Université de Lille
Année Universitaire 2022/2023

Faculté de Pharmacie de Lille

THESE
POUR LE DIPLOME D'ETAT
DE DOCTEUR EN PHARMACIE

Soutenue publiquement le 10 février 2023
Par Mme Facon Chloé

LA BLOCKCHAIN PEUT-ELLE RESOUDRE LES ENJEUX LIES A LA GESTION ET AU PARTAGE DES DONNEES DE SANTE ?

Membres du jury :

Président et Directeur, conseiller de thèse : Serghereart, Eric, Professeur, Université de Lille, Lille

Assesseur(s) :
Grunewald, Alizée, Docteur en Pharmacie et Chef de Produit Senior Oncologie Thoracique, AstraZeneca, Paris
Olivier, Corentin, Pharmacien et Chef de Projet Digital Customer Engagement, Lundbeck, Paris

THESE
POUR LE DIPLOME D'ETAT
DE DOCTEUR EN PHARMACIE

LA BLOCKCHAIN PEUT-ELLE RESOUDRE LES ENJEUX LIES A LA GESTION ET AU PARTAGE DES DONNEES DE SANTE ?

REMERCIEMENTS

A Monsieur Eric Sergheraert, Directeur de thèse et Président du Jury, pour son accompagnement, ses relectures et ses conseils avisés ;

A Alizée, pour toutes ces belles années d'amitié, ta présence dans tous les moments importants de ma vie, les terrasses parisiennes ne sont pas prêtes de nous oublier ! ;

A Corentin, pour avoir accepté de faire partie de mon jury et surtout pour avoir réussi à transformer nos années d'agence en beaux souvenirs ;

A mes parents, Julie, Rob, ma famille et tous ceux qui me demandent « à quand la thèse ? » : on y est ! Un merci particulier à Maman et Papa pour leur soutien et leur présence sans faille ;

A Juliette, Justine et Justine, parce que les mojitos valent tout l'or du monde ;

A mes copains, Tristan, Thomas, Claire, Agathe, Mélanie H, Alexandre G, Mehdi, Alexandre R, pour ces belles années passées en pharma et qui font partie de ces familles qu'on choisit avec le cœur ;

A Robin, mon bel amour, hâte de construire notre avenir ensemble !

Faculté de Pharmacie de Lille

3 Rue du Professeur Laguesse – 59000 Lille
03 20 96 40 40
https://pharmacie.univ-lille.fr

L'Université n'entend donner aucune approbation aux opinions émises dans les thèses ; celles-ci sont propres à leurs auteurs.

Faculté de Pharmacie de Lille
3 Rue du Professeur Laguesse – 59000 Lille
03 20 96 40 40
https://pharmacie.univ-lille.fr

Université de Lille

Président	Régis BORDET
Premier Vice-président	Etienne PEYRAT
Vice-présidente Formation	Christel BEAUCOURT
Vice-président Recherche	Olivier COLOT
Vice-présidente Réseaux internationaux et européens	Kathleen O'CONNOR
Vice-président Ressources humaines	Jérôme FONCEL
Directrice Générale des Services	Marie-Dominique SAVINA

UFR3S

Doyen	Dominique LACROIX
Premier Vice-Doyen	Guillaume PENEL
Vice-Doyen Recherche	Éric BOULANGER
Vice-Doyen Finances et Patrimoine	Damien CUNY
Vice-Doyen Coordination pluriprofessionnelle et Formations sanitaires	Sébastien D'HARANCY
Vice-Doyen RH, SI et Qualité	Hervé HUBERT
Vice-Doyenne Formation tout au long de la vie	Caroline LANIER
Vice-Doyen Territoires-Partenariats	Thomas MORGENROTH
Vice-Doyenne Vie de Campus	Claire PINÇON
Vice-Doyen International et Communication	Vincent SOBANSKI
Vice-Doyen étudiant	Dorian QUINZAIN

Faculté de Pharmacie

Doyen	Delphine ALLORGE
Premier Assesseur et Assesseur en charge des études	Benjamin BERTIN
Assesseur aux Ressources et Personnels	Stéphanie DELBAERE
Assesseur à la Santé et à l'Accompagnement	Anne GARAT
Assesseur à la Vie de la Faculté	Emmanuelle LIPKA
Responsable des Services	Cyrille PORTA
Représentant étudiant	Honoré GUISE

Professeurs des Universités - Praticiens Hospitaliers (PU-PH)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	ALLORGE	Delphine	Toxicologie et Santé publique	81
M.	BROUSSEAU	Thierry	Biochimie	82
M.	DÉCAUDIN	Bertrand	Biopharmacie, Pharmacie galénique et hospitalière	81
M.	DINE	Thierry	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
Mme	DUPONT-PRADO	Annabelle	Hématologie	82
Mme	GOFFARD	Anne	Bactériologie - Virologie	82
M.	GRESSIER	Bernard	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
M.	ODOU	Pascal	Biopharmacie, Pharmacie galénique et hospitalière	80
Mme	POULAIN	Stéphanie	Hématologie	82
M.	SIMON	Nicolas	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
M.	STAELS	Bart	Biologie cellulaire	82

Professeurs des Universités (PU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	ALIOUAT	El Moukhtar	Parasitologie - Biologie animale	87
Mme	AZAROUAL	Nathalie	Biophysique - RMN	85
M.	BLANCHEMAIN	Nicolas	Pharmacotechnie industrielle	85
M.	CARNOY	Christophe	Immunologie	87
M.	CAZIN	Jean-Louis	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	CHAVATTE	Philippe	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	COURTECUISSE	Régis	Sciences végétales et fongiques	87
M.	CUNY	Damien	Sciences végétales et fongiques	87

Mme	DELBAERE	Stéphanie	Biophysique - RMN	85
Mme	DEPREZ	Rebecca	Chimie thérapeutique	86
M.	DEPREZ	Benoît	Chimie bioinorganique	85
M.	DUPONT	Frédéric	Sciences végétales et fongiques	87
M.	DURIEZ	Patrick	Physiologie	86
M.	ELATI	Mohamed	Biomathématiques	27
M.	FOLIGNÉ	Benoît	Bactériologie - Virologie	87
Mme	FOULON	Catherine	Chimie analytique	85
M.	GARÇON	Guillaume	Toxicologie et Santé publique	86
M.	GOOSSENS	Jean-François	Chimie analytique	85
M.	HENNEBELLE	Thierry	Pharmacognosie	86
M.	LEBEGUE	Nicolas	Chimie thérapeutique	86
M.	LEMDANI	Mohamed	Biomathématiques	26
Mme	LESTAVEL	Sophie	Biologie cellulaire	87
Mme	LESTRELIN	Réjane	Biologie cellulaire	87
Mme	MELNYK	Patricia	Chimie physique	85
M.	MILLET	Régis	Institut de Chimie Pharmaceutique Albert Lespagnol	86
Mme	MUHR-TAILLEUX	Anne	Biochimie	87
Mme	PERROY	Anne-Catherine	Droit et Economie pharmaceutique	86
Mme	ROMOND	Marie-Bénédicte	Bactériologie - Virologie	87
Mme	SAHPAZ	Sevser	Pharmacognosie	86
M.	SERGHERAERT	Éric	Droit et Economie pharmaceutique	86
M.	SIEPMANN	Juergen	Pharmacotechnie industrielle	85
Mme	SIEPMANN	Florence	Pharmacotechnie industrielle	85
M.	WILLAND	Nicolas	Chimie organique	86

Maîtres de Conférences - Praticiens Hospitaliers (MCU-PH)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	BLONDIAUX	Nicolas	Bactériologie - Virologie	82
Mme	DEMARET	Julie	Immunologie	82
Mme	GARAT	Anne	Toxicologie et Santé publique	81
Mme	GENAY	Stéphanie	Biopharmacie, Pharmacie galénique et hospitalière	81
M.	LANNOY	Damien	Biopharmacie, Pharmacie galénique et hospitalière	80
Mme	ODOU	Marie-Françoise	Bactériologie - Virologie	82

Maîtres de Conférences des Universités (MCU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	AGOURIDAS	Laurence	Chimie thérapeutique	85
Mme	ALIOUAT	Cécile-Marie	Parasitologie - Biologie animale	87
M.	ANTHÉRIEU	Sébastien	Toxicologie et Santé publique	86
Mme	AUMERCIER	Pierrette	Biochimie	87
M.	BANTUBUNGI-BLUM	Kadiombo	Biologie cellulaire	87
Mme	BARTHELEMY	Christine	Biopharmacie, Pharmacie galénique et hospitalière	85
Mme	BEHRA	Josette	Bactériologie - Virologie	87
M.	BELARBI	Karim-Ali	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	BERTHET	Jérôme	Biophysique - RMN	85
M.	BERTIN	Benjamin	Immunologie	87
M.	BOCHU	Christophe	Biophysique - RMN	85
M.	BORDAGE	Simon	Pharmacognosie	86
M.	BOSC	Damien	Chimie thérapeutique	86
M.	BRIAND	Olivier	Biochimie	87
Mme	CARON-HOUDE	Sandrine	Biologie cellulaire	87
Mme	CARRIÉ	Hélène	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86

Mme	CHABÉ	Magali	Parasitologie - Biologie animale	87
Mme	CHARTON	Julie	Chimie organique	86
M.	CHEVALIER	Dany	Toxicologie et Santé publique	86
Mme	DANEL	Cécile	Chimie analytique	85
Mme	DEMANCHE	Christine	Parasitologie - Biologie animale	87
Mme	DEMARQUILLY	Catherine	Biomathématiques	85
M.	DHIFLI	Wajdi	Biomathématiques	27
Mme	DUMONT	Julie	Biologie cellulaire	87
M.	EL BAKALI	Jamal	Chimie thérapeutique	86
M.	FARCE	Amaury	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	FLIPO	Marion	Chimie organique	86
M.	FURMAN	Christophe	Institut de Chimie Pharmaceutique Albert Lespagnol	86
M.	GERVOIS	Philippe	Biochimie	87
Mme	GOOSSENS	Laurence	Institut de Chimie Pharmaceutique Albert Lespagnol	86
Mme	GRAVE	Béatrice	Toxicologie et Santé publique	86
Mme	GROSS	Barbara	Biochimie	87
M.	HAMONIER	Julien	Biomathématiques	26
Mme	HAMOUDI-BEN YELLES	Chérifa-Mounira	Pharmacotechnie industrielle	85
Mme	HANNOTHIAUX	Marie-Hélène	Toxicologie et Santé publique	86
Mme	HELLEBOID	Audrey	Physiologie	86
M.	HERMANN	Emmanuel	Immunologie	87
M.	KAMBIA KPAKPAGA	Nicolas	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	KARROUT	Younes	Pharmacotechnie industrielle	85
Mme	LALLOYER	Fanny	Biochimie	87
Mme	LECOEUR	Marie	Chimie analytique	85
Mme	LEHMANN	Hélène	Droit et Economie pharmaceutique	86
Mme	LELEU	Natascha	Institut de Chimie Pharmaceutique Albert Lespagnol	86

Mme	LIPKA	Emmanuelle	Chimie analytique	85
Mme	LOINGEVILLE	Florence	Biomathématiques	26
Mme	MARTIN	Françoise	Physiologie	86
M.	MOREAU	Pierre-Arthur	Sciences végétales et fongiques	87
M.	MORGENROTH	Thomas	Droit et Economie pharmaceutique	86
Mme	MUSCHERT	Susanne	Pharmacotechnie industrielle	85
Mme	NIKASINOVIC	Lydia	Toxicologie et Santé publique	86
Mme	PINÇON	Claire	Biomathématiques	85
M.	PIVA	Frank	Biochimie	85
Mme	PLATEL	Anne	Toxicologie et Santé publique	86
M.	POURCET	Benoît	Biochimie	87
M.	RAVAUX	Pierre	Biomathématiques / Innovations pédagogiques	85
Mme	RAVEZ	Séverine	Chimie thérapeutique	86
Mme	RIVIÈRE	Céline	Pharmacognosie	86
M.	ROUMY	Vincent	Pharmacognosie	86
Mme	SEBTI	Yasmine	Biochimie	87
Mme	SINGER	Elisabeth	Bactériologie - Virologie	87
Mme	STANDAERT	Annie	Parasitologie - Biologie animale	87
M.	TAGZIRT	Madjid	Hématologie	87
M.	VILLEMAGNE	Baptiste	Chimie organique	86
M.	WELTI	Stéphane	Sciences végétales et fongiques	87
M.	YOUS	Saïd	Chimie thérapeutique	86
M.	ZITOUNI	Djamel	Biomathématiques	85

Professeurs certifiés

Civ.	Nom	Prénom	Service d'enseignement
Mme	FAUQUANT	Soline	Anglais

M.	HUGES	Dominique	Anglais
M.	OSTYN	Gaël	Anglais

Professeurs Associés

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
M.	DAO PHAN	Haï Pascal	Chimie thérapeutique	86
M.	DHANANI	Alban	Droit et Economie pharmaceutique	86

Maîtres de Conférences Associés

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	CUCCHI	Malgorzata	Biomathématiques	85
M.	DUFOSSEZ	François	Biomathématiques	85
M.	FRIMAT	Bruno	Pharmacologie, Pharmacocinétique et Pharmacie clinique	85
M.	GILLOT	François	Droit et Economie pharmaceutique	86
M.	MASCAUT	Daniel	Pharmacologie, Pharmacocinétique et Pharmacie clinique	86
M.	MITOUMBA	Fabrice	Biopharmacie, Pharmacie galénique et hospitalière	86
M.	PELLETIER	Franck	Droit et Economie pharmaceutique	86
M.	ZANETTI	Sébastien	Biomathématiques	85

Assistants Hospitalo-Universitaire (AHU)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	CUVELIER	Élodie	Pharmacologie, Pharmacocinétique et Pharmacie clinique	81
M.	GRZYCH	Guillaume	Biochimie	82
Mme	LENSKI	Marie	Toxicologie et Santé publique	81
Mme	HENRY	Héloïse	Biopharmacie, Pharmacie galénique et hospitalière	80
Mme	MASSE	Morgane	Biopharmacie, Pharmacie galénique et hospitalière	81

Attachés Temporaires d'Enseignement et de Recherche (ATER)

Civ.	Nom	Prénom	Service d'enseignement	Section CNU
Mme	GEORGE	Fanny	Bactériologie - Virologie / Immunologie	87
Mme	N'GUESSAN	Cécilia	Parasitologie - Biologie animale	87
M.	RUEZ	Richard	Hématologie	87
M.	SAIED	Tarak	Biophysique - RMN	85
M.	SIEROCKI	Pierre	Chimie bioinorganique	85

Enseignant contractuel

Civ.	Nom	Prénom	Service d'enseignement
M.	MARTIN MENA	Anthony	Biopharmacie, Pharmacie galénique et hospitalière

SOMMAIRE

GLOSSAIRE **15**

LISTE DES FIGURES **16**

INTRODUCTION **17**

1. La blockchain **18**
1.1 Définition et fonctionnement **18**
1.2 Blockchain publique, privée et de consortium **24**
1.3 Blockchain et santé : opportunités **27**
1.3.1 Intérêt du marché pour la Blockchain 27
1.3.2 Domaines d'application de la Blockchain 30

