- Le consommateur final achetant le médicament peut vérifier l'intégralité du parcours de son médicament. Le pharmacien peut retrouver son patient en cas de rappel d'un lot de médicament [1].

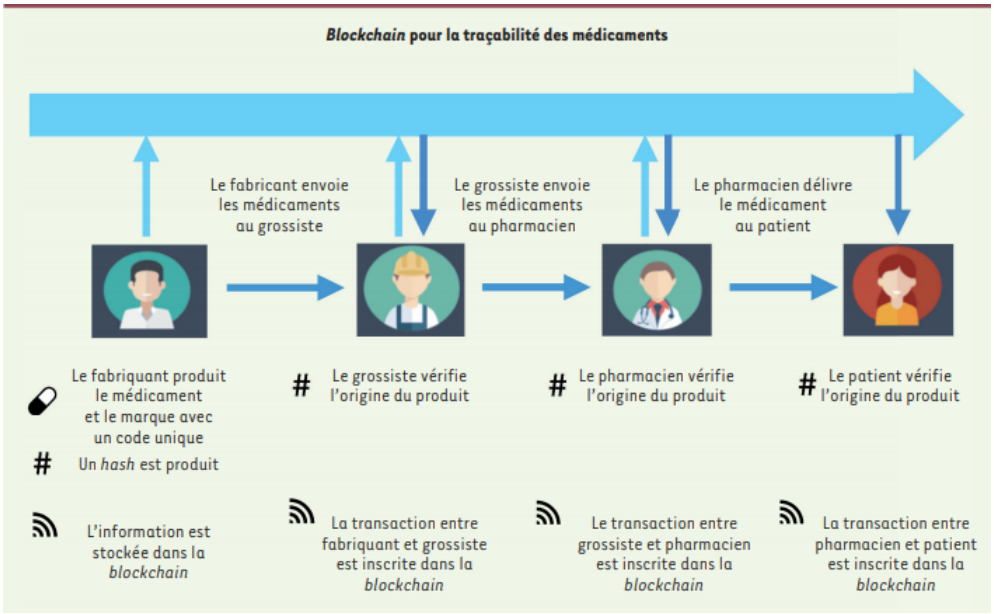

FIGURE 2.2 – Blockchain pour la traçabilité des médicaments [55]

.

Blockpharma

Blockpharma est un service de traçabilité des médicaments reposant sur la technologie Blockchain qui permet de vérifier l'authenticité d'un médicament. L'application Blockpharma permet au consommateur de vérifier instantanément l'authenticité de la boîte de médicament qu'il achète. Blockpharma s'appuie sur les toutes dernières technologies de Machine Learning pour améliorer la détection des cas de contrefaçons. Les fondateurs de BLOCKPHARMA sont Fanny Roseau et Vincent Riffier [58].

4.3 La Blockchain pour les donnée génétique

Avec le développement à venir du séquençage du génome humain, l'intérêt porté aux données génétiques est appelé à se démultiplier au cours des prochaines années et décennies. Or de nombreuses problématiques liées à la privacy et la sécurité de ces données se présentent, pour lesquelles l'utilisation de la Blockchain pourrait s'avérer intéressante. Mais, il existe un risque non négligeable que ces données soient exploitées par des entreprises ou des gouvernements mal intentionnés. La Blockchain pourrait justement assurer la privacy des données génétiques tout en permettant d'exploiter ces dernières à des fins de recherche [59].

Nebula Genomics

Start-up lancé en février dernier par le généticien Georges Church, vise à dynamiser le marché émergent des données génétiques. Nebula Genetics propose de séquencer les patrimoines génétiques individuels en conciliant l'intérêt des propriétaires des données et l'intérêt des industriels. L'idée : les données issues des séquençages sont mises à la disposition des industriels via une Blockchain et les propriétaires reçoivent, en contrepartie de l'utilisation des données, une rémunération en cryptomonnaie. En théorie, tout le monde y gagne, le marché est dynamisé et les données génétiques sont protégées [60]. Les données sont protégées et l'accès est sécurisé. Les propriétaires des données sont anonymes et l'identité des acheteurs est apparente.

Le réseau Nebula agrège les données génétiques et organise la concordance entre les besoins des propriétaires des données et ceux des acheteurs des données. La mise au point de standards et le recours à des supports digitaux et à l'intelligence artificielle facilitent les transactions : "through decentralized data storage, flexible utilisation of available computing power and efficient file transfers enabled by space-efficient data encoding, the Nebula network will absorb the fothcoming data explosion" [60].

5 Comparaison entre les applications

La technologie Blockchain peut être considérée comme une nouvelle révolution numérique, elle est sur le point de coloniser tous les secteurs de la vie. Le tableau ci-dessus présente une liste de certaines applications qui existent déjà et qui touchent plusieurs domaines.

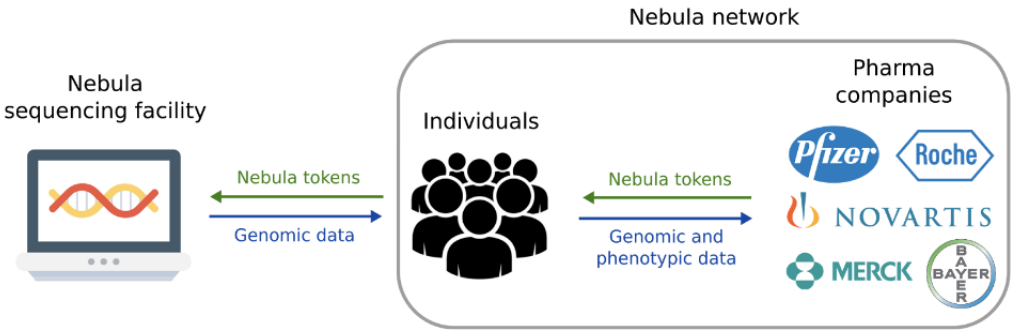

FIGURE 2.3 – genitique [18]

.

Ces applications sont divisées en deux parties à savoir : les applications intelligentes et non intelligentes. La plupart des applications intelligentes utilisent la Blockchain et l'apprentissage automatique, tandis que d'autres applications dépendent de la Blockchain et d'autres techniques.

Concernant le secteur de la santé, il est probable qu'il soit le secteur le moins avancé dans l'exploration de la technologie Blockchain, en raison des restrictions imposées à ce secteur telles que le stockage des données personnelles et médicales. Cependant, il existe des applications en cours de développement.

Type d'application	**Les Applications**	**Techniques et approches utilisées**	**Leur rôle**	**Vise à**
Intelligent	FINALZE	o La Blockchain o apprentissage automatique	améliorer les infrastructures civiles	rendre les processus cruciaux plus efficaces
	BEXT360	o La technologie cloud o les robots o la Blockchain o reconnaissance d'image o apprentissage automatique	améliorer la transparence et l'efficacité de la chaîne d'approvisionnement dans les industries du café, du bois, des fruits de mer et des minéraux	o évaluer les cultures qui sont soumises dans les installations de production. o classer la note et attribuer un prix.
	BURSTIQ	o la Blockchain o le big data o l'apprentissage automatique o l'intelligence collaborative	gérer de manière holistique les données d'un patient	o lutter contre la crise des opioïdes o améliorer la sécurité avancée des mégadonnées o réduire les coûts des soins de santé
	NETOBJEX	o la Blockchain o l'IoT o l'IA o La technologie cloud	fait la plateforme d'infrastructure de ville intelligente pour tout alimenter, des appareils connectés aux produits.	o améliorer le suivi logistique, o la détection des pannes en temps réel o l'authentification des données et des appareils
	SYSTÈMES HANNAH	o le deep learning o la Blockchain o outil de cartographie, o un tableau de bord d'informations	la véhicule autonome peut rapidement absorber , interpréter et stocker en toute sécurité les données.	o prédit les informations routières o prend en compte les notifications carte et les encombrements
	NEUREAL	o l'IA o la Blockchain o la technologie cloud	moteur de prédiction pour tout prévoir.	o casser un hachage inutile o cherche à donner à l'humanité le pouvoir de voir l'avenir o prédire la trajectoire exacte des ouragans
Non intelligent	Bitcoin	o Blockchain o cryptographie asymétrique	Présente un réseau de paiement novateur et une nouvelle forme d'argent.	o personne ne possède ni ne contrôle Bitcoin et tous peuvent s'y joindre o assurer le suivi des transactions et soldes o permet de traiter entre nous
	Ethereum	o contrats intelligents o Blockchain o langage de programmation appelé «Solidity»	Sert à une plate-forme globale et open-source pour des applications décentralisées.	o enregistrer des contrats, des emprunts o exécuter le code de programmation de n'importe quelle application décentralisée. o créer et déployer des contrats intelligents
	contrat intelligent	o La Blockchain o hachage cryptographique o Tolérance aux pannes	accord auto-exécutoire géré par un réseau d'ordinateurs P2P	o fournir un cadre de coordination et d'application pour les accords entre les participants au réseau
	CHAÎNE	o Le protocole FEB o La Blockchain o La technologie cloud	construit des infrastructures de Blockchain cloud pour les services financiers.	o résoudre le problème des fiat via notre consortium Fiat Exchange Blockchain o créer efficacement des instruments financiers
	OCULAIRE	o la Blockchain	Sert à une plaque-forme anti-blanchiment	o garantir que les données ne peuvent pas être manipulées o attraper des voleurs d'identité o la recherche de faux passeports
	VOATZ	o la Blockchain o chaîne d'identité o chaîne de vote	Sert à une plateforme de vote mobile	o voter en toute sécurité
	STEEM	o la Blockchain	Sert à une plaque-forme de médias sociaux	o permet à n'importe qui d'écrire sur des sujets intéressants et de gagner de l'argent

Type d'application	**Les Applications**	**Techniques et approches utilisées**	**Leur rôle**	**Vise à**
Médical	**PassCare**	o La Blockchain	Présente un passeport numérique de santé personnel	o propose aux patients des programmes de prévention o des campagnes de dépistage ciblées o une gestion de sa vaccination suivi de maladie chronique ou encore des entretiens nutritionnels
	Blockpharma	o Machine Learning o La Blockchain	permet d'une service de traçabilité des médicaments	o permet de vérifier l'authenticité d'un médicament
	Nebula Genomics	o les supports digitaux o l'intelligence artificielle o la Blockchain	dynamiser le marché émergent des données génétiques	o Nebula agrège les données génétiques o organise la concordance entre les besoins des propriétaires des données et ceux des acheteurs des données

6 Conclusion

En conclusion, cette liste non exhaustive des applications potentielles de la Blockchain montre l'impact réel sur l'organisation et l'efficience des systèmes. Il est important de noter que la combinaison de la technologie Blockchain et de l'intelligence artificielle reste un domaine largement inconnu. Même si la convergence des deux technologies a reçu sa juste part d'attention scientifique, les projets consacrés à cette combinaison révolutionnaire sont encore rares.

Chapitre 3

Conception d'une approche Blockchain pour un Dossier Médical Partagé Sécurisé

1 Introduction

Dans le secteur de la santé, la technologie Blockchain a la capacité d'agir sur le partage de données cliniques, en stockant les données elles-mêmes ou en indiquant les personnes qui peuvent accéder à ces données. Ce qui fournit aux patients la preuve et la certitude que le dossier ne peut pas être modifié, et ainsi assurer la confidentialité.

Dans ce chapitre, nous présentons les entités du système : **D**ossier **M**édical **P**artagé **S**écurisé (**DMPS**), qui interagissent pour fournir le service de contrôle et de protection des données dans l'échange d'informations sur la santé. Nous mettons en évidence le rôle de la Blockchain dans le processus et décrivons brièvement les blocs créés pour sécuriser davantage le processus. Donc, on va présenter l'architecture générale de notre système **DMPS**, ainsi que sa conception détaillée appliquée au domaine médical.

2 Architecture globale

Dans le domaine médical nous allons intégrer dans notre proposition conceptuelle des acteurs dans la prise en charge d'un malade. Nous considérons le médecin, le pharmacien, l'analyste du laboratoire,... etc.

2.1 Étapes de développement

Le développement d'une application Blockchain nous oblige également à délimiter la portée et le but de l'application. Les étapes de développement d'une application Blockchain sont réparties comme suit :

Étape 1 : Clarification de l'idée

1. La première question à laquelle il faut répondre est :

Pourquoi on utilise Blockchain ?

Les principales raisons pour lesquelles il est préférable d'utiliser la Blockchain sont :

La sécurité : la technologie Blockchain est plus sécurisée que les systèmes de base de données centralisés. Cela signifie qu'une Blockchain est beaucoup moins susceptible d'être la cible d'une tentative de piratage informatique, car il n'y a pas de point de défaillance unique. Les informations médicales du patient seront plus sécurisées, ce qui permet au patient non seulement d'avoir une visibilité sur ses données, mais aussi d'en contrôler les accès.

L'interopérabilité : La Blockchain permet d'améliorer l'interopérabilité entre les cliniques, les hôpitaux et les autres prestataires de services de santé. Donc, les fournisseurs de services pourront travailler ensemble sur un seul système.

Transparence : Les systèmes Blockchain peuvent également donner aux patients des niveaux de transparence renforcés sur leurs propres informations de santé, il est aussi possible d'offrir un niveau de sécurité supplémentaire contre les erreurs humaines et les falsifications intentionnelles.

2. La deuxième question est :

Est-il nécessaire d'utiliser Blockchain ?