2. Les enjeux liés aux données de santé **33**
2.1 Définition **33**
2.2 Le dossier médical partagé **35**
2.3 Sécurité des données de santé **39**
2.4 L'interopérabilité des systèmes d'information de santé **42**

3. La réponse blockchain **47**
3.1 Blockchain de consortium **47**
3.2 Sécurité des données **48**
3.3 Stockage des données **52**
3.4 Interopérabilité et standardisation **55**
3.5 Exemples d'utilisation de blockchain en santé **58**

4. Limites et défis à relever **62**
4.1 Scalabilité et limitations pratiques **62**
4.2 Un flou réglementaire **65**
4.3 Ethique et partage des données **68**
4.4 La blockchain et l'écologie **69**

CONCLUSION **70**

BIBLIOGRAPHIE **72**

GLOSSAIRE

API : Application Programming Interface
ANSI : American Nation Standards Institute
ASIP : Agence des Systèmes d'Information Partagés
CI-SIS : Cadre d'Interopérabilité des Systèmes d'Information de Santé
CIM : Classification Internationale des Maladies
CNAM : Caisse Nationale d'Assurance Maladie
CNIL : Commission Nationale de l'Informatique et des Libertés
COFRAC : Comité Français d'Accréditation
CPAM : Caisse Primaire d'Assurance Maladie
CSP : Code de Santé Publique
DLS : Distributed Ledger Technologie
DMP : Dossier Médical Partagé
EMRAM : Electronic Medical Records Adoption Model
GIE : Groupement d'Intérêt Economique
HAS : Haute Autorité de Santé
HIMSS : Healthcare Information and Management Systems Society
HL7 : Health Level 7
HPRIM : Harmoniser et Promouvoir l'Informatique Médical
INS : Identifiant National de Santé
INS-c : Identifiant National de Santé calculé
ISO : International Organization for Standardization
OMS : Organisme Mondial de la Santé
PIA : Privacy Impact Assessment
PoS : Proof of Stake
PoW : Proof of Work
RGPD : Règlement Général relatif à la Protection des Données
RNIPP : Répertoire National d'Identification des Personnes Physiques
SI : Système Informatique
SIH : Système d'Information Hospitalier
SNOMED : Systematized Nomenclature of Medicine
TPS : Transaction Par Seconde

LISTE DES FIGURES

Figure 1 : Systèmes centralisés, décentralisés et distribués (5) 18
Figure 2 : Schématisation d'une transaction via la Blockchain (3) 19
Figure 4 : Estimation de mise en place 27
Figure 5 : Bénéfices attendus 28
Figure 6 : Barrières à l'adoption de la Blockchain 29
Figure 7 : Roadmap des projets blockchain en santé (13),(14) 30
Figure 8 : Dossier Médical Partagé 35
Figure 9 : chiffrement asymétrique (50) 49
Figure 10 : Data lake (54) 53
Figure 11 : Fonctionnement de la blockchain avec data lake 53
Figure 12 : Smart Contract (57) 55
Figure 13 : Application Programming Interface 57
Figure 14 : Fonctionnement de MedRec 60

INTRODUCTION

Depuis quelques années, la révolution numérique bouleverse le monde tel que nous le connaissons. Le digital est devenu omniprésent, indispensable et touche tous les secteurs, de la politique à la culture, en passant par l'économie et la santé.
Avec l'émergence des objets connectés, de l'intelligence artificielle ou encore du big data, les nouvelles technologies sont en train de transformer radicalement l'écosystème de santé.

La blockchain fait partie de ces technologies qui promettent d'opérer un changement dans le monde de la santé. Technologie aussi disruptive qu'Internet, capable de renverser et de moderniser les structures de santé pour certains, simple illusion pour d'autres, la blockchain est une technologie qui fait débat et qui intéresse de plus en plus d'entreprises.
Initialement développée et essentiellement connue pour son utilisation dans le domaine financier et des crypto monnaies, cette technologie de stockage et de partage d'informations présente un fort potentiel en santé. Gestion des essais cliniques, traçabilité des médicaments, lutte contre la contrefaçon et gestion des dossiers médicaux électroniques des patients, les applications de la blockchain sont nombreuses.

Grâce à son caractère décentralisé, sa transparence et garantissant l'intégrité et la sécurité des données, la blockchain promet de transformer la manière dont sont traitées, stockées et partagées les informations médicales, notamment grâce aux dossiers médicaux partagés.
Les données de santé sont des données sensibles qui doivent faire face à de nombreuses problématiques, notamment en terme de sécurité et d'interopérabilité. La blockchain peut-elle vraiment être une réponse à ces enjeux ?

Dans le cadre de cette thèse, nous découvrirons le principe et le fonctionnement de la technologie blockchain (partie 1) et les problématiques liées aux données de santé et aux dossiers médicaux électroniques (partie 2). Nous verrons ensuite quelle réponse la blockchain peut apporter (partie 3) et quelles sont ses limites (partie 4).

1. La blockchain

Dans cette première partie, nous découvrirons la technologie blockchain sa définition et son fonctionnement.

1.1 Définition et fonctionnement

Définition :

Conceptualisée pour la première fois en 2008 par une - ou plusieurs - personne connue sous le pseudonyme de Satoshi Nakamoto et utilisée en 2009 comme composante principale du Bitcoin (1), la Blockchain fait partie de ce que l'on appelle les « Systèmes de Registres Distribués » (*Distributed Ledger System* ou *DLS*).
Les DLS sont des systèmes numériques qui permettent l'enregistrement de manière synchronisée et simultanée de données, de transactions ou d'actifs sur un réseau d'ordinateurs, dans plusieurs emplacements à la fois. (2)

Selon Blockchain France, la Blockchain, littéralement « chaîne de blocs », est définie comme étant « *une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. Par extension, elle désigne une base de données sécurisée et distribuée, partagées par ses différents utilisateurs, et contenant un ensemble de transactions dont chacun peut vérifier la validité.* » (3)
A noter qu'il est important de distinguer la Blockchain comme technologie issue des travaux de Satoshi Nakamoto d'une blockchain spécifique, comme les blockchains publiques Bitcoin ou Ethereum par exemple.

Le mathématicien Jean-Paul Delahaye illustre parfaitement le concept blockchain : il faut imaginer un « *très grand cahier qu'il est possible de lire librement et gratuitement, dont tout le monde aurait une copie et sur lequel tout le monde pourrait écrire, mais qui soit impossible à effacer et indestructible.* » (4)

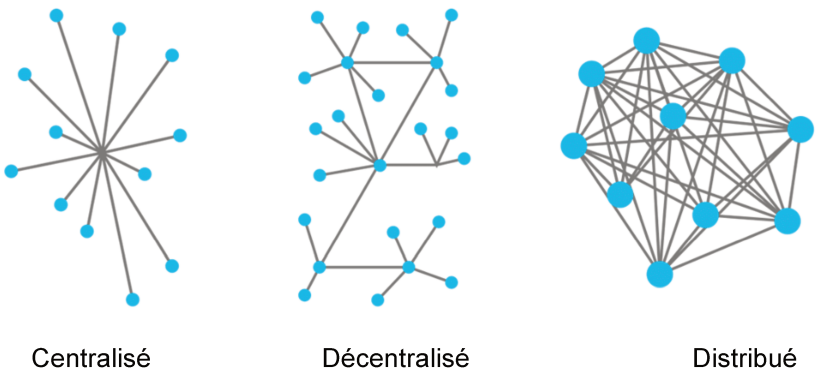

Figure 1 : Systèmes centralisés, décentralisés et distribués (5)

On peut utiliser la technologie de différentes manières :

- Transferts d'actifs : utilisation monétaire (crypto monnaies), titres, votes en ligne, actions, obligations, etc.,

- Registre, base de données sécurisée : stockage de données qui soient facilement traçables et sécurisées

- Smart contracts : programmes autonomes qui exécutent automatiquement les conditions et les termes d'un contrat (*voir partie III. d.*)

Fonctionnement :

Pour illustrer le fonctionnement de la Blockchain, nous prendrons un exemple de transaction de monnaie entre 2 personnes, A et B.

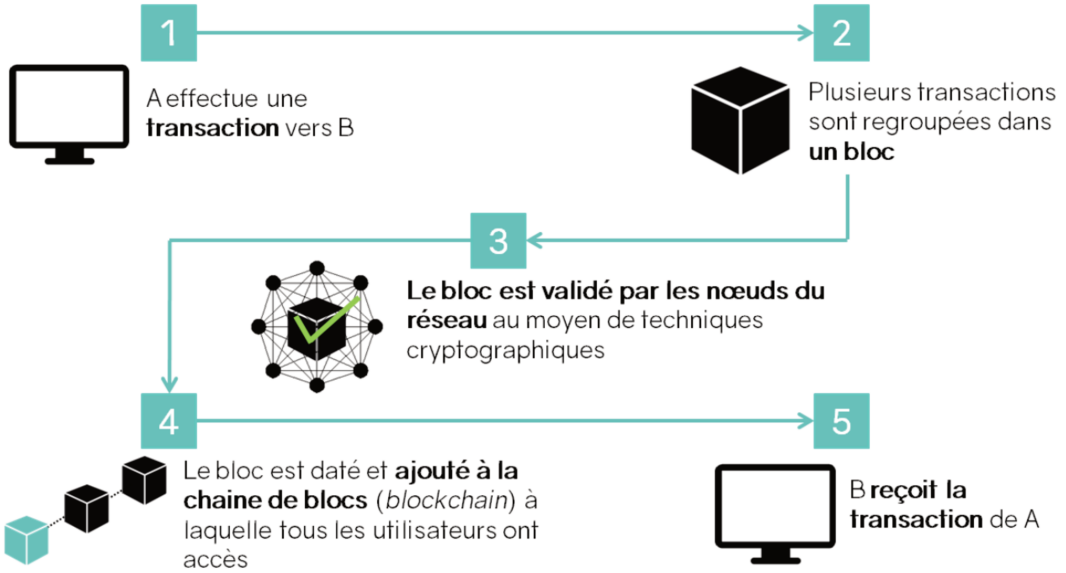

Figure 2 : Schématisation d'une transaction via la Blockchain (3)

La transaction s'effectue en plusieurs étapes :

1. A souhaite effectuer une transaction vers B.

2. Une nouvelle transaction est créée et rejoint un pool de transaction en attente, dans un réservoir temporaire. Les transactions sont ensuite extraites et regroupées pour former un bloc, qui sera crypté grâce à une fonction de hachage.

3. Le nouveau bloc est validé par les nœuds du réseau grâce à des techniques cryptographiques, c'est ce qu'on appelle l'étape de minage. Le but des mineurs, les personnes qui valident les blocs et qui veillent à la fiabilité et à l'exactitude du réseau, est d'arriver à un consensus en résolvant des algorithmes mathématiques complexes.

4. Une fois validé, le bloc ne peut plus être modifié ; il est ajouté à la chaîne de blocs et accessible par tous les utilisateurs.

5. B peut enfin recevoir la transaction de A.

Fonction de hachage et minage :

L'étape de minage, de validation des blocs, est indispensable au fonctionnement d'une blockchain, et permettent d'assurer la validité des échanges.

Une fonction de hachage (de l'anglais « *hash* » par analogie avec la cuisine) est une fonction mathématique particulière qui permet, à partir d'une donnée fournie, de calculer une empreinte, un *hash*. Ce *hash* représente l'identité de la donnée, et permet de l'identifier rapidement.
Par exemple, si on prend le mot « blockchain » et qu'on y applique une fonction de hachage, on obtiendra une série de chiffres et de lettres (d'une longueur dépendante de la fonction utilisée) unique qui correspond à son *hash*. Le mot « Blockchain » ici avec une majuscule possèdera un *hash* différent.

Il est impossible de retrouver spontanément la donnée d'entrée à partir de son *hash*. Le seul moyen est d'y aller à la « force brute », c'est à dire de tester, une par une, toutes les combinaisons qui permettraient de retrouver la fonction d'entrée.

Cette phase de test correspond à l'étape de minage. Il faut imaginer le minage comme un concours de mathématiques géant : chaque participant, les mineurs, tentent de résoudre le plus rapidement un algorithme mathématique de la fonction hachage, à partir du *hash* du bloc précédent. Cela demande une puissance de calcul conséquente pour arriver au résultat final.
C'est lorsque que l'algorithme est résolu, que les mineurs sont arrivés à un consensus, que le bloc pourra être validé et rajouté sur la chaîne.
Chaque bloc est horodaté (*timestamp*), possède un hash propre et unique qui prouve son identité et qui le relie au bloc précédent. Chaque bloc est en quelque sorte « photographié » dans le temps, ce qui permet de ne pas douter de son identité, qui le rend immuable et traçable.

Ce procédé de minage par calcul et résolution d'algorithmes est ce qu'on appelle le *Proof-of-Work* (*PoW*), la « preuve de travail ». Les mineurs doivent fournir la preuve

qu'ils ont suffisamment « travaillé », c'est à dire qu'ils ont suffisamment mis leur puissance de calcul à contribution, pour valider le bloc. La validation est alors considérée comme « honnête », ce qui permet de s'assurer de l'intégrité des données.
La complexité des calculs est augmentée tous les 2016 blocs selon la puissance globale des mineurs, afin de s'assurer que les mineurs fournissent toujours un effort suffisant.

La méthode de validation par *PoW* est la méthode utilisée sur la blockchain Bitcoin, l'une des premières crypto monnaies à avoir vu le jour.
Certaines chaînes souhaitent mettre en place d'autres méthodes de validation, qui demandent moins de ressources en matière de calcul. C'est par exemple le cas d'Ethereum, blockchain publique qui a émis sa propre crypto monnaie, l'Ether, qui va installer la validation par « *Proof-of-Stake* » (*PoS*), la « preuve d'enjeu ». Cela demandera de prouver que les ressources des utilisateurs sont suffisantes lorsqu'ils souhaitent effectuer une transaction.

Afin d'inciter à participer à ce grand concours qu'est l'étape de minage, les mineurs se voient attribuer des « prix » pour leur travail. Dans le cas du Bitcoin, les mineurs reçoivent un certain montant de crypto monnaies comme récompense.

Il peut arriver que 2 mineurs résolvent et valide un bloc quasiment en même temps et qu'ils n'aient pas eu le temps d'être informés de la validation par l'autre. Une nouvelle branche sera alors créée.

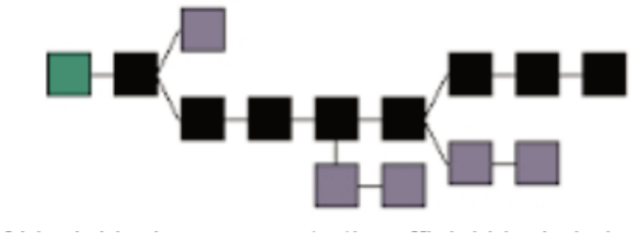

Figure 3 : Branches d'une blockchain

La règle qui prévaut et qui est suivie par l'ensemble du réseau est que seule la chaine la plus longue compte. Les branches secondaires, en gris sur le schéma, sont abandonnées.

Ainsi, si un mineur « malhonnête » souhaite ajouter des informations et/ou modifier une transaction réalisée par un mineur précédent, il devra créer une banche plus longue que la branche principale. Il devra donc générer suffisamment de blocs, et ce assez rapidement, pour que sa branche devienne branche principale.
Or, la création de nouveaux blocs dépend de la puissance de calculs des mineurs. Le mineur malveillant devra donc posséder à minima 51% de la puissance du réseau pour valider ses blocs et ainsi devancer les autres mineurs.