Évidemment, la réponse est affirmative. Et pour vous montrer pourquoi on a réellement besoin d'une Blockchain, l'arbre de décision de la figure 3.1 vous donnera toutes les réponses aux questions que vous vous posez. Tout d'abord,

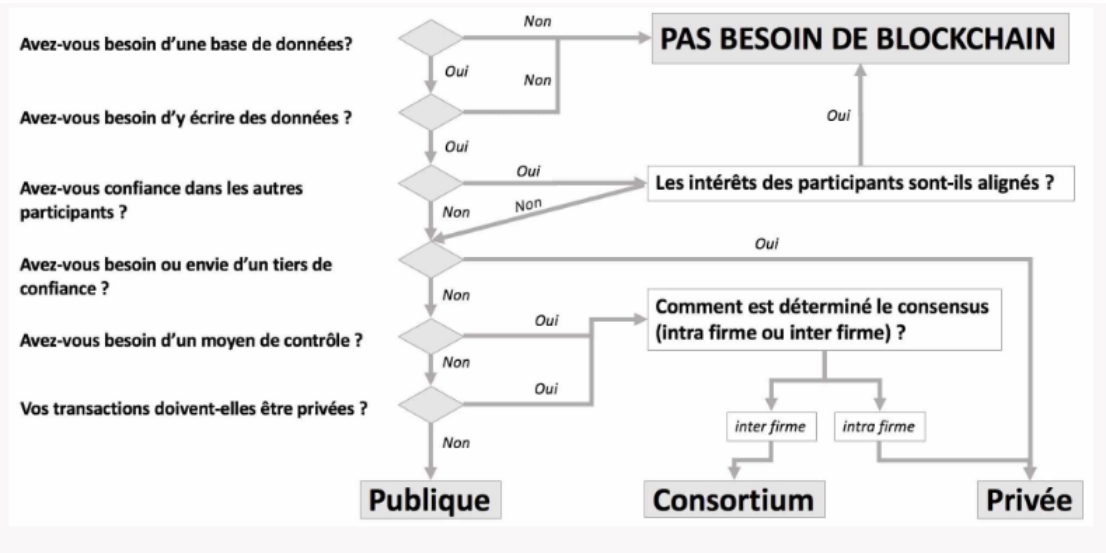

FIGURE 3.1 – Arbre de décision

on a besoin d'une base de donnée où on écrit, et donc on stocke, les informations médicales des patients telque les ordonnances, les analyses, les radios,... etc.

Ensuite, la Blockchain a du sens pour notre système car on n'a pas de confiance dans les autres participants. Finalement, et puisque on a besoin d'un moyen de contrôle centralisé, on a orienté vers une Blockchain privée.

Étape 2 : Identification du problème et objectif

Le problème c'est qu'il est difficile de visualiser toutes les données médicales liées à un patient. Ces données proviennent de sources très variées, comme les médecins, les hôpitaux, les assurances, les pharmaciens ou les laboratoires d'analyses médicales. Lors de l'admission d'un patient à l'hôpital. Les professionnels de santé n'ont en effet pas toujours accès à son historique, il n'y a pas de visibilité complète sur les traitements qu'il prend, l'histoire de sa maladie, et aussi ses antécédents familiaux.

Et donc notre système vise à résoudre ce problème en suivant les antécédents médicaux et l'état de santé actuel du patient. Il prend les examens, les analyses et les chirurgies, et donc il mentionne les traitements nécessaires.

Étape 3 : Identification des acteurs du système DMPS

Évidemment, les acteurs de notre système sont :

Les utilisateurs : sont, d'une part, les médecins, les hôpitaux, les assurances, les pharmaciens, les laboratoires d'analyses médicales,... etc. Et d'un autre côté, les patients.

Les organisateurs : et on précis ici l'administrateur du système.

Étape 4 : Identification du mécanisme de consensus le plus approprié

Puisque on a choisi la plateforme privée pour notre système, les nœuds du système sont connus et validés par l'administrateur pour le staff médical et par ce dernier pour les patients. Ainsi, le nombre de nœuds distribués est faible par rapport à Bitcoin, il n'est donc pas nécessaire de mettre en place un mécanisme de PoW très gourmand (en termes de consommation d'énergie). On préfère alors déployer un mécanisme de PoW plus léger.

Dans ce qui suit, on présente l'architecture globale du système DMPS.

2.2 Architecture globale du système DMPS

L'architecture proposée de notre DMPS se compose de trois entités illustrées par la figure Fig 2.2 et décrites comme suit.

- **Les acteurs du DMPS**, incluant les :
  - ▷ **Les utilisateurs**, qui englobent tous ceux qui ont besoin d'accéder aux données pour accomplir leurs tâches, y compris ici les médecins et les patients.

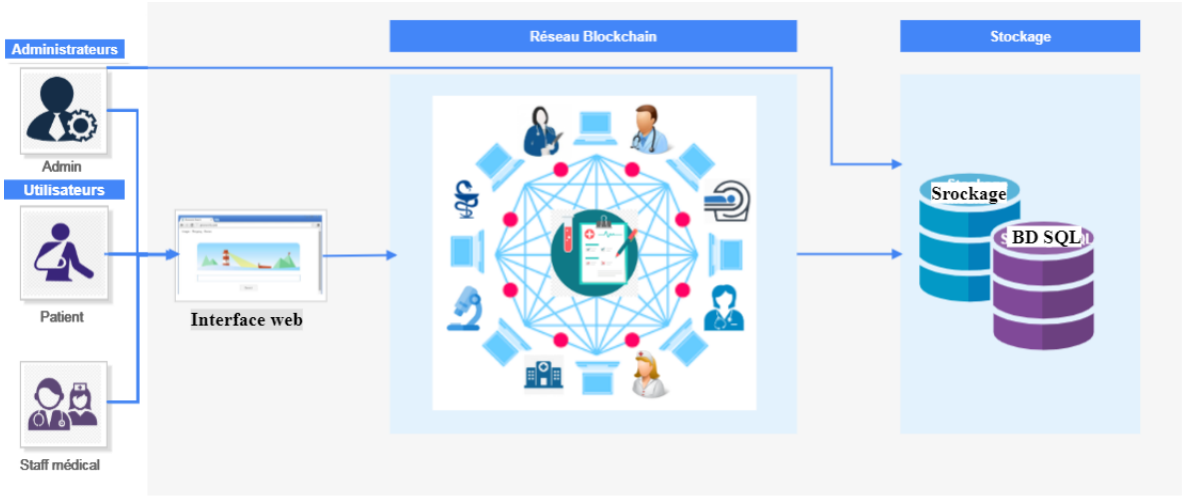

FIGURE 3.2 – Architecture globale du système DMPS

▷ **Les administrateurs**, comme des organisateurs du système DMPS.

- **Le stockage**, pour stocker et gérer les données médicales de manière distribuée et décentralisée. Le professionnel de santé a le plein contrôle des dossiers médicaux de ses patients. Alors qu'un patient peut seulement visualiser ses données sans avoir la main pour les modifier.

- **Le réseau Blockchain**, qui reçoit et stocke les journaux de consultation qui ont été traités par blocs, ainsi qu'il stocke les détails de chaque consultation.

3 Fonctionnement globale

Dans cette partie du chapitre, on va décrire les aspects de fonctionnement du système DMPS.

3.1 Organigramme fonctionnel du système DMPS

On commence par montrer l'organigramme fonctionnel du système proposé, Figure 3.1, en présentant les tâches accomplies par chacun de ses acteurs.

Au début, les professionnels de santé sont enregistrés dans le système et ont donc leurs propres comptes. Lorsqu'un patient se rend chez l'un des professionnels de santé, par exemple un médecin, ce dernier doit d'abord créer un compte via son propre compte pour ce patient, bien entendu s'il n'est pas déjà inscrit dans le système, et donc avoir un dossier médical. L'étape suivante consiste à ajouter ce patient à ses patients puis à accéder à son dossier afin d'en avoir une copie. À partir de là, le professionnel de santé devient capable de visualiser les différentes actions menées sur ce dossier par d'autres professionnels de santé, et d'ajouter également de nouvelles données médicales.

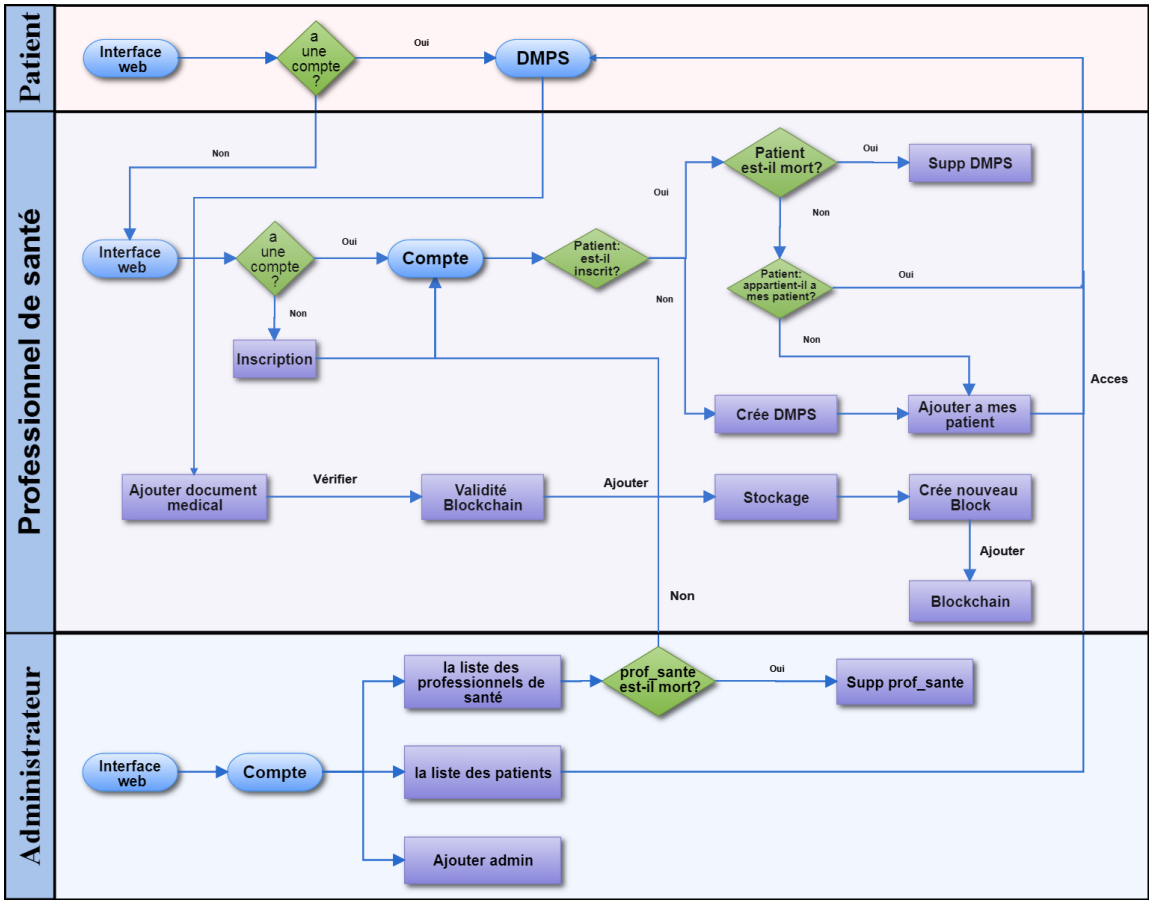

FIGURE 3.3 – Organigramme fonctionnel du système DMPS

Lors de l'ajout d'un nouveau document (ordonnance, radio, analyse, ... etc) à un dossier médical, le système doit tout d'abord vérifier la validité de la Blockchain. Ici, le système va détecter tout sort de violation pouvant arriver au dossier du patient. Et puisqu'il y a plusieurs copies de ce dossier dans le réseau Blockchain, les données peuvent être récupérées simplement, donc on récupère la validité du dossier. Après la tâche de validation, le document va être ajouté au dossier du patient en créant un nouveau bloc pour ce document. Enfin, le bloc va être ajouté après l'approbation de tout les professionnels de santé partageant le dossier du patient (faire l'ajout à la base de données du système et au réseau Blockchain).

Tandis qu'un patient ne peut que consulter son dossier médical et les divers actions effectuées sur celui-ci, visualiser ou modifier ses données personnelles.

L'administrateur DMPS peut accéder à tous les dossiers médicaux du patient, y compris leurs informations. Il peut également consulter les informations de tous les professionnels de santé et les listes de leurs patients. En cas de décès d'un professionnel de santé, l'administrateur a la main pour supprimer son compte du système. Vous pouvez avoir plusieurs administrateurs où l'ajout d'un administrateur ne peut être effectué que par un administrateur.

3.2 Diagrammes de séquence

Dans cette partie du chapitre, on présente les diagrammes de séquence pour définir les différentes interactions entre chacun des acteurs et les composants du système DMPS.

Diagramme de séquence Patient

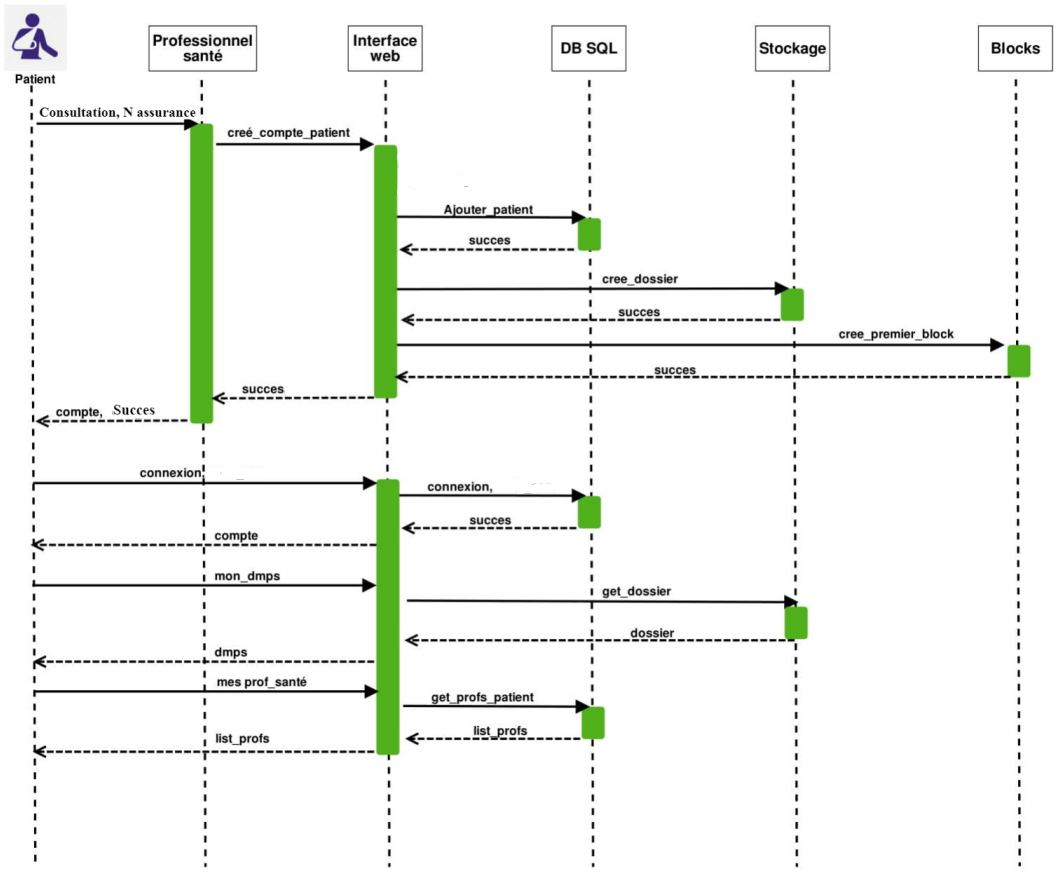

FIGURE 3.4 – Diagramme de séquence "**Patient**"

Comme vous pouvez le voir (Figure 3.4), le scénario d'inscription de patient se déroule par le professionnel de santé. La réussite de l'opération se traduit par la création d'un dossier médical (compte). Après l'inscription, le patient peut se connecter et donc accéder à son dossier et visualiser les actions effectuées sur celui-ci.

Diagramme de séquence Consultation

On spécifie ici la tâche de consultation du patient. Comme le montre Figure 3.5, le professionnel de santé doit tout d'abord accéder au dossier médical du patient, bien sûr après son authentification. Chaque consultation se termine par la création d'un nouveau bloc qui la décrit avec des nouveaux données qui la caractérisent comme un ordonnance, un radio, ... etc, et éventuellement les commentaires du professionnel du santé.

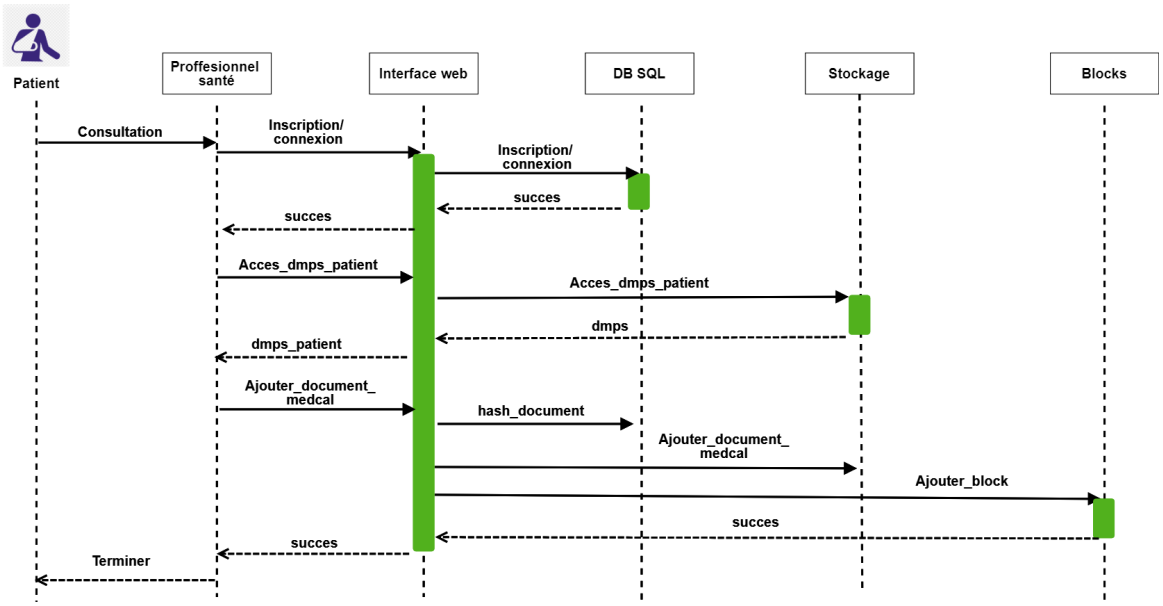

FIGURE 3.5 – Diagramme de séquence "**Consultation**"

Diagramme de séquence Professionnel de santé

Au contraire du patient, le professionnel de santé peut s'inscrire dans le système DMPS, voir Figure 3.6. En plus de l'enregistrement d'un nouveau patient dans le système DMPS, et de la tâche de consultation du patient, le professionnel de santé peut supprimer le dossier médical (compte) d'un patient décédé.

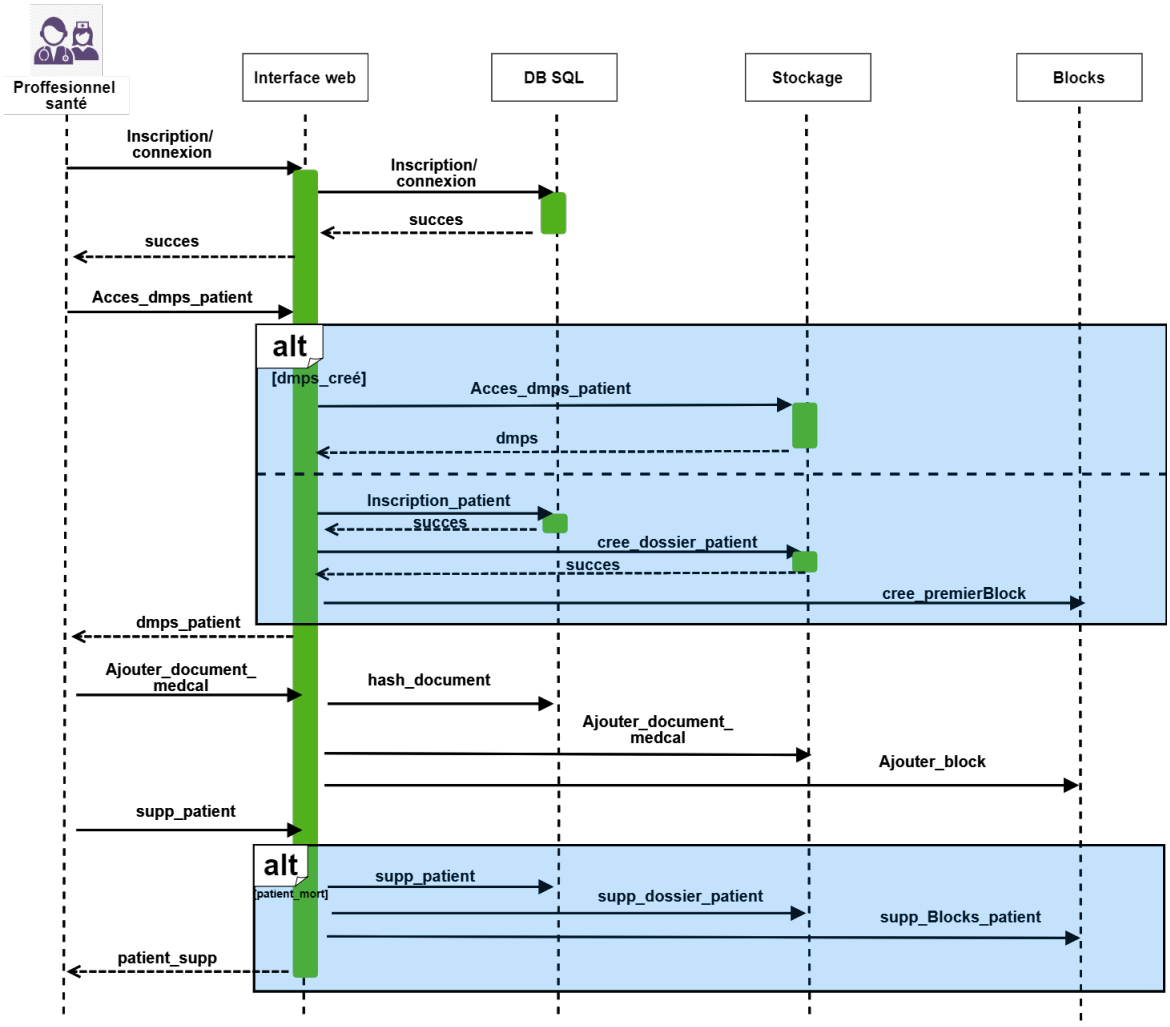

FIGURE 3.6 – Diagramme de séquence "**Professionnel de santé**"

Diagramme de séquence Administrateur

L'administrateur (Figure 3.7), comme les utilisateurs, est obligé de s'authentifier pour accéder au système DMPS. Et comme son nom l'indique, il a eu la main pour accéder à la liste des professionnels de santé et à leurs informations ainsi qu'à la liste des patients et de leurs dossiers médicaux, définir d'autres administrateurs, ou accéder à la Blockchain. De plus, lorsqu'un professionnel de santé est décédé, c'est l'administrateur qui peut supprimer son compte du système.

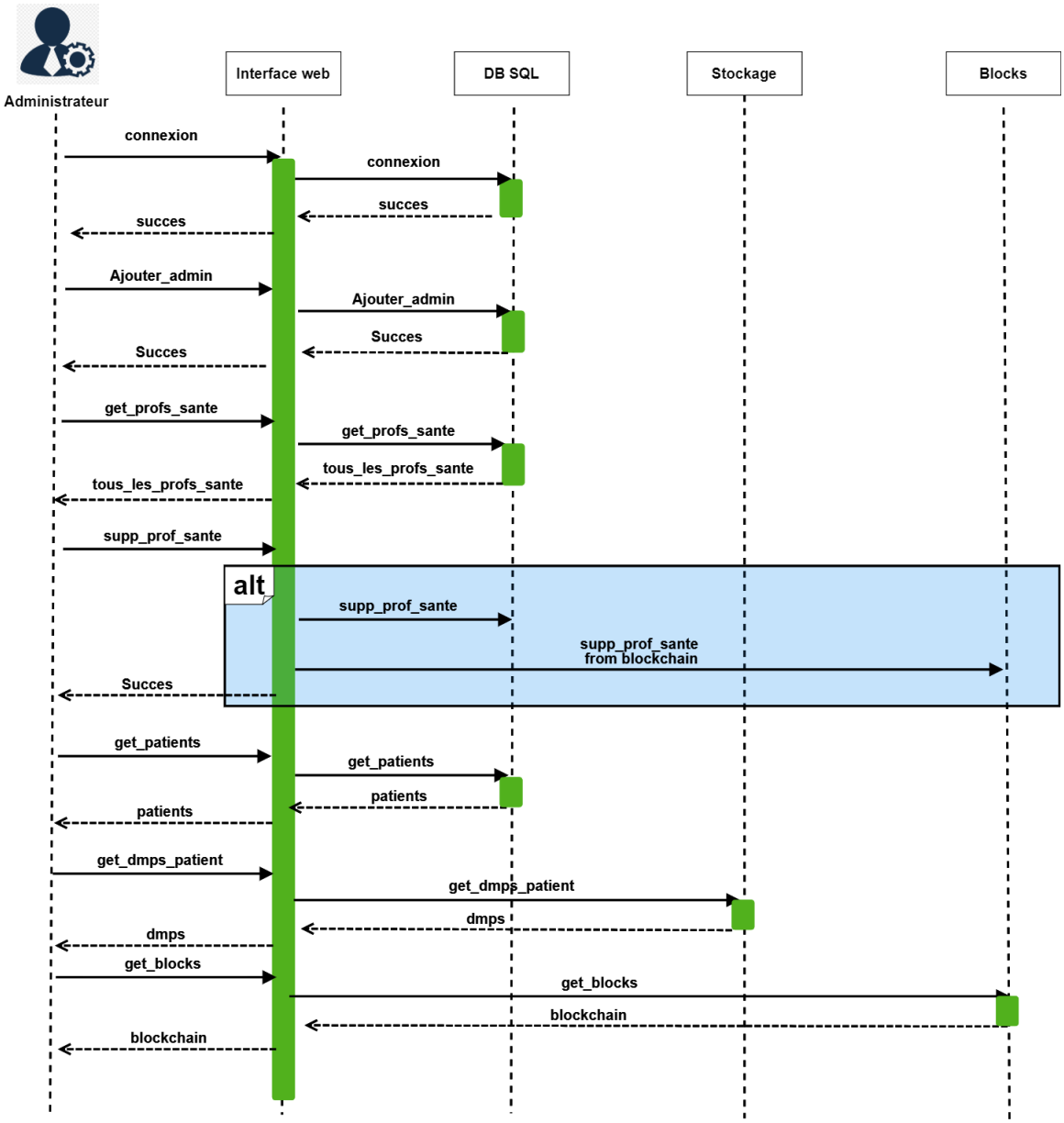

FIGURE 3.7 – diagramme de séquence "**Administrateur**"

4 Architecture de chaque sous système

Ici, le système est considéré comme un ensemble de modules, et donc on va décrire chacun d'eux.