Le caractère décentralisé de la blockchain, le fait que chaque utilisateur possède une copie de la chaîne et la complexité des algorithmes de calcul rendent ce scénario hautement improbable. A ce jour, ce qu'on appelle « l'attaque 51% », n'a jamais aboutie.
Cela assure l'immuabilité des transactions et permet d'avoir une chaîne de blocs uniques et non modifiables.

Une blockchain qui sert uniquement de base, de stockage de données fonctionne de manière identique : chaque nouvelle donnée sera intégrée dans un bloc, qui sera vérifié par les mineurs afin d'avoir une donnée cohérente, qui ne puisse pas entrer en conflit avec les données préalablement enregistrées. Le bloc contenant l'information sera finalement intégré à la blockchain et consultable par les utilisateurs.

A quel besoin répond la blockchain ?

La réponse à cette question tient en quelques mots : le besoin de confiance.

Reprenons l'exemple d'une transaction de monnaie entre 2 personnes, A et B. Si A est face à B et qu'il souhaite lui donner un certain montant d'argent « physique », B peut directement voir si A possède bien cette somme.
Si maintenant A souhaite faire une transaction à B de manière numérique, comment B peut-il être certain qu'A possède bien la somme qu'il souhaite lui donner ? Intervient alors la personne que l'on appelle le « tiers de confiance ». Le tiers de confiance, comme les banques par exemple, sont là pour vérifier que A possède bien le montant indiqué et qu'il est transférable à B. Ce tiers de confiance possède un certain pouvoir sur les transactions, et peut par exemple décider de les annuler.
Mais alors comment faire si, maintenant, on ne fait pas confiance à cette tierce personne ?

C'est en réponse à cette question que la blockchain a été créé. Les chaînes sont des systèmes « *peer-to-peer* », de pair-à-pair, qui permettent de s'affranchir du tiers de confiance. Toutes les transactions sont validées et visibles par l'ensemble du réseau. Le système Bitcoin permet par exemple de s'affranchir des banques.
La blockchain permet aux utilisateurs « d'avoir confiance sans confiance ». Il n'y a pas de confiance entre utilisateurs, mais une confiance dans la technologie qui valide méthodiquement les blocs et donc une confiance dans les données qui y sont inscrites.

En résumé, la blockchain est donc une technologie qui est :

- **Décentralisée** : le réseau « *peer-to*-peer » fonctionne sans organe central de contrôle, où un tiers de confiance n'est plus nécessaire pour valider une transaction ou une information.

- **Partagée et transparente** : chaque utilisateur possède une copie de la blockchain et peut avoir accès à tous les blocs de données de manière libre.

- **Immuable et sécurisée** : une fois validés, les blocs cryptés sont infalsifiables et ne peuvent être supprimés de la chaine. Ce caractère immuable garantit la traçabilité des données d'une blockchain.

Dans la prochaine partie, nous verrons qu'il existe plusieurs formes de blockchain, chacune ayant des caractéristiques spécifiques.

1.2 Blockchain publique, privée et de consortium

Il existe plusieurs types de blockchain, qui, bien qu'elles reposent sur des principes similaires, se différencient en fonction de leur accessibilité, de leur fonctionnement et du niveau de confiance entre chaque utilisateur. (6)
Ainsi, plus le niveau de confiance entre les utilisateurs est faible plus le consensus à atteindre lors du minage et le niveau de sécurité sont élevés ; plus le niveau de confiance est élevé, plus le consensus sera rapide à atteindre, moins demandeur en puissance de calcul, moins coûteux et les transactions plus rapides.

- **Blockchain publique :**

Ce type de blockchain est la blockchain dite « historique », créée par Satoshi Nakamoto, et dont les exemples les plus connus sont ceux du Bitcoin (7) et d'Ethereum (8).
C'est un système open source, où n'importe qui peut devenir membre du réseau, accéder à la chaîne et effectuer des transactions sans condition d'admission. Autrement dit, chaque personne qui souhaite utiliser et participer à ce type de blockchain peut le faire localement, sur son ordinateur, et sans avoir à révéler son identité (système d'anonymisation, notamment grâce au chiffrement asymétrique (*voir partie III. b.*)).
Il suffit, afin de devenir membre, de télécharger le protocole correspondant à la chaîne (i. e. la « charte interne » qui définit les règles régissant le réseau) et d'avoir un accès à internet.

De même, chaque personne peut devenir un mineur et mettre à contribution sa puissance informatique pour participer à la validation des blocs. Ici, le niveau de confiance entre utilisateurs étant très faible voire nul (puisque les utilisateurs sont inconnus), le processus de minage demande une puissance importante de calcul.

La blockchain publique est donc une blockchain totalement décentralisée, libre et transparente, mais qui présente plusieurs inconvénients :

- Taille limitée des blocs : le nombre de transactions pouvant être contenu dans un bloc est limité, chaque bloc ne pouvant faire plus de 1 MB.

- Lenteur : conséquence directe de la limitation de taille, les transactions mettent du temps à être ajoutée sur la blockchain. Par exemple, le protocole Bitcoin ne permet l'ajout d'un bloc que toutes les 10 minutes.

- Coût de transaction élevé : comme expliqué précédemment, un système de récompense est mis en place pour inciter les mineurs à participer de manière

honnête et pour leur permettre de rembourser et rentabiliser les coûts personnels engendrés (électricité, matériel informatique puissant, connexion internet). Sur la chaîne Bitcoin, les mineurs reçoivent 1,25 bitcoins par bloc validés auxquels s'ajoutent des frais de transactions payés par l'utilisateur.

Bien que lente et coûteuse, une blockchain publique a l'avantage de garantir entièrement la sécurité et l'intégrité des données : annuler ou modifier une transaction requiert une trop grande puissance de calcul (principe de « l'attaque 51%).

- **Blockchain privée :**

Si le caractère décentralisé et sécurisé de la blockchain en fait une technologie innovante et disruptive, beaucoup craignent le côté public nécessaire à cette décentralisation et à la validation des données.
Est alors progressivement apparu le concept de « blockchain privée », qui permet de contrôler l'accès, la lecture et la vérification du registre tout en gardant l'authenticité et la sécurité d'une blockchain publique.
La blockchain privée est en opposition totale avec la blockchain publique, puisqu'elle perd son caractère décentralisé, et revient en quelque sorte à rétablir une autorité centrale.

Ainsi, le mécanisme de minage est concentré dans les mains d'une seule entité, qui aura pour mission de vérifier et de valider toutes les transactions effectuées sur la chaîne. Il n'y a donc plus besoin de mettre en place des techniques de minages utilisées par les blockchains publiques comme le « *Proof of Work* » ou le « *Proof of Stake* ».

Ce contrôle présente plusieurs avantages :

- Absence de frais : le minage étant réalisé par une seule entité, les coûts liés aux récompenses des mineurs n'existent plus dans le cadre d'une blockchain privée.

- Maitrise du registre : de même, le fait qu'une seule entité valide les blocs permet de revenir à tout moment sur une transaction déjà validée, bien que cela risquerait de casser la chaîne. Cependant, la maitrise des blockchains privées influe sur la sécurité du registre : il devient alors plus facile de l'attaquer et de récupérer des données.

- Rapidité des transactions : le consensus étant plus simple à atteindre, les blocs sont plus rapidement validés et ajoutés à la chaîne. De plus, l'entité

« centrale » qui contrôle le registre peut décider d'augmenter la taille des blocs et ainsi augmenter encore plus la rapidité des transactions.

- Privatisation des données : l'entité en charge de l'administration peut décider de limiter les accès et de ne pas rendre les transactions publiques.

- **Blockchain de consortium :**

La blockchain de consortium est similaire à une blockchain privée, si ce n'est qu'elle n'est pas gérée par une entité unique, mais par un réseau pré-sélectionnés (entreprises, administrations etc.).
Ce type de blockchain hybride associe les avantages d'une blockchain privée, soit la rapidité, le coût et la privatisation des données, tout en augmentant son niveau de sécurité, puisque le minage sera effectué par plusieurs entités.

Si l'on voulait faire une comparaison, on pourrait considérer la blockchain publique comme l'équivalent d'internet, libre et accessible à tous, et les blockchains privées et de consortium comme des intranets, plus restreints mais plus confidentiels.

Considérés comme une « hérésie » par certains, les blockchains privées et de consortium permettent de répondre aux exigences réglementaires et de confidentialité qu'ont certaines institutions, financières ou non. Ce type de blockchain serait particulièrement adapté au monde de la santé.

Le fonctionnement et les types de blockchain maintenant définis, nous découvrirons quelles sont les opportunités que présente une technologie comme la Blockchain dans l'univers de la santé (partie 1.3).

1.3 Blockchain et santé : opportunités

Souvent associée au Bitcoin et au monde de la finance où elle est présentée comme une technologie révolutionnaire qui remet en cause les structures bancaires et monétaires actuelles, la blockchain est une technologie qui présente des applications dans beaucoup de domaines différents, allant de l'industrie agroalimentaire, en passant par les transports, l'énergie, jusqu'à l'industrie pharmaceutique et de santé.
Utilisée en tant que base de données garantissant la véracité des informations enregistrées, la blockchain possède un fort potentiel disruptif et permettrait de répondre aux exigences de traçabilité et de sécurité qui sont nécessaires dans le monde de la santé.

Le laboratoire Sanofi, qui a pour projet d'utiliser la blockchain pour conduire leurs essais cliniques, s'est d'ailleurs récemment exprimé sur l'arrivée de cette nouvelle technologie : « *Il est possible de multiplier à l'infini ses applications et de l'utiliser pour conduire des essais cliniques, accélérer l'approbation des nouveaux traitements, réduire les risques de contrefaçon et renforcer la transparence des coûts.* » (9)

1.3.1 Intérêt du marché pour la Blockchain

La technologie blockchain présente un fort potentiel dans la santé, mais ne pourra se mettre en place que si les différents acteurs du marché s'y intéressent.

Une étude menée par IBM sur 200 organisations de santé (industries, institutions etc.) dans 16 pays démontre que 16% des répondants souhaitent mettre en place une solution avec blockchain d'ici 2018. (10) Ce sont les pionniers (*trailblazers)* de l'utilisation de la technologie en santé, ceux qui donnent l'impulsion et qui seront massivement suivis (*mass adopters*).

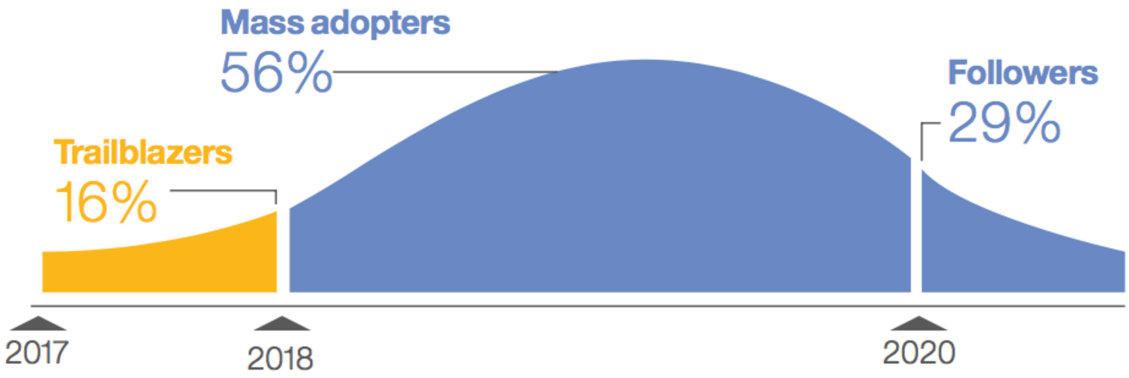

Figure 4 : Estimation de mise en place

Parmi ces pionners, 6 sur 10 estiment que la Blockchain leur permettra d'accéder à des nouveaux marchés et 7 sur 10 attendent des bénéfices dans les essais cliniques, sur la compliance réglementaire et sur les dossiers médicaux.

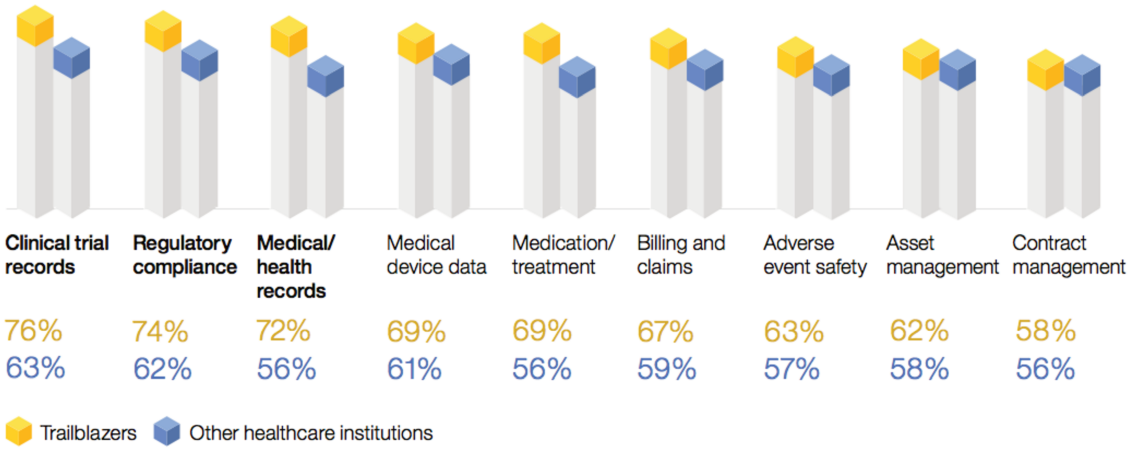

Figure 5 : Bénéfices attendus

La plupart des répondants, les *mass adopters*, préfèrent attendre quelques années avant d'utiliser une blockchain afin d'avoir un peu de recul sur ce qui aura déjà été fait, que la technologie soit éprouvée.

Les freins à l'utilisation d'une blockchain seraient, entre autres, la jeunesse de la technologie, les compétences insuffisantes des différents acteurs dans le domaine, les contraintes réglementaires, et le manque de business cases suffisamment développés.