4.1 Inscription

On spécifie ici le module d'**Inscription** pour ceux qui ont besoin d'utiliser DMPS : le professionnel de santé et le patient.

Inscription Professionnel de santé, grâce à une interface Web, le professionnel de la santé peut simplement s'inscrire au système DMPS en remplissant un formulaire et ainsi être enregistré dans la base de données du système.

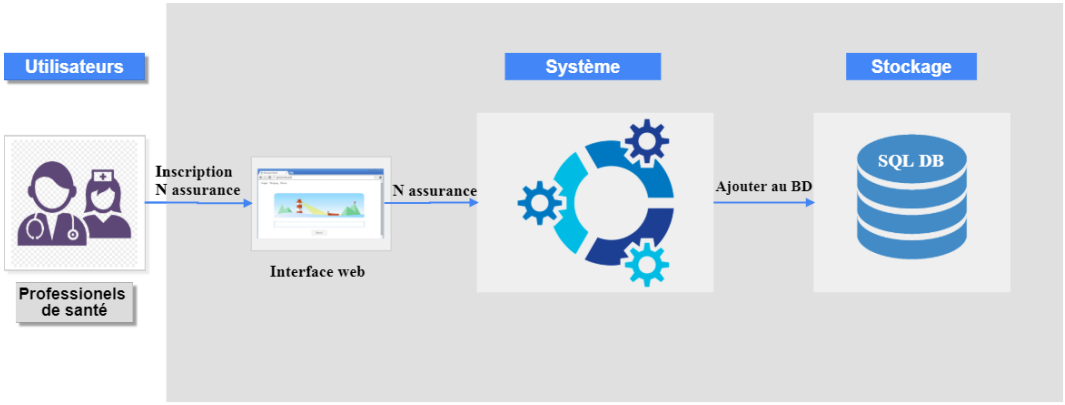

FIGURE 3.8 – Architecture module "**Inscription Professionnel de santé**"

Inscription Patient, de même, le patient peut avoir une compte dans la base de données du système mais avec l'aide d'un professionnel de santé qui l'enregistrera en se basant à son numéro d'assurance. l'enregistrement du patient s'accompagne de la création d'un dossier médical stocké dans le système.

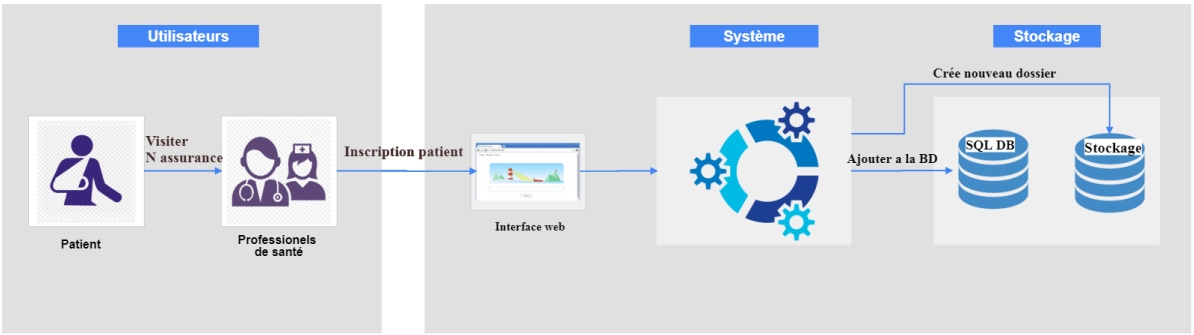

FIGURE 3.9 – Architecture module "**Inscription Patient**"

4.2 Administrateur

l'administrateur a une vue sur le système complet. A travers une interface web (Figure 3.10), il peut consulter l'espace de stockage du DMPS par visualiser les utilisateurs ainsi que les dossiers médicales des patients, comme il peut faire un accès au réseau Blockchain.

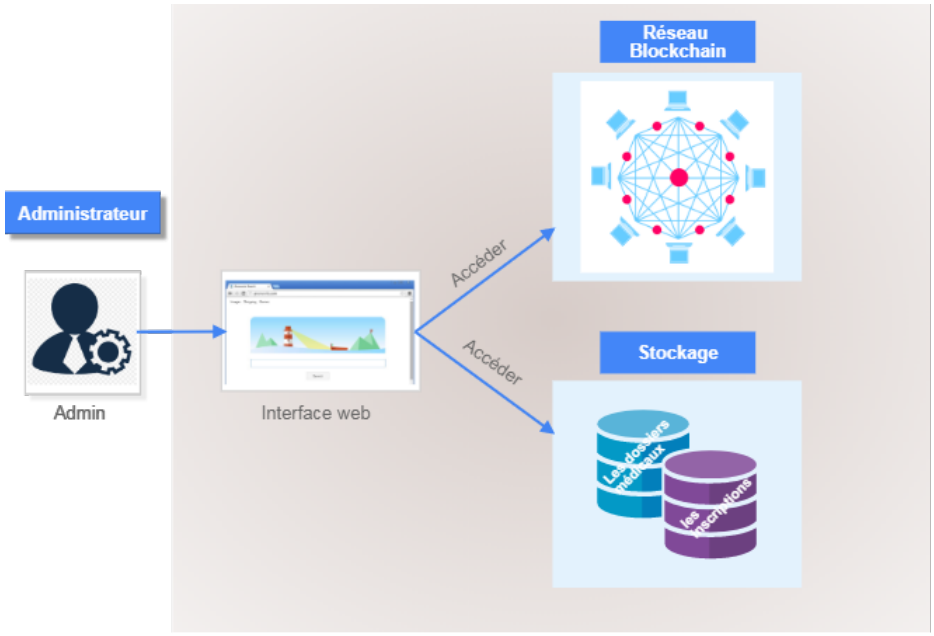

FIGURE 3.10 – Architecture module "**Administrateur**"

4.3 Réseau Blockchain

Les informations médicales sont stockées et partagées fréquemment entre divers participants concernés tels que les patients, les médecins, les prestataires de soins de santé, les pharmacies, les compagnies d'assurance et les chercheurs, entre autres (Figure 3.11). Le dossier médical contient des informations médicales hautement critiques et sensibles liées au patient qui doivent être stockées, partagées, traitées et accessibles en toute sécurité.

Ici, la Blockchain ajoute plus de transparence, car elle maintient un registre distribué entre toutes les entités impliquées dans le réseau. La Blockchain fournit un moyen fiable et sécurisé de partage de données et de mécanismes de gestion où toutes les parties sont au courant des transactions.

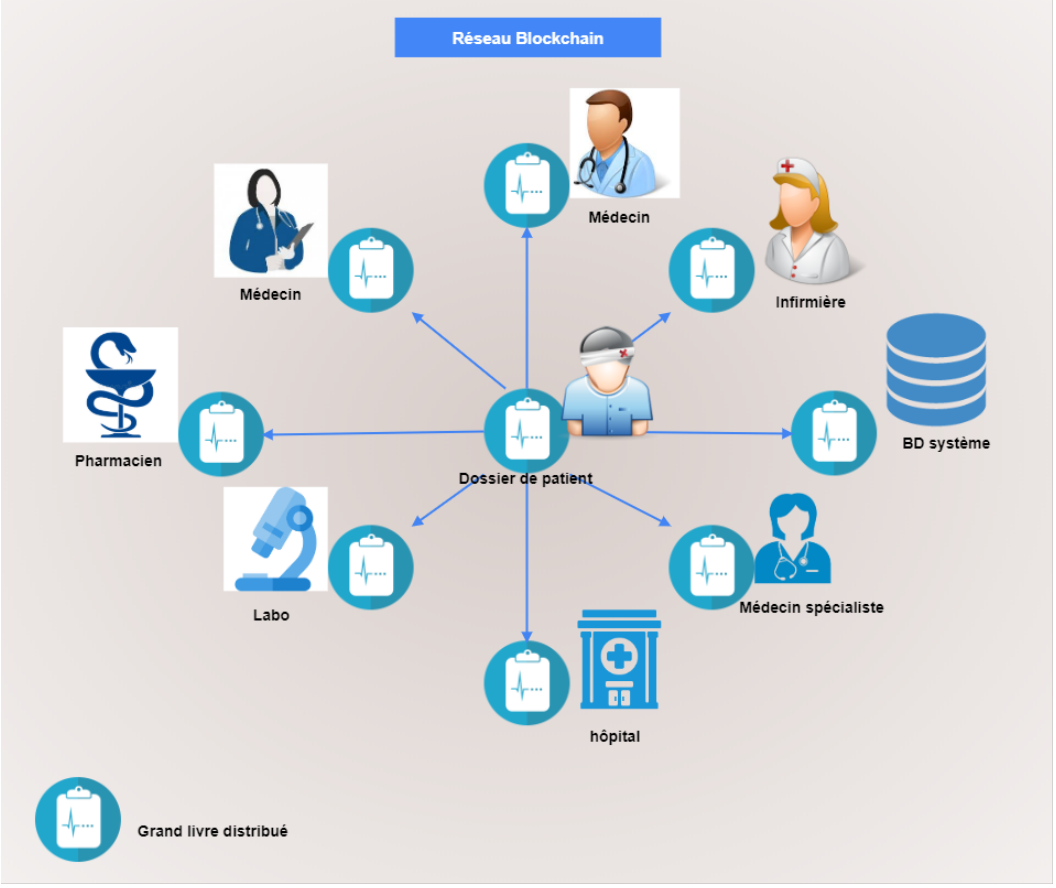

FIGURE 3.11 – Architecture module "**Réseau Blockchain**"

4.4 Ajout d'un nouveau document

Le processus d'ajout d'un nouveau document se déroule en trois étapes (Figure 3.12). Tout d'abord, on stocke le fichier dans la base de données système. Par la suite, on calcule le hachage de document et on le stocke également dans la base de données système. La dernière étape consiste à créer un nouveau bloc pour ce document. Après la création, le système ajoute ce bloc (et son fichier) à la chaine de tous le staff médical qui partage ce dossier médical.

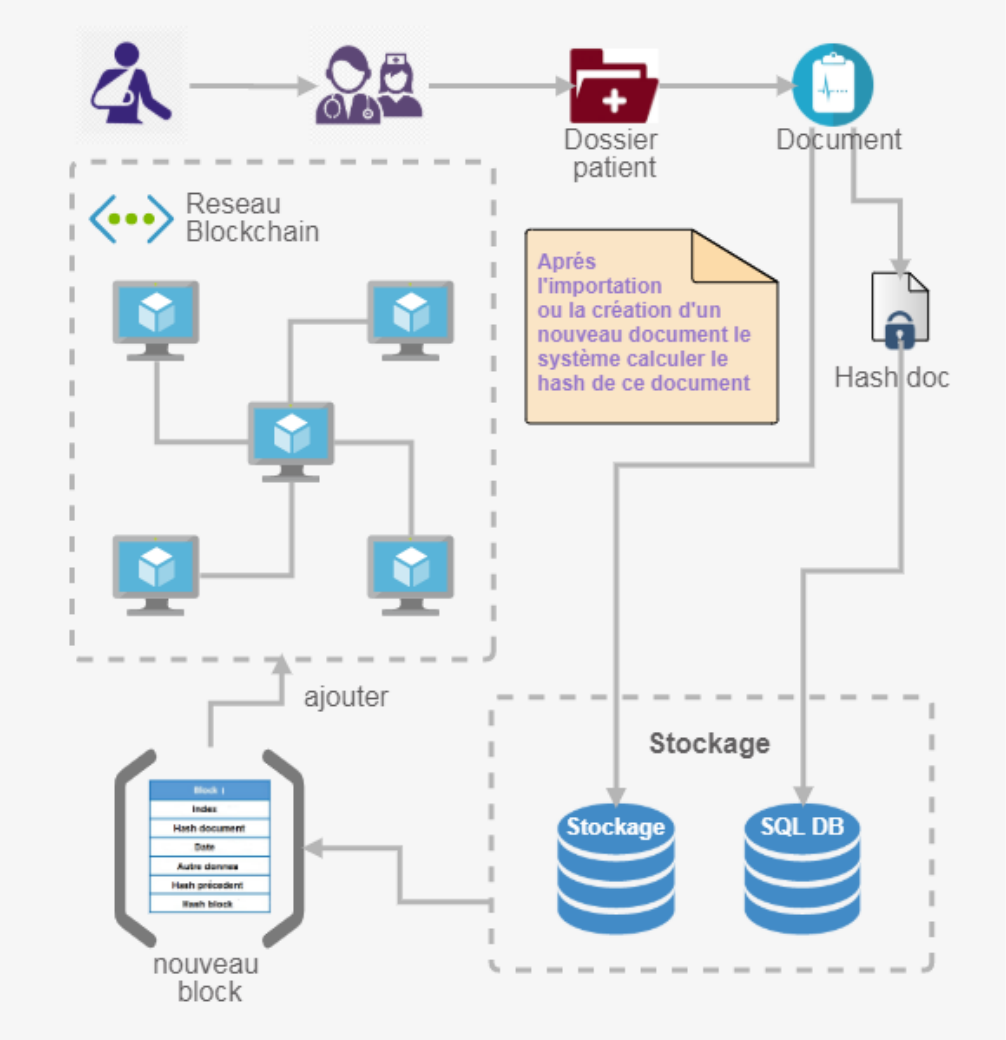

FIGURE 3.12 – Architecture module "**Ajout document**"

5 Conclusion

Dans ce chapitre, on a présenté le développement de notre système DMPS en adoptant une approche Blockchain, où les données de santé peuvent être gérer en utilisant des dossier médicaux électroniques. Dans ce qui suit, on présente la réalisation effective du système DMPS.

Chapitre 4

Implémentation

1 Introduction

Dans le chapitre précédent, on a présenté l'architecture ainsi que les détails du système DMPS et ses différents composants. Dans ce chapitre, on va présenter l'implémentation du système spécifié. On commence par la citation des outils et langages utilisés pour la réalisation de notre système. On passe par la suite à décrire les composants principaux de notre système en offrant des imprimes écrans.

2 Outils & Langages de programmation

Tout d'abord, les principaux outils que nous avons utilisé pour la réalisation de notre système sont les suivants :

— ***Vscode*** : comme un éditeur de code multi-plateforme, open source et gratuit, supportant une dizaine de langages,

— ***Bootstrap*** : pour la création du design (graphisme, animation et interactions avec la page dans le navigateur, etc.) de notre application web,

— ***XAMPP*** pour mettre en place un serveur Web local. Il s'agit d'une distribution de logiciels libres (X (cross) Apache MariaDB Perl PHP) offrant une bonne souplesse d'utilisation, réputée pour son installation simple et rapide, comme il permet de configurer un serveur de test local avant la mise en œuvre d'un site internet.

Concernant les langages de programmation, nous avons utilisé **Php** pour la côté serveur pour la récupération des informations issues d'une base de données, ou les données envoyées par le navigateur afin d'être interprétées ou stockées pour une utilisation ultérieure. **Javascript** pour créer des pages web dynamiques et interactives. Et pour faciliter l'écriture de scripts côté client dans le code HTML des pages web, on a utilisé **jQuery**.

Php

PHP,Hypertext Preprocessor, est un langage de programmation libre utilisé le plus souvent côté serveur. Il a été conçu pour permettre la création d'applications dynamiques développées pour le Web (en 2018, près de 80 % des sites web utilisent le langage PHP sous ses différentes versions).

PHP est le plus souvent couplé à un serveur Apache bien qu'il puisse être installé sur la plupart des serveurs HTTP tels que IIS ou nginx. Ce couplage permet de récupérer des informations issues d'une base de données, d'un système de fichiers (contenu de fichiers et de l'arborescence) ou plus simplement des données envoyées par le navigateur afin d'être interprétées ou stockées pour une utilisation ultérieure.

Javascript

JavaScript est un langage de programmation de scripts employé principalement dans les pages web interactives, il présente un langage orienté objet à prototype. Il est utilisé pour une grande majorité des sites web, et aussi disposé par la majorité des navigateurs web pour interpréter indépendamment des considérations de sécurité qui peuvent se poser le cas échéant.

Le langage JavaScript se distingue des langages serveurs par le fait que l'exécution des tâches est opérée par le navigateur lui-même, sur l'ordinateur de l'utilisateur, et pas sur le serveur web. Il s'active donc généralement sur le poste client plutôt que côté serveur.

JQuery

JQuery est une bibliothèque JavaScript libre et multiplateforme créée pour faciliter l'écriture de scripts côté client dans le code HTML des pages web. Le but de la bibliothèque étant le parcours et la modification du DOM, elle contient de nombreuses fonctionnalités ; notamment des animations, la manipulation des feuilles de style en cascade (accessibilité des classes et attributs), la gestion des évènements, etc.

Depuis sa création en 2006 et notamment à cause de la complexification croissante des interfaces Web, jQuery a connu un large succès auprès des développeurs Web. Il est à l'heure actuelle la bibliothèque front-end la plus utilisée au monde (plus de la moitié des sites Internet en ligne intègrent jQuery).

3 Implémentation et réalisation du système

Dans cette partie du chapitre, on offre une description bien détaillée de notre système DMPS et illustrée avec des imprimes écrans de ses différentes pages web.

3.1 Description du système

Notre système vise à gérer les données de santé en collectant, stockant et partageant des dossiers médicaux électroniques. Il permet également de fournir aux médecins des informations médicales (antécédents médicaux, résultats d'analyses de laboratoire, imagerie, traitement en cours ... etc), en provenance d'autres médecins (médecins généralistes, spécialistes, ou bien hospitaliers), en définissant un profil médical pour chaque patient. De cette manière, on facilite la communication, et en toute sécurité, entre divers professionnels de santé (médecin traitant, infirmier, ... etc) en relation avec ce patient. On entend ici le système ***Dossier Medical Partagé*** et ***Sécurisé***, figure 4.1 représente le logo du système DMPS.

FIGURE 4.1 – Logo du système DMPS

En fait, le système DMPS est centré sur le **patient**, le patient étant toujours au centre du cercle de soin ; alors que le bord du cercle comprend différents professionnels de santé (médecin, pharmacien, laboratoire, ... etc) liés à ce patient, on peut dire ici le **Staff médical**. Et bien sûr, le système est géré par un administrateur **Admin** qui a des tâches spécifiques. Dans ce qui suit, on détaille les tâches associés à chacun d'eux.

Lorsqu'un patient est ajouté par un professionnel de santé, le système crée un dossier médical (compte) défini par son numéro d'assurance pour lui permettre, ainsi que bien sûr les autres professionnels de santé, d'accéder à son dossier médical.

Au début, lorsque le dossier médical est créé, il va contenir le premier bloc de la Chaine qui l'appelle "GenesisBlock", figure 4.2 donne un aperçu de ce bloc.

```
{"index":0,
"nomDocument":"genisisFichier.txt",
"typeDocument":"block 0",
"commentaire":"premier block",
"date":"Dimanche 2 aout 2020. 21:38:12",
"prof":"prof",
"role":"role",
"hashPrecedent":"0",
"hash":"15efdf2c84b1e8138ea921aa497ded1ed1c6d89ac0836415f1f8a109d408aaf9",
"nonce":0},
```


FIGURE 4.2 – *GenesisBlock* : premier bloc du dossier médical.

Que signifie un *Bloc* dans ce cas ?

Un *bloc* est défini comme une unité contenant les informations de chaque consultation, où :

index : représente le numéro du bloc,

nomDocument, ***typeDocument***, et ***commentaires*** : pour définir le nom du document ajouté (créé) durant la consultation, son type : ordonnance, radio, analyse, ... etc, et les commentaires ajoutés par le professionnel de santé associé,

date : définit la date de la consultation,

prof et ***role*** : définissent le nom du professionnel de santé associé, et son rôle : médecin, pharmacien, ...etc,

hashPrecedent : définit le hachage du bloc précédent. Le hashPrecedent du "genesisBlock" est 0,

hash : est le hachage du bloc actuel. En d'autres termes, le hachage de toutes les informations présentes dans ce bloc,

nonce c'est l'abréviation de "*number only used once*", qui est un nombre ajouté à un bloc haché dans une Blockchain qui répond aux restrictions de niveau de difficulté. Pour le premier bloc, le nonce est 0.

Au fur et à mesure, il y aura une chaîne de blocs, *Blockchain*, pour le dossier médical de chaque patient. Figure 4.3 représente un bloc décrivant une consultation, nécessitant une radiographie, d'un tel patient par le chirurgien *Benidire Rachid*.

```
{"index":1,
"nomDocument":"radio2.jpg",
"typeDocument":"Radio",
"commentaire":"radio",
"date":"Dimanche 2 aout 2020. 23:04:05",
"prof":"benidire rachid",
"role":" la chirurgie g\u00e9n\u00e9",
"hashPrecedent":"15efdf2c84b1e8138ea921aa497ded1ed1c6d89ac0836415f1f8a109d408aaf9",
"hash":"05475fcb2dfa4982a45c43c7d17d05960f24a2c9f7a2877ff35f0a0941cba781",
"nonce":7}
```


FIGURE 4.3 – Bloc décrivant un radio

Remarque 1 *Le patient peut consulter ses informations de santé, et donc visualiser*

les divers actions réalisées sur son dossier ; mais il ne peut pas ajouter ou bien supprimer des fichiers médicaux.

Soit un médecin, un pharmacien, un soignant, on dit en général un professionnel de santé. Il peut accéder au dossier médical du patient après la création d'une compte dans le système.

L'accès au dossier patient est très facile pour un professionnel de santé [1]. Une fois ce professionnel fait accès au dossier du patient, une copie de ce dossier est devenu sur son ordinateur. Donc, il peut voir toutes les informations et les données de son patient, comme il peut faire l'ajout d'autres fichiers médicaux mais pas de suppression ou bien des modification des anciennes informations.

Lorsqu'un patient visite un professionnel de santé. Durant la consultation, le professionnel va recommander l'ajout d'un nouveau fichier médical au dossier de ce patient, une ordonnance par exemple. D'abord, le système DMPS vérifie que la chaîne n'a pas été compromise ou modifiée. En d'autres termes, le système vérifie la validité de la chaîne.

Dans le cas où la chaîne d'un utilisateur a été piratée ou modifiée, le système va découvrir cette violation car le fichier est stocké sur plusieurs ordinateurs(les participants de ce dossier médical), et donc il est facile de traiter ce problème. Pour cette raison, le dossier du patient reste sécurisé de pénétration ou modification tout le temps.

Après la vérification de la validité de la chaîne, le système calcule le hachage de ce document par la fonction "Sha256", et crée un nouveau bloc contenant le hash de ce document et d'autres informations liée comme le nom du document, type, date de consultation, ... etc, et aussi le hash du bloc précédent. Après la création du bloc, le système fait appel à la fonction de ***minage***, Figure 4.4, pour valider le bloc crée. Une fois le bloc est validé, le système ajoute ce bloc à la chaîne de tous le staff médical qui partage ce dossier médical.

```
mineBlock(difficulty, hashFichier){
    while(this.hash.substring(0, difficulty) !== Array(difficulty + 1).join("0")){
        this.nonce++;
        this.hash = this.caculateHash(hashFichier);
    }
}
```

FIGURE 4.4 – Code fonction ***minage***

Remarque 2 *Le **minage** consiste à résoudre un problème mathématique. Ici, la résolution se traduit par la validation du bloc. Le problème mathématique que nous propose c'est que le hachage d'un bloc doit commencer par deux zéros successives.*

1. Dans les cas de confusion entre les patient le code de sécurité va être utilisé.

3.2 Interface du système

Cette partie vous permet d'avoir un aperçu de notre système DMPS, où on va montrer ses pages web principales (imprimes écrans), commençant par l'accueil.

Accueil (accès comme un patient)

Accueil (Figure 4.5), c'est la page d'entrée ou principale de notre DMPS, où vous pouvez vous identifier comme un professionnel de santé, un patient, ou bien un administrateur.

Lorsque vous vous identifiez comme un patient, c'est le cas devant nous, vous pouvez parmi d'autres opérations obtenir de l'aide ou bien se connecter à votre DMPS, bien sûr, si vous êtes déjà inscrit.

FIGURE 4.5 – Page d'accueil du DMPS

Une fois que vous vous avez connecté au votre DMPS (à travers le bouton '*Mon DMPS*'), vous accédez au profil patient.

Comme un patient, vous pouvez consulter la liste de vos documents médicaux : ordonnance, radio, analyse, ... etc, comme le montre Figure 4.6.

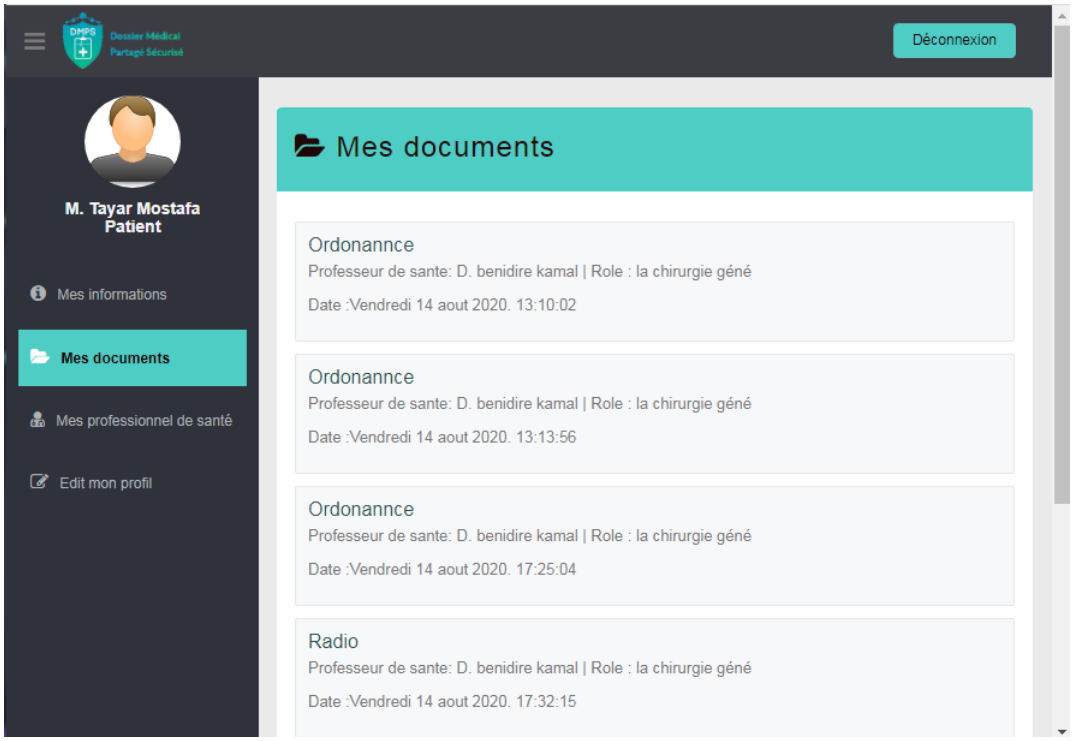

FIGURE 4.6 – La page 'Mes documents' du profil patient

En cliquant sur l'un de vos documents, par exemple "Radio", une page d'information du document choisi s'affiche, voir Figure 4.7.