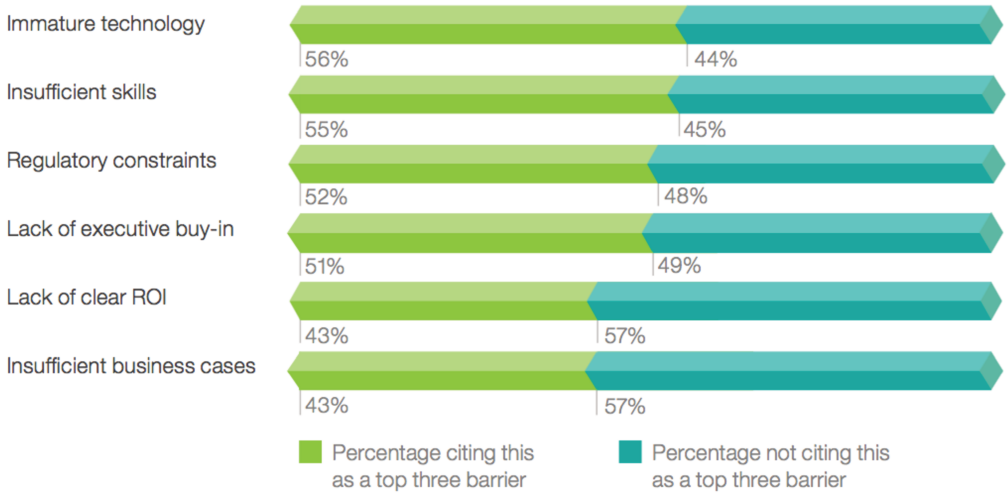

Figure 6 : Barrières à l'adoption de la Blockchain

Une nouvelle étude de PwC (PricewaterhouseCoopers) confirme l'intérêt des acteurs de la santé pour la blockchain : sur une étude menée sur 74 industries pharmaceutiques en 2018, 84% des répondants admettent qu'ils sont activement impliqués et presque 50% affirment actuellement travailler avec une solution blockchain. (11),(12)

1.3.2 Domaines d'application de la Blockchain

La Blockchain présente de nombreuses applications dans le monde de la santé, qui pourront être mises en place à plus ou moins long terme, en fonction du nombre d'acteurs impliqués, du nombre d'utilisateurs (scalabilité) et du volume de données et de transactions à gérer.

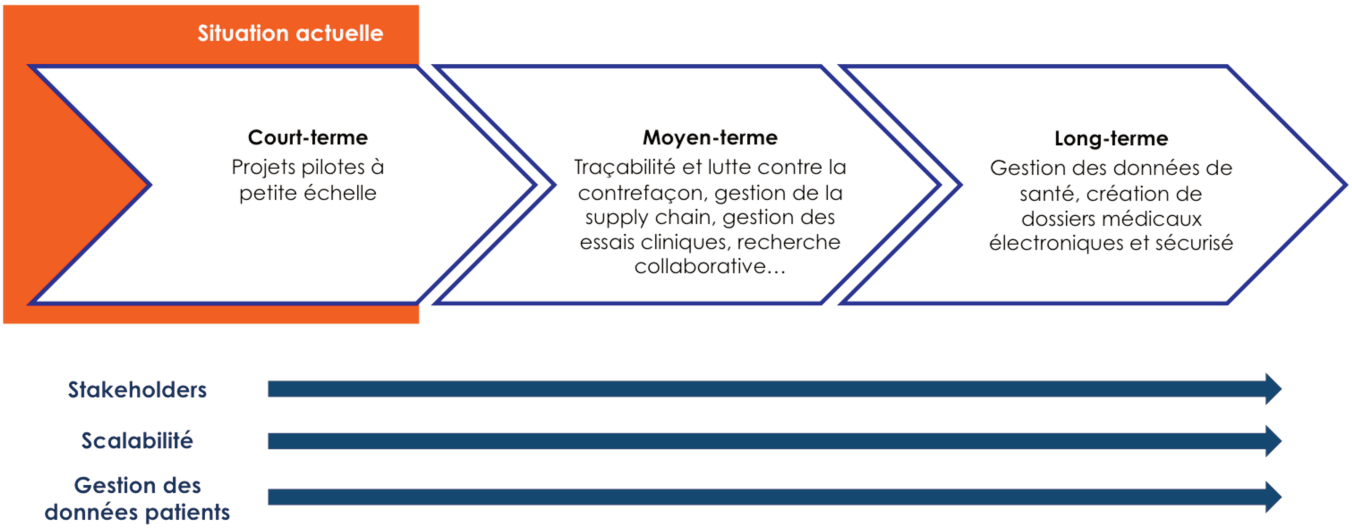

Figure 7 : Roadmap des projets blockchain en santé (13),(14)

Les applications à long terme demanderont plus d'investissements et de coordination de la part des acteurs de santé (*stakeholders*) avec un flux important de données de santé pour en faire des projets de grande envergure.

Il n'existe pas encore, à ce jour, de projet blockchain grande échelle concrètement établi dans le monde de la santé, la technologie étant encore trop récente. La plupart des projets sont encore au stade pilote ou en phase d'expérimentation.
De plus en plus d'industrie s'intéressent à cette technologie et souhaiteraient l'intégrer dans leurs stratégies digitales, comme le montre Sanofi Ventures qui vient d'investir dans Curisium, une start-up californienne qui développe une solution blockchain. (15)

Un certain nombre d'applications sont envisagées par l'Industrie Pharmaceutique à moyen terme (partie 1.3.2.1) et à plus long terme (partie 1.3.2.2) notamment autour de la gestion et du partage des données de santé.

1.3.2.1 Projets à moyen-terme

Lutte contre la contrefaçon et traçabilité des médicaments :

Grâce à ses propriétés de transparence et son immuabilité, la blockchain peut être un atout dans la lutte contre les faux médicaments en permettant de vérifier les origines des produits distribués et les ordonnances.
L'Organisation Mondiale de la Santé (OMS) estime qu'en 2018, au moins 1 médicament sur 10 dans les pays à pauvres et moyens revenus est une contrefaçon, ce qui coûterait plus de 38 millions de dollars chaque année au système de santé. (16),(17)
L'industrie pharmaceutique a donc tout intérêt à lutter contre les faux médicaments. Mettre en place une blockchain permettrait de tracer chaque action liée à un médicament, vérifier leur provenance et leur intégrité et ce, à chaque étape du processus de fabrication et de distribution.
Cette initiative ne serait pas forcément nécessaire dans les pays développés comme la France où la traçabilité des médicaments est déjà assurée avec la mise en place du code CIP, mais serait intéressante pour d'autres pays moins développés qui font face à de nombreux problèmes de contrefaçon.

Gestion de la supply chain :

De la même manière que pour la lutte contre la contrefaçon, la blockchain permettrait d'améliorer la gestion de la supply chain en permettant la traçabilité des matières premières, des substances actives et en permettant de vérifier si la chaîne du froid est correctement respectée.
De plus, une blockchain permettrait de simplifier les contraintes administratives liées à la supply chain. Chaque étape logistique serait visible en temps réel par l'ensemble des acteurs de la supply chain, ce qui rendrait sa gestion plus fluide.

Gestion des essais cliniques :

Les essais cliniques sont un processus longs, coûteux, incertains mais indispensables pour assurer l'efficacité et la sureté d'un médicament.
L'industrie pharmaceutique doit faire face à plusieurs enjeux concernant les essais cliniques : la reproductibilité, le partage et la confidentialité des données, le recrutement des patients et les coûts qui sont de plus en plus élevés. Une étude récente a démontré que seul 16% des patients étaient au courant des essais cliniques en cours lorsqu'ils recherchaient les différentes options de traitement. (18)
Utiliser un registre distribué comme une blockchain permettrait aux patients en recherche de traitements de mettre à disposition leurs données afin que les recruteurs puissent les voir et inclure les patients correspondants à leurs besoins dans différents essais cliniques.

Cela permettrait également aux différents acteurs d'un essai clinique d'accéder aux données en temps réel, de pouvoir les partager de manière totalement sécurisée et confidentielle et ainsi réduire la durée d'un essai clinique en supprimant le temps perdu lié au transfert de données.
Trois grands acteurs pharmaceutiques, Amgen, Pfizer et Sanofi, réfléchissent actuellement ensemble sur la manière d'implémenter une blockchain dans leurs essais cliniques, afin d'essayer de réduire les coûts et donc de diminuer le prix des médicaments.

Rendre la recherche plus collaborative :

Toujours dans une logique de transparence et de partage, la blockchain permettrait de mettre en place un modèle de recherche plus collaboratif et plus efficient.
Les chercheurs pourraient se partager leurs travaux et leurs données, faire des remarques et des suggestions. Chacun serait ensuite rémunéré à la hauteur de son implication dans les différentes recherches.

1.3.2.2 Projets à long-terme

Les applications à long terme concernent la gestion des données de santé, notamment celles contenues dans les dossiers médicaux des patients. Ce sont les projets les plus ambitieux et certainement les plus complexes, mais ce sont ceux qui seront directement profitables aux patients et aux professionnels de la santé.

Grâce à la blockchain, il sera possible de mieux gérer les données de santé de manière totalement sécurisée, de partager les informations entre les différents acteurs de santé et d'améliorer l'interopérabilité des systèmes de santé.

Dans le cadre de cette thèse, nous étudierons comment la technologie permet de créer un dossier médical patient, électronique et unique, avec des données qui soient partageables afin d'améliorer la coordination et le parcours de soin du patient ; et à quels défis ce type de système décentralisé devra faire face.

Pour cela, nous découvrirons au préalable, dans la partie suivante, comment définir et caractériser les données de santé (partie 2.1), leur utilisation au sein des dossiers médicaux partagés (partie 2.2), quel cadre juridique permet d'assurer leur sécurité (partie 2.3) et comment l'interopérabilité des systèmes informatiques est indispensable à leur partage (partie 2.4).

2. Les enjeux liés aux données de santé

Définir une donnée de santé n'a pas toujours été aisé. Nous verrons dans la partie suivante (partie 2.1) comment certains organismes, comme la Commission Nationale de l'Informatique et des Libertés (CNIL), ont permis d'apporter un éclairage sur cette notion.

2.1 Définition

Pendant longtemps, les professionnels de santé, les autorités de santé et les juristes ont essayé de donner une définition officielle à la notion de donnée relative à la santé, jusque-là sans succès.
Le Règlement Général relatif à la Protection des Données (RGPD) a permis de combler ce vide et défini la donnée de santé comme étant « *une donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne.* » (19)

La Commission Nationale de l'Informatique et des Libertés (CNIL) vient compléter cette définition un peu large en précisant que 3 types de données sont considérées comme données de santé (20) :

- Les données de santé par nature : antécédents médicaux, maladies, résultats d'examens, traitements, handicap, prestations de soins réalisés, etc.

- Les données qui deviennent données de santé une fois croisées avec d'autres informations et qui permettent d'obtenir une information sur l'état de santé d'une personne : croisement d'une mesure de poids avec un apport calorique par exemple, croisement d'une mesure de tension avec un test à l'effort, etc.

- Les données qui deviennent données de santé en raison de leur destination et de leur utilisation sur le plan médical.

Cette définition ne comprend pas les données de santé dont on ne peut tirer une information sur l'état de santé de la personne concernée (exemple : nombre de pas collectés sur une application sans croisement avec d'autres données).

Les données de santé sont des informations personnelles et sensibles, auxquelles un certain nombre de législations s'appliquent :

- Loi Informatique et Libertés (art. 8 et chapitre IX)
- Dispositions sur le secret médical (art. L- 1110-4 du CSP)

- Dispositions sur les référentiels de sécurité et d'interopérabilité des données de santé (art. L 1110-4-1 du CSP)
- Dispositions sur l'hébergement des données de santé (art. L 1111-8 et R. 1111-8-8 et s. du CSP)
- Dispositions sur la mise à disposition des données de santé (art. L. 1460-1 et s. du CSP)
- Interdiction de céder ou d'exploiter les données dans un but commercial (art. L. 1111-8 du CSP, art. L. 4113-7 du CSP)

A noter que ces différentes législations ne s'appliquent pas aux données de santé qui sont utilisées exclusivement à des fins personnelles, notamment pour les applications mobiles qui proposent la collecte et l'enregistrement de données de manière locale.

C'est donc ce type de données sensibles que l'on va retrouver dans les dossiers médicaux électroniques et notamment dans le Dossier Médical Partagé, que nous aborderons dans la partie 2.2 et qui montre toute la complexité que représente la mise en place d'un dossier médical électronique unique par patient.

2.2 Le dossier médical partagé

Créé en 2004 par la loi n°2004-810 relative à l'Assurance Maladie (21), le Dossier Médical Partagé (DMP) est un « *carnet de santé numérique gratuit, confidentiel et sécurisé qui conserve les informations de santé du patient (traitements, résultats d'examens, pathologies, allergies…).* » (22)

Le but du DMP est de faciliter l'échange des données des patients entre professionnels de santé de manière sécurisée, pour éviter les actes redondants, les risques d'accidents médicaux comme les risques anesthésiques et les interactions médicamenteuses. Selon la Loi de modernisation du système de santé, cet outil numérique est destiné à « *favoriser la prévention, la qualité, la continuité et la prise en charge coordonnée des soins des patients.* » (23)

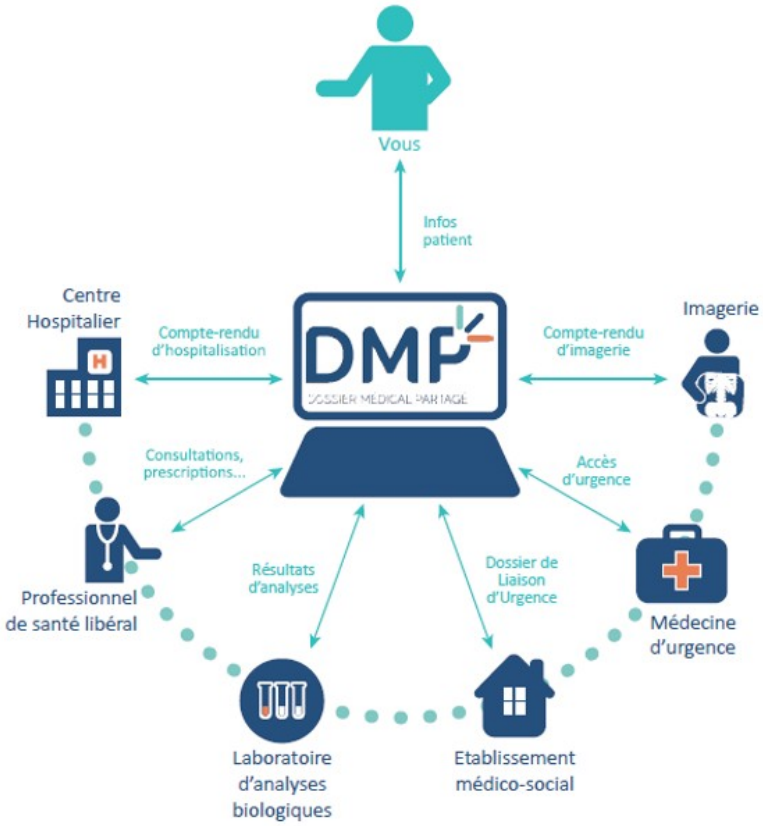

Figure 8 : Dossier Médical Partagé

Le DMP contient plusieurs types d'informations :

- L'identification du patient avec l'Identification National de Santé (INS), numéro patient unique (*voir partie III. b.*),
- L'identité et les coordonnées du médecin traitant,

- Les personnes à contacter en cas d'urgence,
- L'historique des remboursements sur les six derniers mois,
- Les comptes rendus de consultation médicale,
- Les imageries médicales,
- Les actes diagnostiques, thérapeutiques et les traitements en cours,
- Le carnet de vaccination,
- Les directives associées au don d'organe,
- Les coordonnées de la personne de confiance du patient.

Les Dossiers Médicaux Partagés peuvent être créés par le patient lui même, par tout professionnel de santé lors d'une consultation (en ville et à l'hôpital) ou par le personnel de l'Assurance Maladie. La création se fait en ligne, sur le site du DMP.
Toute création d'un dossier nécessite le consentement express et éclairé du patient.