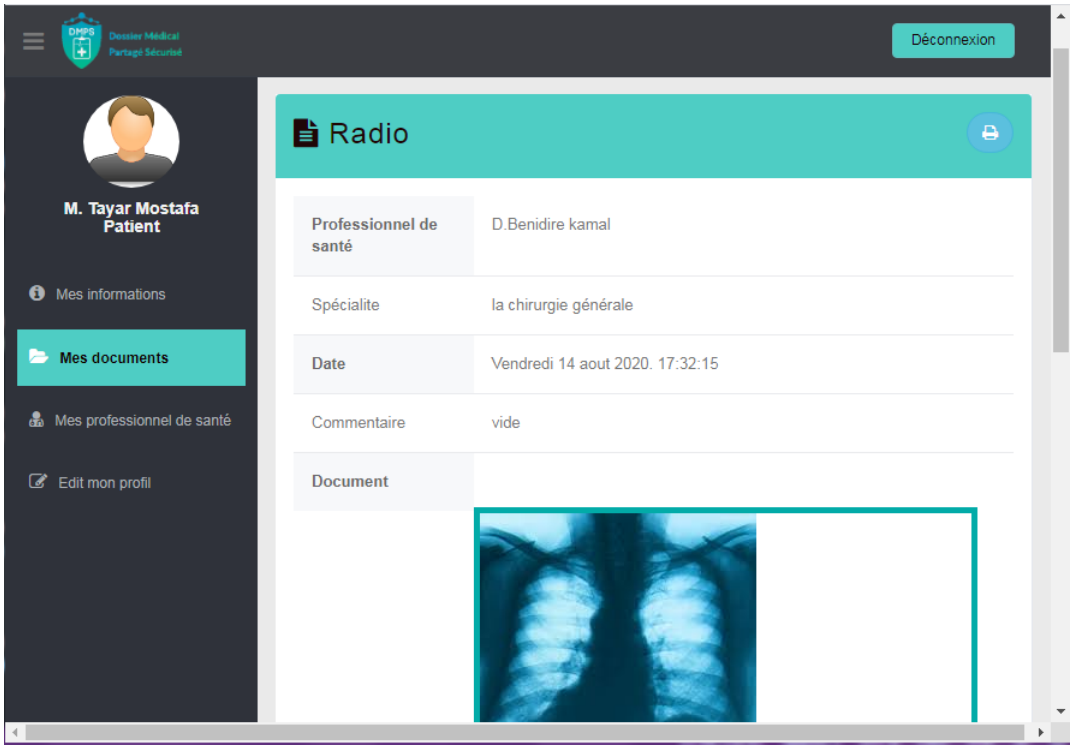

FIGURE 4.7 – La page d'information du document "Radio"

Chaque document est défini par : le professionnel de santé qui le crée ainsi que son spécialité, la date de création, des commentaires s'il existe, et le document soi-même. Vous pouvez également avoir une copie imprimée de ce document.

Vous pouvez aussi visualiser vos professionnels de santé, Figure4.8.

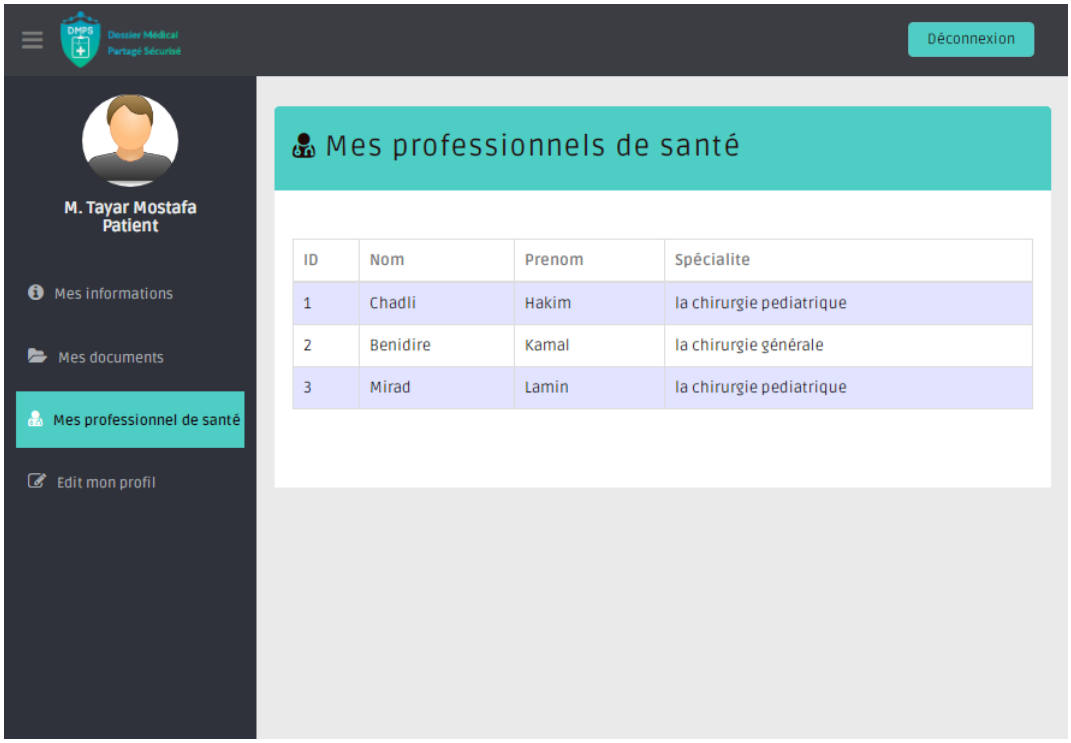

FIGURE 4.8 – La page "Mes profs de santé"

Finalement, vous pouvez accéder à vos informations personnelles, ici, le système vous donne la main pour les modifier si vous voulez.

Accès comme un professionnel de santé

Lorsque vous vous identifiez comme un professionnel de santé, vous aurez deux options :

- ▷ Soit vous avez déjà un compte, et dans ce cas vous pouvez l'accéder.
- ▷ Soit vous n'avez pas de compte, et donc vous devez cliquer sur le lien *'Inscrire'*. Ici, vous arrivez sur un formulaire simple d'inscription comme celui-ci (Figure 4.9).

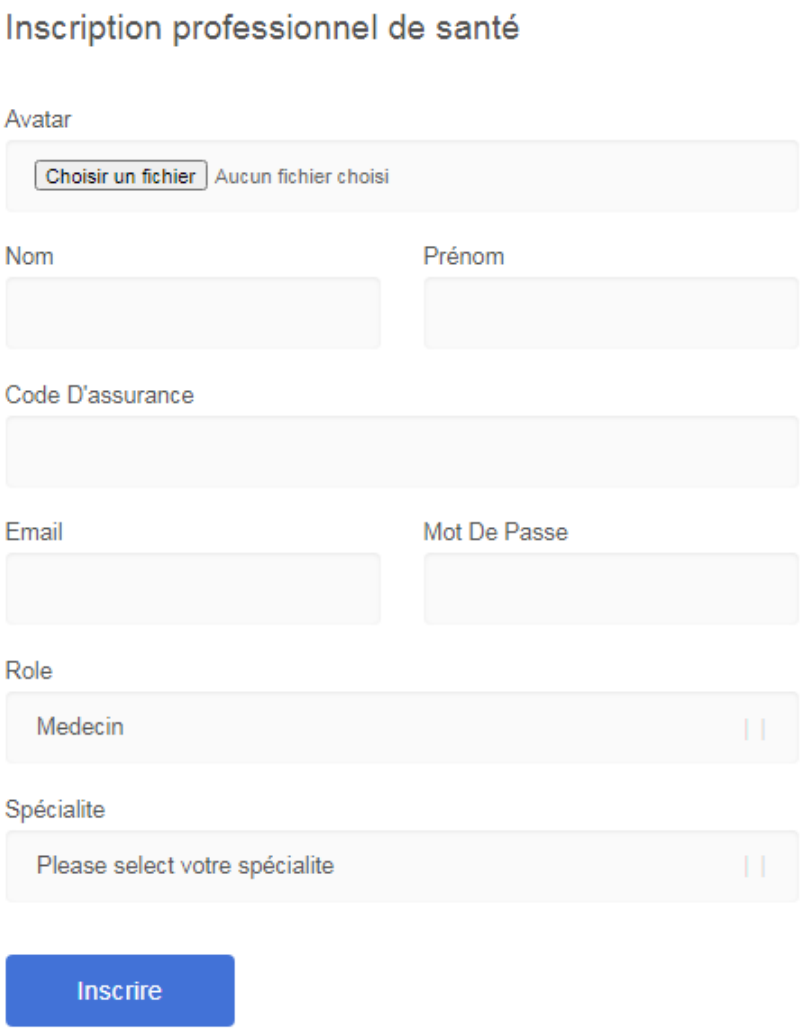

FIGURE 4.9 – Formulaire d'inscription

Il est à noter qu'un tel processus nécessite un code d'assurance pour assurer que vous êtes un vrai professionnel de santé. Votre adresse email doit être correct, une confirmation vous sera envoyée par la suite.

Lors de la validation, votre compte est créé. Vous êtes alors redirigé automatiquement sur le profil professionnel de santé.

Une fois le formulaire rempli et envoyé, vous devez confirmer l'adresse email, pour cela DMPS va vous parvenir un message avec un code comme le montre Figure 4.10. A la réception de celui-ci vous devez le saisir et valider.

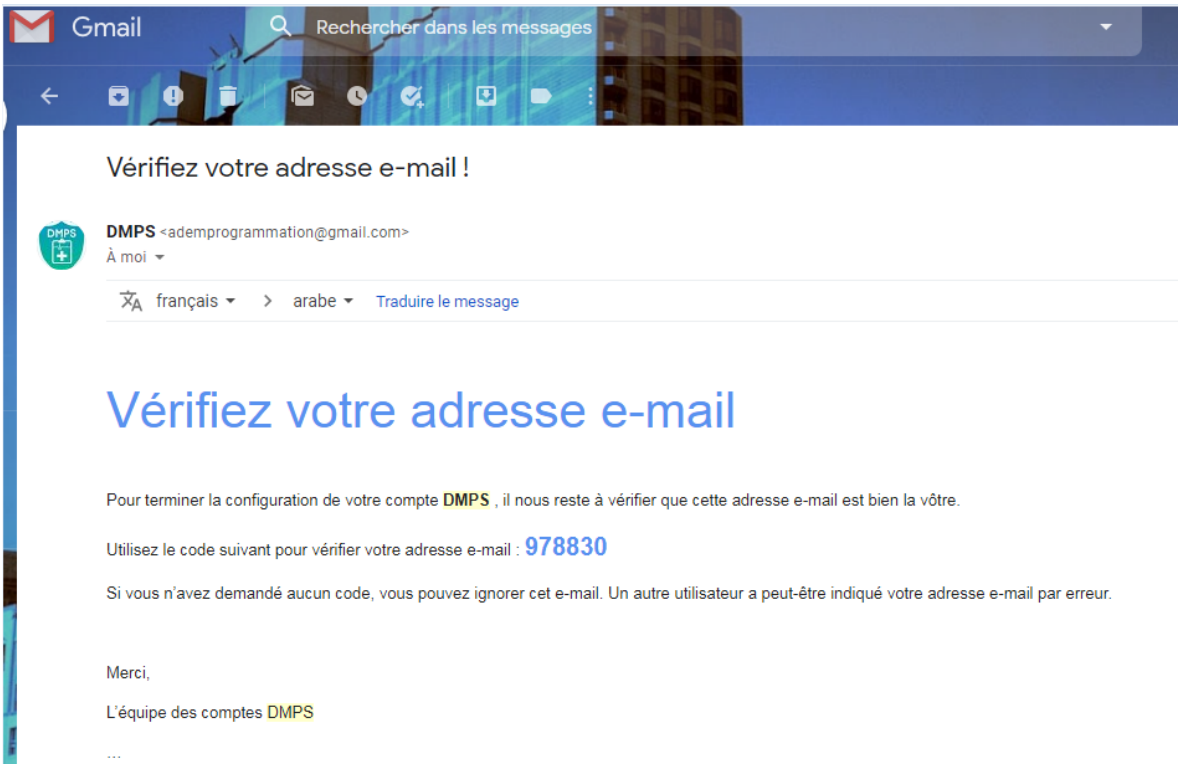

FIGURE 4.10 – Le message "Vérification email"

- Vous pouvez donc accéder à la liste des patients ayant des comptes DMPS, voir Figure 4.11. À partir de cette liste, vous pouvez ajouter des patients à vous. ou bien de supprimer un patient du système en cas de décès.