Le patient peut décider d'ouvrir ou non l'accès à son dossier aux différents professionnels de santé, et de masquer certaines informations s'il le souhaite. Les services d'urgences peuvent accéder à la totalité du dossier si le patient en a autorisé l'accès.
De même, le patient peut décider à tout moment de clôturer son dossier ; les données enregistrées seront conservées pendant 10 ans avant la destruction définitive du dossier.

Historique du DMP :

L'histoire du DMP est un peu tumultueuse, reflet de la complexité du partage de données entre les différents acteurs de santé.

La création du Dossier Médical Partagé en 2009, alors appelé « Dossier Médical Personnel », est confiée à l'Agence des Systèmes d'Information Partagés (ASIP), une agence gouvernementale chargée de développer la e-santé et soutenir l'innovation.
La première version du DMP est lancée en 2011, mais c'est un échec : le déploiement est lent, l'échange de données de santé est alors un sujet sensible et la mise en place est jalonnée de problèmes techniques.
Bilan : en 2016, seuls 500 000 patients ont ouvert un DMP contre 5 millions prévus, alors que les dépenses de l'Etat s'élèvent à presque un demi milliard d'euros. (24)

Cependant, le gouvernement croit au projet du Dossier Médical Partagé et des bénéfices qu'il procurerait. En 2016, le Dossier Médical Personnel est refondé avec la Loi de modernisation du système de santé et devient le Dossier Médical Partagé.
Le développement est alors confié à la Caisse Nationale d'Assurance Maladie (CNAM) qui prévoit quelques améliorations, comme ne plus restreindre la création du dossier aux médecins et laisser la possibilité au patient de le faire par lui même. Un

projet pilote est lancé sur 9 départements en 2017, afin de tester l'adhésion des patients et du personnel médical.
Les pharmaciens touchent un intéressement à chaque création de dossier (1 euro par DMP), les Caisses Primaires d'Assurance Maladie (CPAM) sont poussées à aussi en ouvrir, mais il n'est pour l'instant pas prévu d'intéressement pour l'ouverture de dossier par des médecins.

Le DMP est finalement lancé sur tout le territoire depuis le 6 Novembre 2018, l'objectif étant d'atteindre 40 millions de dossiers ouverts en 2022. Actuellement, 1,9 millions de français auraient un dossier ouvert (25).

Objectifs du DMP :

Le but du Dossier Médical Partagé est d'augmenter le rôle du patient dans la gestion de ses données médicales, et d'améliorer la coordination des soins. C'est également d'essayer de réduire les erreurs liées à l'identification du patient, de réduire les coûts dus aux actes redondants et aux hospitalisations causées par des erreurs médicales.

Plusieurs enquêtes réalisées aux Etats-Unis, dont celles menées par l'Institut de médecine américain (26) et l'Harvard Medical Practice Study (27), ont démontré que les erreurs médicales sont responsables de plus de décès que les accidents de la route ou que certains cancers comme le cancer du sein. Surtout, ces études démontrent que la moitié de ces erreurs étaient évitables.
En France, l'Enquête Nationale sur les Evènements Indésirables graves liés aux Soins (ENEIS) réalisée en 2004 arrive à des conclusions similaires : 35 à 45% des hospitalisations liées à des effets indésirables graves sont évitables, soit 125 000 à 205 000 hospitalisations par an. (28)
L'erreur d'identification du patient est l'une des principales sources d'erreurs évitables (soins inappropriés, erreurs médicamenteuses, accidents transfusionnels etc.). (29)

On parle également de 25% à 30% d'actes médicaux non pertinents, c'est à dire non nécessaires et inappropriés selon les besoins du patient (30) ou redondants au regard des antécédents du patient.

Lors de la présentation du projet en 2004, les économies réalisables grâce à l'instauration du Dossier Médical Partagé étaient estimées à 3,5 milliards d'euros par an selon l'ancien Ministre de la Santé, Philippe Douste-Blazy, bien que le Ministère actuel n'ait jamais reparlé de ce chiffre. (25)

Raisons de l'échec :

On comprend bien l'intérêt du Dossier Médical Partagé, tant pour le patient qui pourra facilement avoir accès à son historique médical que pour les médecins qui auront toutes les informations nécessaires pour mieux prendre en charge leur patient et limiter les erreurs. Alors pourquoi un tel échec lors du premier lancement du DMP ?

En dehors du côté chronophage nécessaire pour le remplir et le maintenir à jour, l'échec du DMP peut être lié à deux causes principales :

- La méfiance des patients et du corps médical vis-à-vis de l'utilisation des données de santé et de leur sécurité

- Le manque d'interopérabilité entre les logiciels métiers utilisés par les professionnels de santé, en ville et à l'hôpital

Ces deux problématiques sont, de manière plus générale, représentatives des enjeux liés à la gestion et au partage des données de santé entre les acteurs du système de santé.

Les parties suivantes permettront d'aborder plus en détails ces problématiques : la sécurité des données de santé (partie 2.3) et l'interopérabilité des systèmes informatiques de santé (partie 2.4).

2.3 Sécurité des données de santé

La sécurité des données personnelles de santé est l'un des enjeux majeurs dans le monde de la santé. Considérées par certains comme le « nouvel or noir du XXIème siècle » (31), les données de santé, particulièrement l'ensemble d'un dossier médical patient, sont très convoitées par certains hackers.
Un rapport d'Intel Security estime qu'une donnée de santé seule se vend entre quelques centimes et 2,42$, alors qu'un dossier médical complet, avec informations individuelles, numéro de Sécurité Sociale etc., se vend entre 14 et 25$ sur le marché noir (32). A titre de comparaison, une carte de crédit se vend entre 4 et 5$.

La sécurité des données semble être le point qui inquiète le plus les patients et les professionnels de santé.
Si 69% de la population est favorable à l'ouverture du DMP (33) et que 72% des Français sont convaincus qu'utiliser des données de santé puisse faire avancer la recherche médicale et améliorer la santé de tous, seuls 10% sont convaincus par l'encadrement législatif assurant la sécurité de leurs données. (34)
De même, l'étude réalisée par le cabinet Care Insight dans le cadre de la campagne « Faire avancer la santé numérique » révèle que plus de 70% des acteurs de santé (industriels, professionnels libéraux et hospitaliers etc.) pensent que les échanges de données entre professionnels ne sont pas sécurisés et que la confidentialité n'est pas préservée. (35)

Les données de santé sont des données sensibles, auxquelles la CNIL reconnaît un caractère particulier et qui disposent d'un encadrement spécifique dans le Code de Santé Publique (CSP).

Ainsi, selon les dispositions sur l'hébergement des données de santé prévues par l'article L. 1111-8 du CSP, l'activité d'hébergement des données de santé devait être agréée spécifiquement par le Ministère de la Santé. (36)
Depuis l'adoption de la Loi de modernisation du système de santé et de l'ordonnance du 12 janvier 2017, les hébergeurs de données de santé ne doivent plus être agréés mais doivent obtenir une certification délivrée par des organismes accrédités.
Cette certification concerne « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même.* » (37)
Les hébergeurs sont certifiés pour 3 ans, les organismes certificateurs sont accrédités par le Comité Français d'Accréditation (COFRAC) pour 5 ans.

Ces dispositions sont censées assurer un haut niveau de sécurité et de protection des données. Le Règlement Général pour la Protection des Données (RGPD) vient renforcer ces dispositions en encadrant le traitement des données.

Le RGPD et la loi Informatique et Libertés posent le principe d'interdiction du traitement des données sensibles, sauf en cas de :

- Consentement explicite de la personne, le traitement de données doit faire l'objet d'un consentement libre et éclairé du patient,

- Sauvegarde des intérêts vitaux de la personne,

- Traitement nécessaire dans le cadre d'une médecine préventive ou de la médecine du travail, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de santé ou de protection sociale.

De plus, l'utilisation des données de santé doit se faire en respect des grands principes de protection explicités par le règlement :

- Finalité de traitement déterminée et légitime
- Données pertinentes
- Durée de conservation déterminée
- Respect du droit des personnes et de leur information
- Mise en place de mesures de sécurité de nature à garantir la confidentialité des données

Chaque acteur traitant des données doit être en mesure de démontrer *a priori* qu'il respecte ces principes et devra notamment réaliser une analyse d'impact (le *Privacy Impact Assessment* ou *PIA*) mesurant les conséquences négatives qu'aurait sur les personnes une compromission de l'intégrité des données.

La sécurité et le traitement des données sont donc fortement encadrés par la loi, afin de garantir l'intégrité et la confidentialité des informations. Mais est-ce suffisant ?

Avec le secteur de la grande distribution, le secteur de la santé est celui qui possède le taux le plus bas de chiffrement de données, ce qui le rend fortement vulnérable. (38)

En février 2016, deux grands hôpitaux américains ont été la cible de cyber attaques : le Hollywood Presbyterian Medical Center a subit une attaque de grande envergure, les hackers demandant une rançon de 3,2 millions d'euros contre la restitution des données médicales volées (39) ; l'hôpital de York a été victime d'une attaque compromettant les données personnelles de 1 400 employés, dont des médecins et des infirmiers. (40)

Dans un rapport publié par le procureur général de Californie, on estime qu'il y a eu des 657 brèches de sécurité en 3 ans, pour 49 millions de données et dont 16% de ces failles concernaient le secteur de la santé. (41)
La France n'est pas en reste puisque 68% des entreprises ont été victimes de fraudes en 2016, dont plus de la moitié ont été causées par des cyber attaques. Avec 25 000 données volées en moyenne, la France se classe 4ème au classement mondial en terme de données volées, derrière les Etats-Unis, le Moyen-Orient et l'Inde. (42)
De plus, selon un rapport d'IBM en 2017, un vol de données coûterait 3,62 millions de dollars en moyenne dans le monde contre 4,27 millions de dollars pour un vol de données en France. (43)

En dehors des pertes financières importantes, les attaques contre les bases de données médicales sont une violation de l'intégrité des données et mettent en péril la vie privée des patients. Le secteur de la santé a donc besoin d'un système de sécurité sans faille.

2.4 L'interopérabilité des systèmes d'information de santé

L'interopérabilité des systèmes informatiques (SI) est un des enjeux principaux liés au partage des données de santé.

Elle est définie comme étant la capacité que présentent différents systèmes indépendants à communiquer entre eux de manière harmonieuse, mettant à disposition des informations exploitables et facilement compréhensible sans que l'utilisateur n'ait besoin de procéder à des adaptations particulières.
Une bonne interopérabilité est une condition nécessaire à la coordination des soins, au décloisonnement des données de santé et s'impose à la vue de l'augmentation des connaissances médicales et des compétences des différents acteurs de santé. Elle permet également de supprimer les retranscriptions d'informations déjà existantes, les doublons ou les recodages, et donc de diminuer les coûts liés à la redondance d'informations.

Les systèmes informatiques devraient pouvoir répondre à 3 grandes exigences :

- Avoir une architecture ouverte permettant l'évolution et la mutualisation des fonctions et des tâches

- Gérer des données normalisées et standardisées à un niveau national, voire à un niveau international afin d'éviter les erreurs d'interprétation

- Faciliter le recueil et le traitement de l'information

Aujourd'hui, la plupart des systèmes ne répondent pas à ces exigences. A titre d'illustration, il existe aujourd'hui 864 logiciels métiers disponibles pour les professionnels de santé, on s'imagine aisément qu'ils ne sont pas tous interopérables. (44)
De plus, la diversité des acteurs du système de santé, de l'Etat au patient en passant par les professionnels de santé et les industriels, augmente le nombre de systèmes d'information développés de manière isolée.

On distingue 2 grands types d'interopérabilité (45) :

- L'interopérabilité technique : concerne la définition de formats informatiques communs, notamment le format des interfaces, des données et des protocoles d'échanges.
  Cela comprend également l'interopérabilité syntaxique, c'est à dire la manière dont sont codées et formatées les données.

- L'interopérabilité sémantique : assure que les informations transmises soient comprises de la même manière sur n'importe quelle autre interface et par un utilisateur différent, que les informations ne soient pas libre à interprétation. Dans le cadre des systèmes informatiques de santé, cela correspond à la nomenclature et au vocabulaire utilisé pour définir des pathologies, des actes de soins ou des traitements.

La standardisation des données est une des clés de voûte essentielle à l'interopérabilité, l'utilisation de normes, de standards et de référentiels est donc nécessaire pour avoir une bonne interopérabilité, tant technique que sémantique.
Cependant, il existe beaucoup de systèmes de classification différents (pour la médecine générale, les actes de soins, les maladies rares etc.) ; certaines terminologies permettent de décrire précisément une situation clinique alors que d'autres sont utilisées pour des usages non cliniques (administration, statistiques de santé) et sont moins précises.
Par exemple, on peut citer la Classification Internationale des Maladies (CIM, *ICD* en anglais) qui a été développée par l'Organisation Mondiale de la Santé (OMS) pour en extraire des statistiques sur les causes de mortalité ou la SNOMED (*Systematized Nomenclature of Medicine*), développée afin de décrire précisément des situations cliniques et des concepts médicaux. La documentation scientifique se base elle sur le MeSH (*Medical Subject Headings*), thésaurus de la base de données bibliographique Medline.

En plus des différents systèmes de classification, il existe plusieurs types de données qui peuvent être intégrées dans un dossier médical (46) :

- Les données non structurées : sont les données librement saisies par le professionnel de santé, obtenues en temps réel, qui sont aujourd'hui le plus utilisées par le corps médical. Elles peuvent être interprétées différemment en fonction de chaque professionnel, ne sont pas standardisées et sont difficilement adaptables aux traitements statistiques ou épidémiologiques.

- Les données structurées : sont codées grâce à un référentiel sémantique, mais peuvent être contraignantes à saisir et nécessitent de s'accorder sur le référentiel à choisir.

- Les « méta-données » : sont des données non structurées complexes comme des documents, de l'imagerie médicale, des prélèvements ou des analyses biologiques. Leur indexation dans un système informatique nécessite un référencement essentiel et exhaustif.

Ainsi, une même information peut prendre différentes formes dans une même base de données. Par exemple, la mesure de la tension artérielle systolique peut être représentée par de manière quantitative sous forme de donnée structurée avec une valeur en mmHg, être répertoriée sous forme non structurée dans un compte rendu en texte libre, avec une valeur ou avec différents synonymes tels que « hypertension artérielle » ou « HTA ». Elle pourrait également être une réponse binaire type « oui » ou « non » à une question comme « hypertension ? », réponse qui peut être écrite sous forme de texte ou être inscrite dans des « cases à cocher ». L'information pourrait aussi être codée selon les référentiel CIM ou SNOMED.

L'interopérabilité d'un système ou entre systèmes informatiques dépend donc de la maîtrise des référentiels existants, condition nécessaire mais qui peut parfois ne pas être suffisante. A titre d'illustration, le codage utilisé pour la Tarification à l'Activité (T2A) en milieu hospitalier se base sur un référentiel unique, mais les différentes mises à jour qui amènent des nouvelles règles de codage donnent des contenus différents et non homogènes.

On comprend donc que la cohérence sémantique et technique des données est, bien qu'indispensable, un vaste chantier qui demande une réflexion générale entre les différents acteurs du système de santé.

C'est ce que tentent de faire plusieurs groupements, organisations et associations comme :

- L'IHE (*Integrating the Healthcare Enterprise*) :

  Ce regroupement international de professionnels de santé a pour but de promouvoir l'interopérabilité des systèmes information d'information de santé et ce en adaptant des normes et des standards internationaux à des cas pratiques d'usage en santé. IHE assemble ces normes pour en faire des spécifications implémentables dans les solutions informatiques.

  Parmi les standards utilisés, on retrouve le DICOM (*Digital Imaging and Communication in Medicine*) qui définit un format de fichier pour l'imagerie médicale et un protocole de transmission et le *Health Level 7* (HL7). Le HL7 est un ensemble de spécifications techniques pour l'échange de données cliniques, financières et administratives entre les systèmes d'informations hospitaliers (SIH) qui intègre des normes américaines (ANSI) et internationales (ISO).

- Interop'Santé :

  Créé en 2009, Interop'Santé est une association qui regroupe plusieurs organisations travaillant pour la standardisation des échanges informatiques en santé, comme des fournisseurs de solutions (B. Braun Medical, Siemens Healthcare, …), des consultants, des groupements d'intérêt général (HAS, SNITEM) et des offreurs de soins.

  L'association recommande l'utilisation des standards HL7, HPRIM (Harmoniser et Promouvoir l'Informatique Médical) et les standards IHE.

- Personal Connected Health Alliance :

  Personal Connected Health est un organisme international regroupant des sociétés de technologie et de soins de santé privées à but non lucratif. L'organisme a développé les Continua design guidelines qui ont notamment été adoptées au Danemark, et qui sont en cours d'adoption en Suède et en Norvège. (47)

- HIMSS Europe (*Healthcare Information and Management Systems Society*) :

  L'HIMSS est une organisation américaine à but non lucrative qui a pour but d'améliorer la qualité et la sécurité des soins avec l'utilisation de systèmes informatiques. Elle développe notamment l'EMRAM (*Electronic Medical Records Adoption Model*), outil qui permet de suivre l'état et la progression de l'interopérabilité dans les organisations de soins.

En France, en 2009, un rapport mettait en exergue le manque d'interopérabilité des systèmes d'informations de santé français alors que les bénéfices étaient clairement démontrés et surtout, pointait l'absence d'action concrète de la part de l'Etat : « *il n'existe toujours pas au niveau du ministère de la santé de document de cadrage définissant les grandes orientations de ce que devrait être le système d'information en santé en termes fonctionnels et qui s'imposeraient à l'ensemble des directions du Ministère ainsi qu'à tous les acteurs concernés.* » (46), (48)

A la suite de ce rapport, le gouvernement et l'ASIP Santé ont décidé de créer le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS), qui définit des règles pour améliorer la communication entre systèmes d'information. (49) L'ASIP Santé, sous la responsabilité du Ministère de la Santé, est en charge de la promotion de l'interopérabilité au niveau national, et travaille de manière étroite avec l'IHE.
Le CI-SIS est un « *référentiel d'interopérabilité qui compile des principes et des standards à respecter pour échanger des données de santé en toute sécurité*. »

Le cadre d'interopérabilité se décompose en 3 couches :

- Les contenus : classe les différents types d'informations médicales sous la forme d'un document standardisé (format « CDA R2 » en XML, développé par HL7) afin que les informations soient facilement authentifiables et exhaustives. Ce document contient un en-tête avec les informations générales permettant son identification et les données du contexte médical dans lequel il a été créé (titre, auteur, patient concerné, prise en charge etc.) ; et un corps qui contient la partie « médicale ».

- Les services : indique les modalités d'échange et de partage des données qui doivent être mis en place pour correctement communiquer les contenus. Chaque document créé sera indexé pour faciliter le classement, la recherche et la transmission. Cette indexation suit des règles précises dérivées du CDA R2 et doit contenir l'identifiant du patient, les actes médicaux réalisés, le diagnostic, le type de document et la spécialité de l'auteur.

- Le transport : détermine les protocoles d'acheminement et d'interconnexion de l'information.

Afin de tester le fonctionnement des systèmes d'information, leur capacité à être interopérables grâce à l'application des standards IHE, l'ASIP santé participe aux Connectathons, les plus grandes sessions de tests dans le monde de la santé connectées, réunissant près de 500 ingénieurs pour 3 500 tests en 4 ou 5 jours.

La sécurité, la standardisation et l'interopérabilité sont des enjeux auxquels sont liés les données de santé et leur partage entre acteurs de santé. Comment la blockchain pourrait y répondre afin d'améliorer la prise en charge du patient ? Nous essaierons d'apporter une réponse à cette question dans la partie suivante (partie 3).

3. La réponse blockchain

Il n'existe pas de solution blockchain unique, de modèle prédéfini applicable au domaine de la santé. Dans le cadre de cette thèse, nous allons essayer de voir comment une blockchain pourrait répondre aux différents enjeux liés aux données de santé et permettre la création d'un dossier patient unique.

Nous aborderons successivement le type de blockchain qui paraît être le plus adapté (partie 3.1), comment la blockchain permettrait d'assurer la sécurité des données de santé (partie 3.2), quelles technologies pourraient être utilisées pour stocker les données (partie 3.3), comment, quelle solution pourrait apporter la blockchain aux problèmes d'interopérabilité des systèmes informatiques (partie 3.4) et des exemples concrets d'application de la blockchain (partie 3.5).

3.1 Blockchain de consortium

La première question à se poser avant de voir comment la blockchain pourrait permettre une meilleure gestion des données de santé est : « quel type de blockchain utiliser ? ». En effet, comme expliqué précédemment, les blockchains peuvent être de 3 types : publiques, privées ou de consortium.

Une blockchain publique, de part son caractère décentralisé, permettrait une sécurité absolue des données, mais nécessite de rémunérer les mineurs qui valident l'ajout d'un bloc sur la chaîne. Dans le cas du système de santé, qui, parmi les différents acteurs (hôpitaux, assurance maladie, patients, professionnels de santé, pharmaciens, Etat, etc.) rémunèrerait les mineurs ? Et surtout, quelle type de rémunération offrir afin d'inciter au minage ?
En plus de ces questions, le monde de la santé est tenu à des obligations réglementaires de confidentialité, et doit s'assurer de l'identité des différentes parties prenantes.

La blockchain de consortium semble être l'outil le plus approprié pour le monde de la santé. En plus de permettre une intégration plus rapide des données, de s'affranchir de la notion de coût, de privatiser et de sécuriser les données, la blockchain de consortium permet de distribuer des droits différents pour les participants.
Ainsi, chaque participant pourrait avoir des accès différents en fonction de sa position : les patients et les professionnels de santé pourraient librement consulter et ajouter des informations médicales, tandis que les parties prenantes plus « conséquentes » comme l'Etat, l'Assurance Maladie ou les organisations type ASIP Santé auraient des accès plus privilégiés et participeraient au minage.

3.2 Sécurité des données

La fonctionnement et la décentralisation de la blockchain en font une base de données quasi impossible à altérer, et permet ainsi d'assurer l'intégrité et la sécurité des données qui y sont inscrites.

Contrairement à un modèle de sécurité traditionnel qui s'appuie sur la confidentialité pour protéger les données, la blockchain s'appuie sur la transparence de l'information.
Comme expliqué précédemment, chaque bloc est crypté grâce à une fonction de hachage et possède un *hash*, empreinte unique et non modifiable. Imaginons qu'une personne arrive à compromettre le serveur qui contienne le bloc et qu'il souhaite le changer : il serait dans tous les cas impossible de modifier l'empreinte qui a été créée. L'information contenu dans un bloc ne peut être modifiée sans que cela entraine un changement de *hash*. Il est alors assez simple de comparer l'empreinte du bloc compromis et l'empreinte originelle pour s'apercevoir que les données ont été manipulées.

De plus, chaque bloc étant relié au bloc précédent, il est virtuellement impossible de modifier une transaction d'un bloc sans devoir casser la chaine ou au mieux devoir recalculer tous les blocs suivant. Il est également impossible de supprimer un bloc sans supprimer toute la chaîne qui le suit.

Protection de l'identité :

La blockchain permet également de protéger l'identité des participants grâce à un cryptage à clé publique/privée. (3)

Le principe des clés publiques/clés privées est une méthode de cryptage asymétrique, à sens unique, qui utilise 2 clés : une clé publique, visible par tous et une clé privée, individuelle, unique et secrète, connue de son seul propriétaire. Les clés publiques sont conservées dans des bases de données spécialement prévues à cet effet.
Ces deux clés, à l'inverse du chiffrement symétrique qui utilise une seule clé pour chiffrer et déchiffrer un message, ont des fonctions bien précises : la clé publique permet de chiffrer un message et la clé privée de le déchiffrer.

Chaque personne qui « s'ajoute » à la chaine, qui ouvre son dossier médical, se voit attribuer sa clé publique et sa clé privée, qu'il conservera toute sa vie.

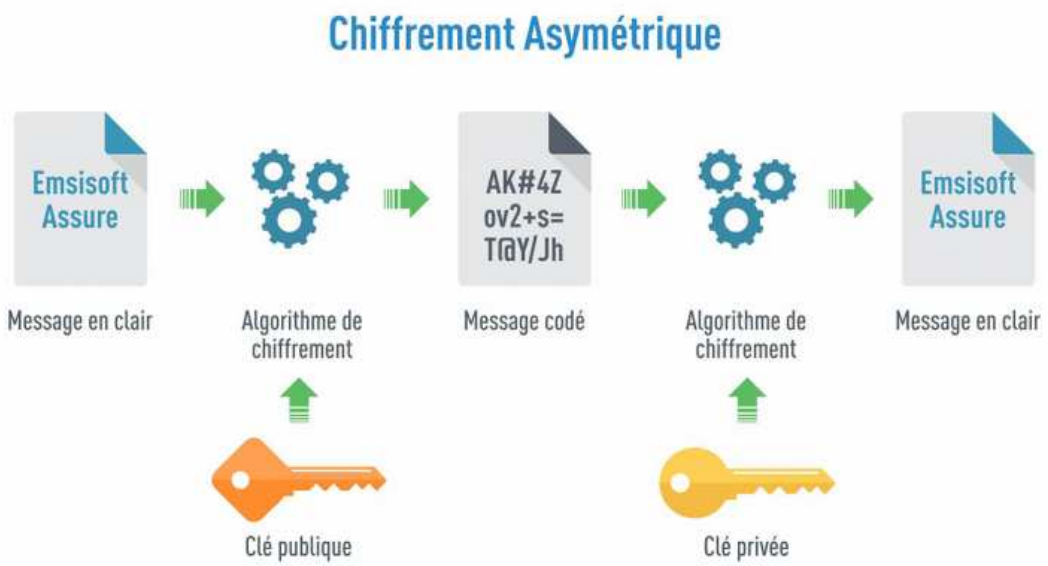

Figure 9 : chiffrement asymétrique (50)

Le chiffrement asymétrique fonctionne en plusieurs étapes :

1. Un message en clair est chiffré à l'aide de la clé publique du destinataire, selon un algorithme défini,

2. On obtient alors un message codé qu'il est impossible de déchiffrer,

3. Le destinataire reçoit le message chiffré qu'il pourra lire en clair après l'avoir décrypté avec sa clé privée.

La clé publique est définie à partir de la clé privée, mais il est impossible de deviner la clé privée à partir de la clé publique, cela nécessiterait d'y aller à la « force brute » en faisant des suppositions jusqu'à trouver la bonne clé, ce qui demanderait des jours et des jours de calcul.
Afin de s'assurer de l'identité de la personne avec qui on communique, une signature est apposée sur chaque message : la personne souhaitant envoyer un message va le « signer » électroniquement avec un message qu'elle aura chiffré avec sa clé privée. Le destinataire pourra ensuite déchiffrer ce message grâce à la clé publique de l'émetteur et ainsi s'assurer qu'il communique bien avec la bonne personne.

Utilisé pour des dossiers médicaux, le principe de chiffrement asymétrique permet au patient de partager ou non ses données en fonction du professionnel de santé et lui redonne un contrôle sur ses données privées.
Il sera alors facile de s'assurer de l'identité d'une personne en faisant correspondre la clé privée du patient que lui seul détient avec sa clé publique.

Se pose alors la question : « comment faire lorsque le patient n'est pas en état de donner sa clé privée ? ».

En effet, un patient en crise, inconscient ou avec un handicap physique et/ou mental conséquent ne pourrait être capable d'autoriser un médecin à accéder à dossier personnel. Plusieurs solutions pourraient être envisagées comme :

- Mettre en place un système de déblocage grâce à l'accord de plusieurs personnes de confiance préalablement désignées (entourage proche, médecin etc.),

- Dans le cadre d'une urgence, associer des informations vitales à la clé publique comme le groupe sanguin ou certaines allergies, qui permettrait aux soignants d'avoir un peu plus d'informations en attendant que le patient puisse communiquer sa clé ou que le dossier soit débloqué comme évoqué ci-dessus.

La méthode de chiffrement asymétrique permet également de garantir l'anonymat des patients : les données sont anonymisées, seul l'identifiant publique du patient est visible.

Une réponse au problème d'identification du patient :

Avec le chiffrement asymétrique, chaque participant de la blockchain possède une clé publique unique qui ne permet pas de l'identifier directement. Cela permettrait de répondre à la question « quel identifiant utiliser pour un patient ? ».

La question de l'identification du patient s'est posée avec l'ouverture du DMP, un identifiant étant indispensable au partage de documents entre professionnels et établissements de santé. Le CSP stipulait en 2007 qu'un Identifiant National de Santé (INS) serait utilisé « *pour la conservation, l'hébergement et la transmission des informations de santé. Il sera également utilisé pour l'ouverture et la tenue du dossier médical personnel et du dossier pharmaceutique*. » (51)
La loi propose alors d'utiliser le Numéro d'Inscription au Répertoire (NIR), plus connus sous le nom de « numéro de Sécurité Sociale » comme base pour définir un INS qui serait anonymisé. Toute personne née en France est inscrit dans le Répertoire National d'Identification des Personnes Physiques (RNIPP) et possède un NIR. De même, une personne étrangère adhérant au système de sécurité sociale se voir attribuer un numéro.

Le NIR est composé de 13 chiffres :

- Le premier chiffre correspond au sexe de la personne
- Les deux chiffres suivant aux derniers chiffres de l'année de naissance
- Les deux suivants au mois de naissance

- Les cinq chiffres suivant correspondant au lien de naissance
- Les trois derniers chiffres forment un numéro qui correspond à un ordre chronologique permettant de distinguer les personnes nées au même endroit dans une même période

Les 13 chiffres sont complétés par une clé de contrôle de deux chiffres permettant de vérifier et d'authentifier le NIR.
Le Numéro d'Inscription au Répertoire est un numéro unique et pérenne mais non anonyme, qui permet facilement d'identifier certaines informations concernant une personne. C'est d'ailleurs ce qu'à fait remarquer la CNIL lorsqu'elle a été consultée pour le lancement du DMP, et qui déconseillait l'usage du NIR : « *partant de la constatation que les données de santé ne sont pas des données personnelles comme les autres et qu'elles appellent à une protection renforcée, la Commission estime que le NIR, compte tenu de son usage répandu, du fait qu'il est signifiant et facile à reconstituer et des risques précédemment évoqués, ne constitue pas, aujourd'hui un numéro adapté pour identifier le dossier médical de chacun.* » (52)

La CNIL recommande alors de créer un nouvel identifiant spécifique aux données de santé, généré à partir du NIR mais totalement anonymisé et non signifiant, utilisable dans l'ensemble du système de santé.
L'ASIP Santé propose alors de créer un « Identifiant National de Santé calculé » (INS-c), calculé à partir du NIR, du prénom et du sexe de chaque patient et anonymisé grâce à une fonction de hachage.