FIGURE 4.11 – La page "Tous les patients"

∗ Vous pouvez également créer un compte pour un nouveau patient qui n'en a pas en cliquant sur le lien *Créer nouveau DMPS*.

- Et afin d'accéder au DMPS d'un tel patient vous devez tout d'abord accéder à la liste "Mes patients" et après cliquer sur le lien "accès" correspond à ce patient. Dans ce cas, vous pouvez consulter la liste de ses document (Figure 4.12).

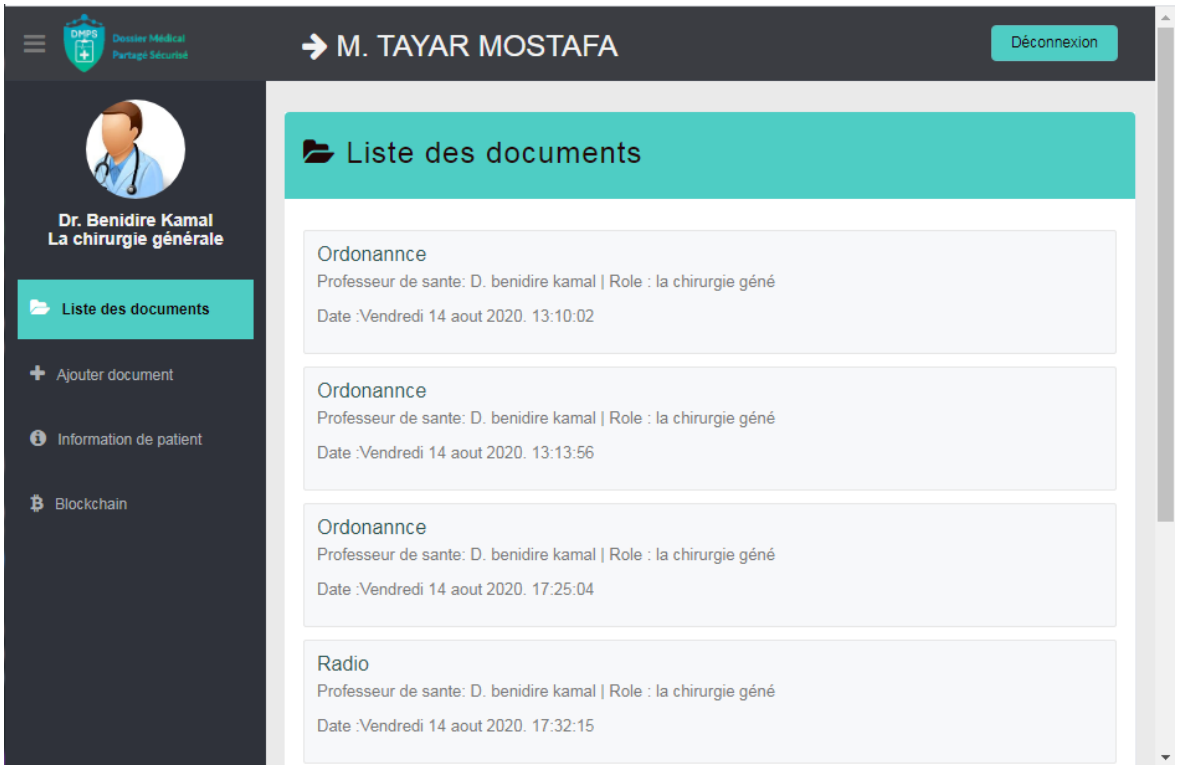

FIGURE 4.12 – La page "Liste des documents"

- Vous pouvez ainsi ajouter un nouveau document à travers le lien "+ajouter document", en l'attachant ou en le rédigeant comme dans le cas d'une ordonnance comme l'indique Figure 4.13.

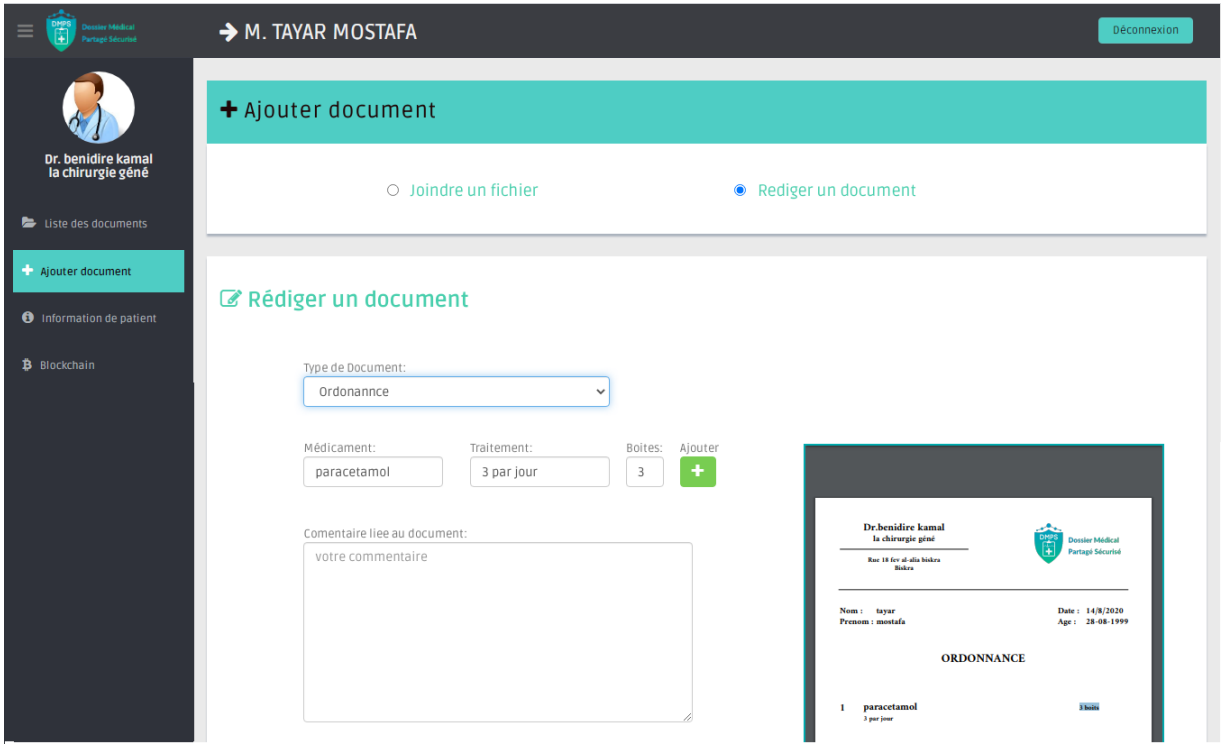

FIGURE 4.13 – La page "Rédaction ordonnance"

- Et pour chaque patient et donc compte DMPS, vous pouvez visualiser la chaine des blocs correspondante (voir Figure 4.14).

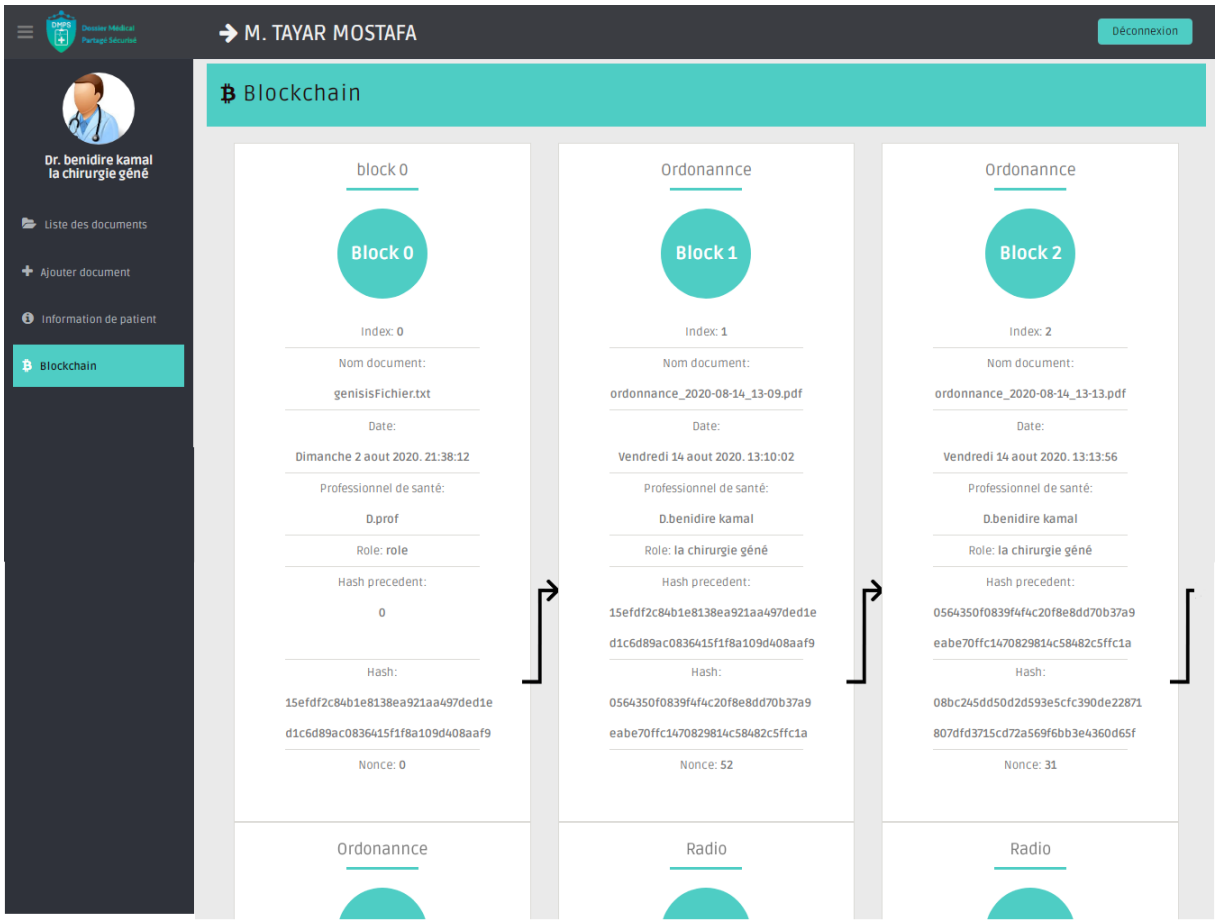

FIGURE 4.14 – La page "Blockchain"

Accès comme un administrateur

Finalement, si vous êtes un administrateur, vous pouvez visualiser votre système et donc :

- Avoir la liste des patients (Figure 4.15), ainsi que leurs DMPSs.

FIGURE 4.15 – La page "Tous les patients"

- Avoir la liste des professionnels de santé (Figure 4.16), où vous avez la main pour supprimer le compte d'un professionnel en cas de décès.

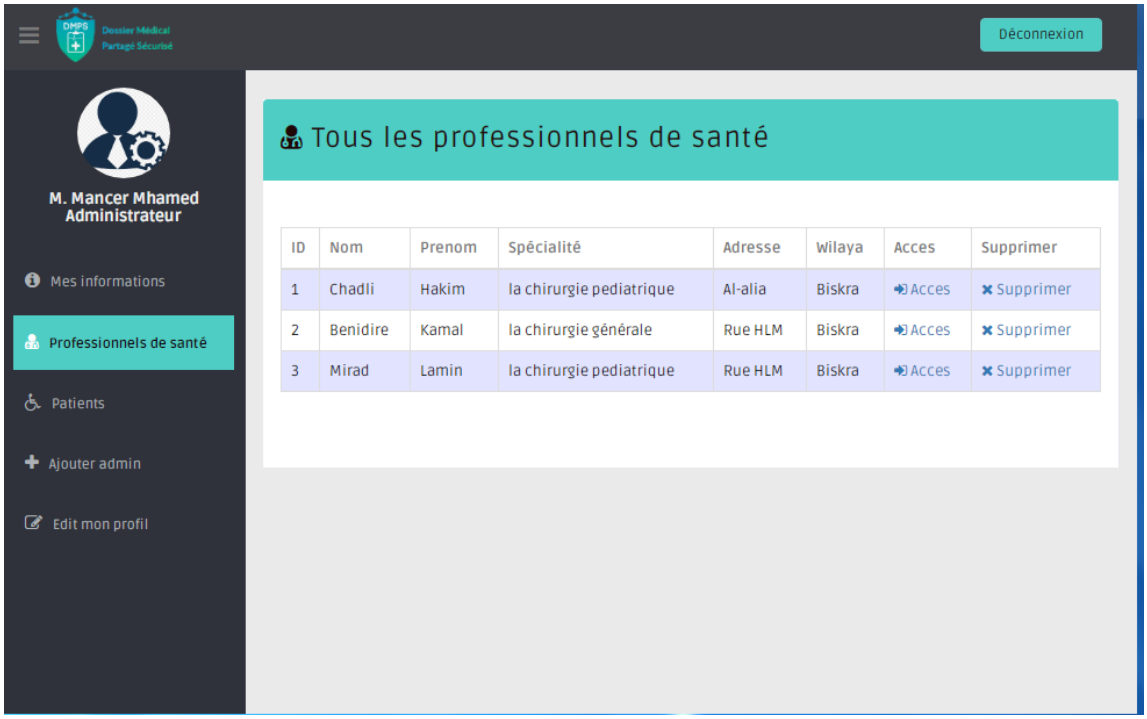

FIGURE 4.16 – La page "Tous les professionnel de santé"

∗ Vous pouvez aussi enregistrer un nouveau administrateur et consulter vos informations ou bien les modifier.