Cependant, le NIR et l'INS-c ne sont pas disponibles pour des ayant-droits comme les enfants qui ne sont pas encore inscrit à la sécurité sociale et qui dépendent du régime de leurs parents.
L'INS-c a donc été abandonné et, en 2015, la Loi de modernisation du système de santé a autorisé l'utilisation du NIR comme identifiant de santé, bien que non anonyme.

La création d'un dossier médical unique avec une blockchain permet de résoudre cette problématique : chaque patient se voit attribuer sa clé publique unique, fiable, sans doublon et non signifiante.

3.3 Stockage des données

Une blockchain contenant l'intégralité de tous les dossiers médicaux, des documents d'analyses et de l'imagerie médicale serait compliquée à mettre en place et serait limitée en terme de stockage. La blockchain étant décentralisée, chaque participant possèderait une copie de l'intégralité de la chaîne et donc de l'intégralité des dossiers médicaux, ce qui ne serait pas optimal et contraignant.

Une partie des informations serait donc stockée sur la chaîne, « on chain » et l'autre partie sur une plateforme différente, « off chain » :

- Informations « on chain » : chaque bloc contiendrait la clé publique unique du patient, un lien encodé redirigeant vers le dossier médical ou le document concerné et un horodatage de la transaction. La transaction contiendrait également des « métadonnées » comme le type et le format de l'information stockée dans le dossier médical. Ces métadonnées fonctionneraient comme un « tag » permettant de facilement retracer l'historique médical du patient.

- Informations « off chain » : toutes les autres informations, les documents, l'imagerie, les analyses etc. seraient contenus dans une base de données spécifique reliée à la blokchain, les « data lakes » ou les « clouds décentralisés ».

Les data lakes :

Un data lake, ou « lac de données », est une méthode de stockage permettant de conserver une très large quantité de données sur une durée indéterminée. (53)
Tous les types de données peuvent y être stockés, qu'elles soient brutes, non structurées comme un pdf ou des emails, semi structurées comme les CSV, les XML ou encore des données structurées en provenance d'autres bases de données (les « datawarehouses »). Des données binaires comme des images, des sons ou des vidéos peuvent également y être stockées.
Chaque donnée se voit attribuer un identifiant unique et est marqué de balises ; dans le cas de la santé, chaque donnée aura un code correspondant au document et à l'acte de soin correspondant en plus de l'identifiant patient.
Par exemple, une radio du thorax pourrait être dénommée « RADTH », une biopsie de la moelle épinière « BIOPME » etc. ; ce qui, en plus d'avoir des standards compréhensibles par tous, permettrait de retrouver plus facilement une information.

Le data lake se comporte comme une base de données géante qui stocke tout type de document, contrairement aux bases de données traditionnelles, et qu'il est possible d'interroger afin de retrouver un document.

Figure 10 : Data lake (54)

Les clouds décentralisés :

Afin d'essayer de résoudre le problème majeur lié au stockage centralisé (« le point unique de défaillance » qui s'avère être le lieu de stockage des données), se développent les clouds décentralisés. (55)
L'idée d'un cloud décentralisé est venue en remarquant que les internautes n'utilisent pas tous l'espace de stockage de leur ordinateur.
Un utilisateur pourrait alors louer son espace disponible afin de stocker des données d'un autre utilisateur, et ce grâce à une blockchain qui permettrait de chiffrer les données, de les décentraliser et de les sécuriser.

Cependant, le cloud décentralisé étant une technologie relativement nouvelle et qui nécessite de rémunérer les personnes louant leurs espaces de stockage, il semble plus judicieux d'utiliser un data lake pour stocker des données de santé.
L'accès au data lake serait protégé par la blockchain afin de garantir la sécurité des données qui y sont mises.

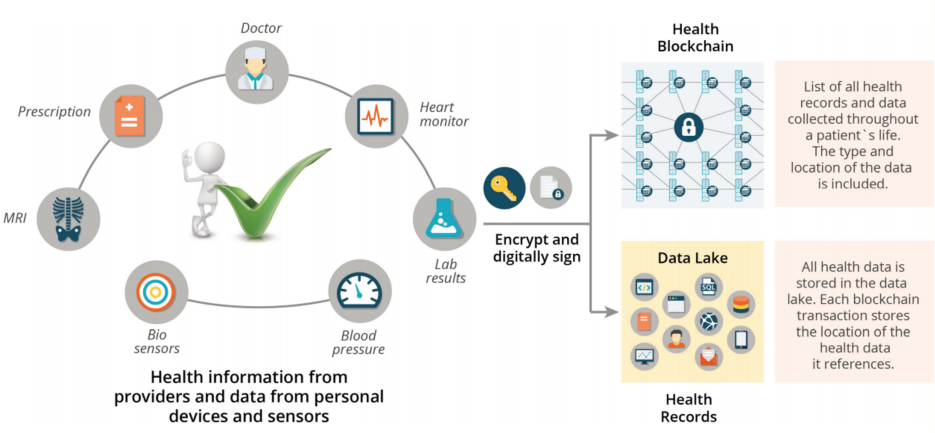

Figure 11 : Fonctionnement de la blockchain avec data lake

Chaque donnée mise sur le data lake serait chiffrée et serait signée afin d'assurer la confidentialité et l'authenticité de l'information.

Ainsi, à chaque document médical créé, l'auteur (le professionnel de santé ou le patient) le signera grâce à sa clé privée pour en garantir l'authenticité. Ce document sera ensuite crypté pour être déposé dans le data lake. Les métadonnées de ce document (type, format etc.) seront reliées à la blokchain, qui datera la transaction.

3.4 Interopérabilité et standardisation

La blockchain a le potentiel pour apporter une réponse au problème de standardisation et d'interopérabilité des systèmes de santé, tant sur le plan informatique que sur la communication entre les acteurs de santé, notamment grâce aux smart contracts et aux API (*Application Programming Interface*).

Les smart contracts :

Les smart contracts, ou « contrat intelligents », font partie des applications les plus prometteuses de la blockchain. Développés sur Ethereum, ces contrats sont des programmes autonomes, accessibles par tous et qui, lorsqu'activés, permettent l'exécution automatique de condition préalablement définies et inscrites dans la blockchain. (56)
Ces programmes fonctionnent selon des instructions conditionnelles type « if – then – else » : si une condition est remplie et vérifiée, alors la conséquence s'exécute. Il est possible d'entièrement personnaliser ces conditions pour déterminer le meilleur moment où échanger de la valeur, transférer des informations ou déclencher des évènements.

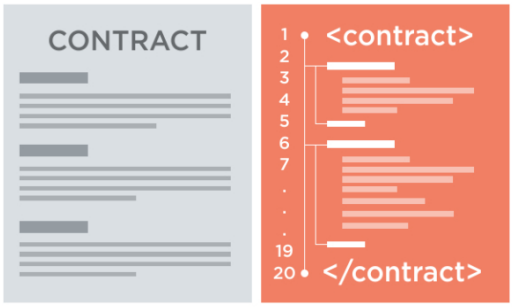

Figure 12 : Smart Contract (57)

L'avantage de ces contrats réside dans le fait que les termes du contrat ne peuvent être modifiés. Ils permettent de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude.

Appliqués sur une blockchain santé, les smarts contracts présenteraient plusieurs applications :

- Standardisation des données : la conformité des données aux différents standards et référentiels serait vérifiée par un contrat avant l'entrée de la donnée sur la chaîne.

- Transmissions des informations et automatisation des processus : les smart contracts permettent la transmission automatique des informations entre les différents acteurs de la santé. Prenons par exemple le cas d'un remboursement d'une prescription en officine. Un contrat est établi entre un patient, les mutuelles, l'Assurance Maladie et une pharmacie. Une entrée est faite dans la blockchain à chaque fois que la pharmacie délivre un médicament au patient venu chercher sa prescription. Une notification est envoyée aux organismes payeurs et si l'information respecte les conditions inscrites dans le contrat, les remboursements de l'Assurance Maladie et de la mutuelle à la pharmacie et au patient s'enclenchent automatiquement. Cela permet de réduire le temps consacré à l'administratif, réduit le nombre d'erreurs de transmissions et facilite l'échange d'informations.

- Notification spontanée : de même, un contrat pourrait permettre de notifier spontanément un patient de l'ajout de données médicales dans son dossier ou le notifier dès qu'un professionnel de santé autorisé accède à ses données. Le patient peut ainsi avoir une vraie vue d'ensemble et un véritable historique de consultation de ses données.

- Vérification de l'accès aux données : le patient autorise l'accès à ses données aux professionnels de son choix, mais peut en plus y ajouter un contrat pour s'assurer complètement de l'identité du professionnel de santé. Dès qu'il autorise un professionnel de santé à accéder à ses données, un contrat est créé auquel est ajoutée une condition de droit d'accès : si la clé du professionnel ne remplit pas les conditions du contrat, alors l'accès est refusé.

Les API :

Les API, pour *Application Programming Interface*, littéralement « interface de programmation d'application », sont des solutions informatiques permettant aux applications de communiquer entre elles, de s'échanger des données. Ce sont en quelque sorte des « ponts » reliant les applications entre eux pour faciliter les échanges.

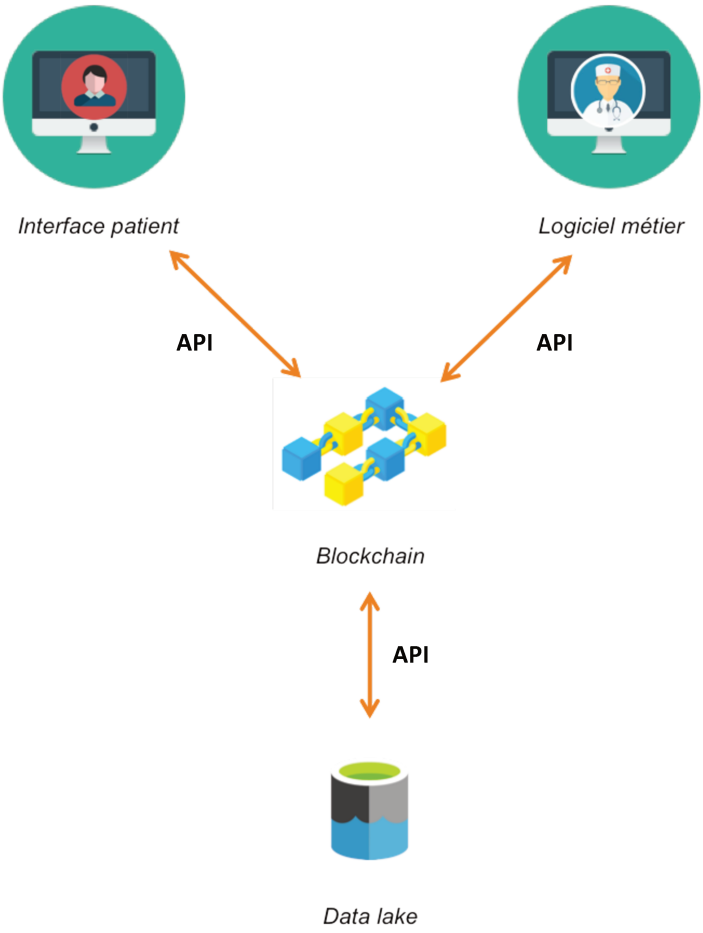

Figure 13 : Application Programming Interface

A titre d'illustration, les API peuvent être mises en place à plusieurs niveaux pour faciliter l'échange d'informations :

- A partir d'une interface unique, le patient peut consulter son dossier médical. Pour cela, une API fait le pont entre l'interface et la blockchain, qui elle même est liée au data lake.

- Les logiciels métiers des professionnels sont liés de la même manière à la blockchain et aux data lakes, les API permettent de faire le lien entre les différents systèmes pour remonter une information lorsque le médecin souhaite consulter un dossier médical.

De la même manière, les logiciels métiers peuvent être liés entre eux par différentes API, ce qui augmenterait grandement l'interopérabilité des systèmes informations. Une liaison peut également être faite entre la blockchain et les bases de données actuelles.

3.5 Exemples d'utilisation de blockchain en santé

- **L'Estonie, le pays blockchain :**

Petit pays balte d'1,3 millions d'habitants, l'Estonie est une référence mondiale en numérique, tant sur des questions de cyberdéfense ou sur l'utilisation de la blockchain, à tel point que le pays est devenu l'avant poste de l'OTAN en cyberdéfense. (58)

Dès 1997, l'Estonie mise sur le numérique et commence à dématérialiser les démarches administratives. Aujourd'hui, 99% des services publics du pays sont accessibles en ligne. Les seules démarches qui restent « physiques » sont le mariage, le divorce et l'achat immobilier, pour des raisons légales et sociales.
La dématérialisation des services publics a été rendue possible avec la mise en place de la carte d'identité électronique, développée par Gemalto, entreprise française numéro une mondial de la carte à puce.
Cette carte est un des pivots du système numérique estonien, qui sert entre autres de carte d'identité, de carte d'électeur, de transports, de fidélité, de Sécurité Sociale etc. Il suffit de 2 jours seulement pour l'obtenir et s'utilise grâce à un code PIN que seul l'utilisateur connaît.

L'échange de données entre les services estoniens se fait grâce à X-Road, système informatique décentralisé développé par plusieurs entreprises locales. X-Road permet aux différents systèmes d'échanger leurs données de manière sécurisée, et permet de limiter les démarches administratives.
Toutes les données sortantes du logiciel sont signées électroniquement et chiffrées ; les données entrantes sont authentifiées, journalisées et sont enregistrées entre les différents systèmes d'information. Une information ne doit donc être entrée qu'une seule fois sur le site d'un service public grâce à l'automatisation des processus. Par exemple, des parents venant d'avoir un enfant n'ont pas à faire toutes les déclarations administratives que l'on connaît habituellement en France : le numéro d'identité de l'enfant est automatiquement créé et transmis à tous les services.
X-Road est une plateforme évolutive sur laquelle peuvent s'ajouter des nouveaux e-services et ce, à l'infini. En 2016, l'Estonie dénombrait 1789 services en ligne contre 536 en France. Le logiciel est garant de l'interopérabilité des services estoniens et permet, à ce titre, d'économiser 800 ans de temps de travail chaque année. (59)

La santé fait également partie des services qui ont été dématérialisés. Chaque habitant possède un dossier médical électronique unique, dont l'évolution se suit grâce à la carte d'identité électronique. Le dossier fonctionne comme une base de donnée géante qui récupère les données des différents prestataires de santé et qui sont accessibles via un portail unique, le portail e-Patient. Depuis ce portail, les

patients peuvent décider ou non d'autoriser l'accès de leur données aux médecins et peuvent visualiser l'historique des consultations, le patient recevant une notification à chaque fois que son dossier est consulté. Ainsi, un médecin n'a pas le droit de consulter les données d'un patient sans son accord, et ne pourrait le faire sans que le patient s'en aperçoive.
Pour donner un aperçu de la digitalisation de la santé, l'Estonie compte (60) :

- 99% d'ordonnances numériques
- 100% de facturation électroniques au sein des systèmes de soins
- 95% de données de santé numérisées

Encore une fois, la carte d'identité numérique a facilité les échanges de données numérisées : chaque ordonnance numérique est directement transmise aux pharmacies, le patient utilise simplement sa carte pour récupérer ses traitements. L'ordonnance devient ainsi disponible dans toutes les pharmacies du pays, ce qui simplifie le parcours de soin du patient. L'Estonie est actuellement d'étendre ses solutions décentralisées avec la Finlande afin que les résidents finnois puissent utiliser les systèmes estoniens et inversement, en rendant notamment accessible le système de soin.