4 Conclusion

La partie implémentation est l'étape la plus importante dans notre projet. Dans ce chapitre, on a présenté les outils de développement qu'on a utilisées avec une description bien détaillée du système réalisé, où on a expliqué les principales interactions pouvant survenir pendant le fonctionnement du système DMPS.

Conclusion Générale

La Blockchain est l'une des technologies à surveiller dans les années à venir. Cela pourrait révolutionner plusieurs secteurs, c'est comme un très gros cahier que tout le monde peut lire gratuitement et librement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible. Il s'agit essentiellement de la Blockchain : une technologie permettant de stocker et de transmettre des informations de manière transparente et sécurisée.

Dans ce mémoire, on a présenté la conception d'un système permettant le partage sécurisé des données de santé qui, en fait, a été un sujet difficile pendant longtemps car il manquait de confiance et donc de sécurité. En effet, la plupart des données médicales sont stockées dans différentes institutions médicales, ce qui entraîne leur dispersion. Et cela rend difficile pour les patients d'acquérir tous leurs dossiers médicaux auprès des diverses institutions médicales qu'ils ont visitées. Pour cette raison, le stockage, le partage et l'application des données médicales sont essentiels dans les cas où la sécurité et la confidentialité sont garanties.

Par conséquent, on a proposé notre système DMPS qui est basé sur la Blockchain pour gérer les données de santé en collectant, stockant et partageant les dossiers médicaux électroniques en toute sécurité. Il permet également de fournir aux médecins, par exemple, des informations médicales d'autres professionnels de santé, en définissant un profil médical pour chaque patient. On peut même citer parmi les points forts du système DMPS :

Pour un patient : il peut accéder en toute sécurité à ses données de santé à tout moment et n'importe où, avec l'élimination du risque de perdre des radiographies ou des analyses. De cette manière, le médecin a connaissance de tous les documents et informations médicales du patient et peut également les mettre à jour, au fur et à mesure.

Tandis que le professionnel de santé : il peut accéder facilement et rapidement au DMPS de son patient à tout moment et en tout lieu. Il peut également retrouver toutes les informations médicales d'un tel patient. Le système DMPS permet d'éviter de prescrire des tests ou des traitements déjà demandés en plus d'éviter les interactions médicamenteuses.

Pour terminer, on peut énoncer des perspectives :

- Mettre en place un réseau de Blockchain médicale reliant autant d'établissements médicaux et de santé que possible.
- Faire un couplage de ce projet avec le modèle du Bigdata.
- Exploiter des systèmes multi-agents.
- Utiliser et bénéficier du Cloud pour résoudre le problème du stockage des données médicales.

Bibliographie

[1] J. Huynh, "Blockchain et secteur santé, quelles opportunités ?." https://www.sih-solutions.fr/sih-a-la-une/blockchain-et-secteur-sante-quelles-opportunites/, 8 avril 2019. Accessed : 2020-02-03.

[2] L. Leloup, *Blockchain : La revolution de la confiance*. Editions Eyrolles, 2017.

[3] R. LONGUECHAUD, "Introduction À la blockchain." http://remilonguechaud.fr/2017/08/25/introduction-a-blockchain/, 25 AOUT 2017. Accessed : 2019-10-02.

[4] uchange.co, *Comprendre la blockchain*. Livre blanc sous licence Creative Commons, Janvier 2016.

[5] "Qu'est-ce que la blockchain ?." https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain. Accessed : 2019-10-25.

[6] J.-P. Delahaye, "Les blockchains, clefs d'un nouveau monde'," *Pour la Science*, no. 449, pp. 80–85, 2015.

[7] S. GOYAL, "History of blockchain technology – timeline infographic." https://bit.ly/3iiqQju, NOVEMBER 3, 2018. Accessed : 2019-10-10.

[8] P. Marrast, "Blockchain : Éléments d'explication et de vulgarisation, pourquoi s' intéresser à la blockchain aujourd'hui ?," 2018.

[9] "L'histoire de la blockchain." https://bit.ly/2XFaWaU. Accessed : 2019-10-05.

[10] M. PIGNEL and D. STOKKINK, "La technologie blockchain une opportunité pour l'économie sociale ?,"

[11] "Bitcoin c'est quoi ?." https://bit.ly/31Kcou7. Accessed : 2019-10-05.

[12] "PrÉsentation d'ethereum." https://bit.ly/3a8PDDy. Accessed : 2019-10-05.

[13] C. F. Plisson, "La blockchain, un bouleversement économique, juridique voire sociétal," *I2D Information, donnees documents*, vol. 54, no. 3, pp. 20–22, 2017.

[14] C. Chedrawi and P. Howayeck, "The role of blockchain technology in military strategy formulation, a resource based view on capabilities," 12 2018.

[15] R. L. G. Valéria Faure-Muntian, Claude de Ganay, "Cf. la note scientifique de l'office 4 : "comprendre les blockchains (chaînes de bloc)"," 12 avril 2018.

[16] A. Lastovetska, "Blockchain architecture basics : Components, structure, benefits and creation." https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture, January 31, 2019. Accessed : 2019-10-20.

[17] Paul, "Everything you need to know about blockchain architecture." https://www.edureka.co/blog/blockchain-architecture/, May 22,2019. Accessed : 2019-10-20.

[18] "Blockchain architecture." https://www.pluralsight.com/guides/blockchain-architecture, Jan 10, 2019. Accessed : 2019-10-20.

[19] Blockgenic, "Different blockchain consensus mechanisms." https://hackernoon.com/different-blockchain-consensus-mechanisms\-d19ea6c3bcd6, November 10th, 2018. Accessed : 2019-10-24.

[20] S. Cherednichenko, "What are blockchain apps and how to develop one." https://www.mobindustry.net/what-are-blockchain-apps-and-how-to-develop-one/, 12.07.2019. Accessed : 2020-01-29.

[21] A. Rathore, "How to develop a blockchain application-overview." https://enappd.com/blog/how-to-develop-a-blockchain-application/4/. Accessed : 2020-01-31.

[22] Anurag, "8 steps to start blockchain development and get your dapp ready." https://www.newgenapps.com/blog/8-steps-how-to-start-blockchain-development-dapp, Apr 18, 2020. Accessed : 2020-01-30.

[23] M. Koropko, "How to develop a blockchain application." https://merehead.com/blog/develop-blockchain-application/, December 27, 2019. Accessed : 2020-01-31.

[24] "How to create a blockchain application." http://ddi-dev.com/blog/programming/how-develop-blockchain-application/, January 2018. Accessed : 2020-02-01.

[25] "Régulation de la blockchain." https://www.legalis.net/legaltech/regulation-de-la-blockchain, 18 JANVIER 2017. Accessed : 2020-02-01.

[26] S. Cherednichenko, "What are blockchain apps and how to develop one." https://www.mobindustry.net/what-are-blockchain-apps-and-how-to-develop-one/, 12.07.2019. Accessed : 2020-02-02.

[27] N. REIFF, "Introduction a la blockchain explained." https://www.investopedia.com/terms/b/blockchain.asp, Feb 1, 2020. Accessed : 2019-10-16.

[28] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain : promises, challenges, and scenarios in health and healthcare," 2018.

[29] K. Curran, "E-voting on the blockchain," *The Journal of the British Blockchain Association*, vol. 1, no. 2, p. 4451, 2018.

[30] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, p. 1, 2018.

[31] "Blockchain." https://bit.ly/3fFuVwe, 20.09.18. Accessed : 2019-10-16.

[32] D. Lalande, "Applications de la blockchain en entreprise." https://bit.ly/3ksAiTs, 19 avril 2017. Accessed : 2019-10-20.

[33] R. Berné, "Blockchain : avantages et inconvénients." https://cryptoast.fr/blockchain-avantages-inconvenients/, le 3 janvier 2019. Accessed : 2019-10-25.

[34] "Comprendre le fonctionnement de la technologie blockchain, le bitcoin et les autres crypto-monnaies.." https://www.cryptoencyclopedie.com/single-post/Quels-sont-les-avantages-de-la-technologie-Blockchain. Accessed : 2019-10-25.

[35] L. SALMERON, "L'intelligence artificielle et la blockchain peuvent-elles se combiner ?." https://mbamci.com/l-intelligence-artificielle-et-la-blockchain-se-combinent/, 5 septembre, 2019. Accessed : 2020-02-03.

[36] S. Daley, "Tastier coffee, hurricane prediction and fighting the opioid crisis : 31 ways blockchain and ai make a powerful pair." https://builtin.com/artificial-intelligence/blockchain-ai-examples, April 6, 2020. Accessed : 2020-05-01.

[37] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[38] F. Pennic, "Healthcare blockchain startup burstiq secures $5m investment." https://hitconsultant.net/2018/02/23/healthcare-blockchain-startup-burstiq-secures-5m/, 02/23/2018. Accessed : 2019-07-17.

[39] G. Srivastava, R. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," 10 2019.

[40] "Blockchain, ai and iot for a smart, connected world." Https://www.startengine.com/netobjexinc. Accessed : 2020-05-05.

[41] https://oriole-greyhound-cz64.squarespace.com/. Accessed : 2020-05-05.

[42] K. Anderson, "What is neureal ?." https://medium.com/@kyler_82404/what-is-neureal-e58e3a47679b, Feb 16, 2018. Accessed : 2020-02-05.

[43] "Bitcoin est un réseau de paiement novateur et une nouvelle forme d'argent.." https://bitcoin.org/fr/. Accessed : 2019-11-20.

[44] "What is bitcoin ?." https://support.blockchain.com/hc/en-us/articles/211122603-What-is-Bitcoin-. Accessed : 2020-05-02.

[45] "L'histoire de la blockchain." https://www.binance.vision/fr/blockchain/history-of-blockchain. Accessed : 2020-01-05.

[46] "PrÉsentation d'ethereum." https://www.blockchain.com/fr/learning-portal/ether-basics. Accessed : 2020-01-05.

[47] "Qu'est ce qu'ethereum ?." https://www.binance.vision/fr/blockchain/what-is-ethereum. Accessed : 2020-01-05.

[48] S. Voshmgir, "Smart contracts." https://blockchainhub.net/smart-contracts/, July 2019,. Accessed : 2019-12-20.

[49] S. Daley, "25 blockchain applications and real-world use cases disrupting the status quo." https://builtin.com/blockchain/blockchain-applications, December 5, 2018. Accessed : 2020-01-05.

[50] "Enabling blockchain financial markets." https://www.chainfinancial.io/. Accessed : 2020-03-05.

[51] M. Weiss and M. Halyard, "Voatz." https://www.hbs.edu/faculty/Pages/item.aspx?num=56024, APRIL 2019. Accessed : 2019-12-25.

[52] J. Zhang, A. Young, and S. Verhulst, "Addressing voting inefficiencies resulting from identity challenges with blockchain," 2018.

[53] "Steem c'est quoi ?." Https://courscryptomonnaies.com/steem. Accessed : 2020-01-15.

[54] "Acheter steem (steem) : Tout savoir sur son prix, cours et autres crypto." https://www.droitdunet.fr/acheter-steem/, mai 6, 2020. Accessed : 2020-05-20.

[55] A. Petre and N. Haï, "Opportunités et enjeux de la technologie blockchain dans le secteur de la santé," *médecine/sciences*, vol. 34, no. 10, pp. 852–856, 2018.

[56] "Comment innovhealth veut booster le déploiement de son passeport médical numérique." https://www.ticsante.com/story/4684/comment-innovhealth-veut-booster-le-deploiement-de-son-passeport\-medical-numerique.html, 08/07/2019. Accessed : 2020-01-20.

[57] "Blockchain et logistique de l'industrie pharmaceutique." https://blog.groupestarservice.com/comment-la-blockchain-impacte-t-elle-la-logistique-de-lindustrie\-pharmaceutique/, 16 septembre 2019. Accessed : 2020-02-20.

[58] F. R. et Vincent Riffier, "Blockpharma , solution blockchain de traçabilité des médicaments." https://www.myfrenchstartup.com/fr/startup-france/167000/blockpharma, 18 janvier 2017. Accessed : 2020-02-22.

[59] C. Dru, "Blockchain et santé," 2017.

[60] E. de Castex, "Données génétiques : stockage et partage via une blockchain." http://www.anthropotechnie.com/stocker-et-partager-les-donnees-genetiques-via-une-blockchain/, 4 May 2018. Accessed : 2020-02-20.

[61] M. M. des entreprises de France), *Livre blanc La blockchain pour les entreprises.* avril 2016.

[62] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An overview of blockchain technology : Architecture, consensus, and future trends," 06 2017.

[63] J. MOY, "La cryptomonnaie, fonctionnement et définitions." https://www.supinfo.com/articles/single/10012-cryptomonnaie-fonctionnement-definitions, 03/10/2019. Accessed : 2020-02-02.

[64] H. Ventures, "Portfolio stories : Nebula genomics." https://medium.com/hemi-ceos/portfolio-stories-nebula-genomics-483c844c3d0d, Oct 11, 2018. Accessed : 2020-03-20.