Cependant, le développement informatique de l'Estonie a attiré de nombreux hackers. En 2007, l'Estonie subit une attaque de grande envergure, devant laquelle le pays résiste mais qui prouve que le système peut avoir des failles.

Le gouvernement décide alors de maximiser la sécurité et l'intégrité des données et mise une nouvelle fois sur une nouvelle technologie prometteuse : la blockchain.
La blockchain KSI, développée par Guardtime, a commencé à être mise en place pour tous les services publics, et notamment pour les données de santé. La blockchain KSI présente la particularité de ne pas être totalement publique : le gouvernement estonien n'a pas accès à la chaine et ne peut donc en aucun cas interférer avec les données de ses citoyens.

- **MedRec :**

Développé par plusieurs étudiants du MIT, MedRec se présente comme étant un « *combinaison d'un besoin social et d'un catalyseur technologique, un système donnant la priorité aux patients, offrant une vision transparente et accessible des dossiers médicaux électroniques*. » (61)
Partant du principe que la concurrence et la multiplicité des acteurs sur le marché des systèmes informatiques médicaux ne sont pas bénéfiques au patient, créant une incompatibilité des échanges et des contrôles difficiles, les étudiants du MIT ont imaginé une solution blockchain qui permettrait de faciliter les échanges de données de santé.

Cette blockchain se base sur la blockchain Ethereum et ses smart contracts. Les smart contracts sont les piliers de la blockchain MedRec et permettent de relier les fournisseurs de soins aux patients. Les smarts contracts de MedRec permettent d'encoder des « pointers », des métadonnées, qui permettent d'identifier et de localiser l'information enregistrée.
Seules les métadonnées des informations médicales, contenant les informations sur la propriété, les autorisations et garantissant l'intégrité des données, sont enregistrées sur la chaîne.

MedRec définit 3 types de smart contract :

- Contrat d'enregistrement : mappe les identifiants des participants à leur adresse IP Ethereum (l'équivalent de leur clé publique). Il est possible de coder une certaine réglementation dans les contrats : cela permet de garantir que seules les institutions certifiées peuvent ajouter des nouvelles informations dans la chaine et que cela ne peut se faire qu'avec l'accord préalable du patient.

- Contrat de relation fournisseur de soin – patient : ce contrat relie les nœuds du réseaux entre eux, un nœud gérant et stockant les informations d'un autre nœud.

- Contrat récapitulatif : permet au patient d'avoir accès à un résumé de ses interactions avec les différents participants de la chaine.

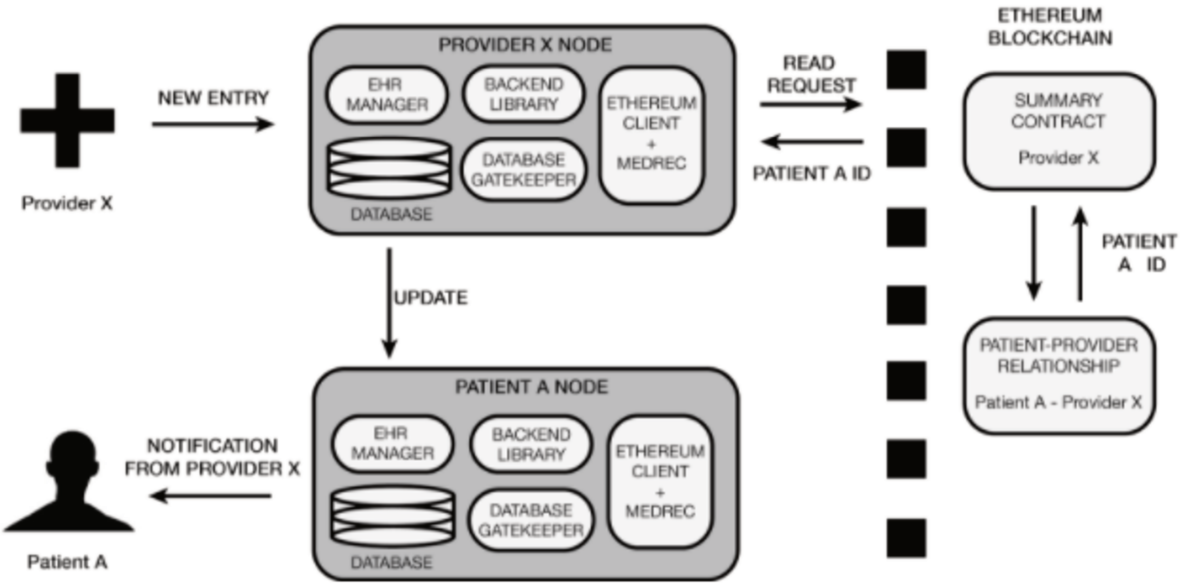

Figure 14 : Fonctionnement de MedRec

La blockchain MedRec est une blockchain hybride, qui présente une particularité de minage : les mineurs sont des chercheurs qui seront rétribués « à la donnée ». Un chercheur qui valide un bloc peut accéder à des données patients anonymisées qui lui permettraient d'approfondir ses travaux de recherche.

La Blockchain est une technologie qui permettrait donc d'apporter des réponses aux enjeux liés aux données de santé, notamment sur les aspects de sécurité et de partage. Cependant, cette technologie doit faire face à différentes problématiques que nous aborderons dans la partie suivante. Nous verrons le défi que représente la mise en place d'une blockchain à grande échelle (partie 4.1), la nécessité de définir un cadre juridique précis (partie 4.2), les questions éthiques qu'elle peut soulever (partie 4.3) et les considérations écologiques (partie 4.4).

4. Limites et défis à relever

4.1 Scalabilité et limitations pratiques

Scalabilité :

Le principal frein à l'adoption d'une blockchain est sûrement son plus gros défaut : la scalabilité, la « mise à l'échelle ».

La scalabilité est la capacité d'une technologie à pouvoir accueillir de plus en plus l'utilisateur, et donc de gérer plus de transactions et de données. Les blockchains les plus utilisées actuellement, comme Bitcoin ou Ethereum, présentent des limites :

- Problématique de taille : l'augmentation du nombre de participants sur une blockchain entraine de fait l'augmentation de sa taille et donc de sa lourdeur informatique. A titre d'illustration, le fichier contenant la chaîne Bitcoin faisait plus de 105 giga octets début 2017, alors qu'il en faisait un peu moins de 90 giga octets en décembre 2016, soit une augmentation de 15% en l'espace de quelques mois. (62)

- Puissance de calcul : la puissance nécessaire pour miner un bloc est révisée tous les 2096 blocs, et augmente au fur et à mesure de l'expansion de la chaîne. Cela demande d'avoir des machines de plus en plus chères et de plus en plus puissantes d'un point de vue énergétique. Ce besoin d'une grande puissance de calcul est en grande partie due au mécanisme utilisé pour la validation des blocs, le *Proof Of Work*.

- Nombre de transaction : à l'heure actuelle, Ethereum et Bitcoin ne sont capables de supporter respectivement que 25 et 7 transactions par seconde (TPS), ce qui est très faible en comparaison de VISA, dont les pics atteignent plus de 20 000 TPS. De plus, une transaction met en moyenne 10 minutes à être validée sur la chaîne Bitcoin, contre quelques secondes pour une transaction VISA.

Le nombre exact d'utilisateurs sur les blockchains type Bitcoin et Ethereum sont confidentielles mais on parle de quelques millions seulement.
Une blockchain utilisée comme réseau de stockage pour les dossiers médicaux doit être adaptable à l'échelle d'un pays entier et doit pouvoir supporter le volume important de données de santé qui sont échangées et créées chaque jour.

On imagine également très mal un médecin ou un patient devoir attendre 10 minutes à chaque fois qu'il souhaite intégrer un document sur la blockchain, les transactions devront donc se faire sans temps d'attente.
Plusieurs solutions sont envisagées pour contrer ces problèmes :

- Remplacer le *Proof-of-Work (PoW)* par d'autres méthodes de calcul :

  Une des solutions est de remplacer le *PoW* par le *Proof-of-Stake (PoS)* : la méthode de validation par « preuve d'état » demande une puissance de calcul moindre que la validation par « preuve de travail », ainsi qu'une consommation et qu'un temps de transaction légèrement inférieurs. Ce changement devrait être opéré sur la blockchain Ethereum.
  D'autres blockchains (comme l'IOTW) souhaiterait remplacer le *PoW* par le *Proof-of-Attribution (PoA)* ou « preuve de cession », qui demanderait encore moins de puissance au point que des ordinateurs « normaux » seraient capables de participer au minage sans trop augmenter leur consommation électrique.

- Utiliser des « solutions de couche 2 » :

  Les solutions de couche sont des applications superposées à la blockchain (comme Lightning pour Bitcoin) qui permettent de traiter des transactions qui ne sont pas stockées sur la chaîne et qui ne sont pas publiques. Ces solutions fonctionnent sur le même principe que certaines applications connectées à internet sur un ordinateur : une partie de l'application fonctionne en réseau et nécessite une certaine puissance mais une autre partie de l'application est capable de fonctionner sans le réseau et donc d'économiser de l'énergie et d'éviter la saturation du réseau.
  Les solutions de couche 2 sont reliées à la blockchain afin de garantir la fiabilité des transactions mais permettent de désaturer le réseau et donc d'augmenter la vitesse des transactions.

Les problèmes de scalabilité sont des enjeux majeurs de la blockchain mais concernent essentiellement les blockchains publiques.

La blockchain utilisée pour gérer des dossiers médicaux serait une blockchain de consortium et permettrait de résoudre une grande partie des problèmes de scalabilité.
En effet, le minage serait restreint et ne serait effectué que par quelques acteurs qui en ont la capacité (institutions de santé, assurance maladie etc.), ce qui permettrait de diminuer l'énergie utilisée et surtout, de pouvoir définir la méthode de validation à utiliser.

Une blockchain de consortium pourrait utiliser une méthode de validation par « preuve d'identité » : l'identité des mineurs suffirait à valider les blocs, ce qui diminuerait considérablement la puissance de calcul et le temps passé à valider une transaction.

Collecte des données et limitations pratiques :

En plus des limites techniques liées au fonctionnement propre de la blockchain, la mise en place d'un tel réseau pose des questions pratiques, notamment sur la collecte des données.
En effet, comment et qui effectuerait la collecte des données ? Comment garder le dossier médical à jour ?

La solution la plus simple serait de réaliser la collecte par les médecins qui, comme pour un carnet de santé, rempliraient le carnet « virtuel » du patient pendant et à la fin de chaque rendez-vous médical, et qui le maintiendrait à jour. Le patient pourrait également rajouter des informations en dehors d'une visite médicale s'il le souhaite.
Cependant, remplir le dossier et le maintenir à jour est une activité assez chronophage à laquelle les médecins risquent de ne pas adhérer.

4.2 Un flou réglementaire

« L'innovation précède le droit ». C'est le cas de la blockchain qui, du fait de sa nouveauté, n'est pas encore encadrée et qui fait face à un flou juridique, notamment en regard du Règlement Général sur la Protection des Données (RGPD). Le RGPD s'applique dès qu'il y a des données personnelles qui entrent en jeu, ce qui serait le cas avec une blockchain en santé.

La blockchain est une technologie qui suit une logique d'ouverture, notamment avec son caractère décentralisé. C'est justement ce trait de caractère qui rend compliqué l'application du RGPD, qui a été créé pour des entités centralisées.
Consciente de l'intérêt grandissant pour la technologie et la nécessité de rattraper le retard de la juridiction, la CNIL s'est emparée du sujet et vient de publier ses premières analyses. (63)

Identification du responsable :

L'article 24 du chapitre IV du Règlement définit la notion du « responsable du traitement des données » qui doit « *mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement (des données) est effectué conformément au règlement* » ; et de « sous traitant » qui peut traiter des données sur instruction du responsable et qui s'engage à en respecter la confidentialité. (64)
Dans le cadre d'une blockchain où tout le monde peut potentiellement gérer des données, qui désigner comme responsable et comme sous-traitant ?

La CNIL distingue trois types d'acteurs dans une blockchain :

- L'accédant : a un droit de lecture et peut posséder une copie de la chaîne
- Le participant : a un droit d'écriture, c'est à dire qu'il est en mesure de réaliser une transaction
- Le mineur : valide la transaction et crée le bloc

La Commission considère que le participant est responsable du traitement :

- Lorsqu'il est une personne physique et que le traitement des données est en lien avec une activité professionnelle ou commerciale, c'est à dire lorsque l'activité n'est pas exclusivement personnelle
- Lorsqu'il est une personne morale

Tous les participants ne sont pas responsables : une personne physique qui inscrit une donnée dans un seul but personnel n'est pas responsable (principe d'exception

domestique (19)), ce qui pourrait être le cas d'un patient entrant une donnée dans son dossier médical dématérialisé.

Dans le cadre d'une blockchain privée ou de consortium, la CNIL recommande de définir en amont de la création de la blockchain le responsable du traitement, notamment en créant une association ou un Groupement d'Intérêt Economique (GIE).
Les mineurs pourraient eux être considérés comme « sous traitants », un contrat précisant les obligations de chacun devra alors être établi.

Format des données :

Les données personnelles doivent avoir une durée de conservation définie en regard de l'utilisation qui en sera faite. (65)
Dans le cadre d'une blockchain qui n'a pas vocation à être « limitée » dans le temps et qui ne permet pas la suppression des données, la CNIL autorise que la durée de conservation des donnée s'aligne avec celle de la blockchain.

Elle préconise également, afin d'assurer le respect des obligations de protection des données dès la conception et par défaut, que la donnée soit traitée en dehors de la blockchain et que soit stocké sur la chaine un engagement cryptographique, une empreinte (le hash) ou un chiffrement de la donnée.
Une blockchain associée à un data lake pourrait convenir et répondre au besoin de la CNIL : ne seront contenues sur la chaîne que les « métadonnées » des informations, qui elles seront traitées et cryptées dans un data lake.

Droit à l'oubli et à la rectification :

L'article 17 du chapitre III stipule que « *la personne concernée à le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais.* » (66)

Or le caractère immuable de la blockchain ne permet pas l'effacement ni la rectification des données et est donc incompatible avec le RGPD. Une donnée ne peut être supprimée que si plus de la moitié des mineurs travaillent ensemble pour invalider une transaction et reconstruire la chaîne.
Effacer les données de cette manière paraît impossible, ou du moins très compliquée à mettre en place, notamment avec un chaîne publique et surtout si la donnée est ancienne et qu'il faille reconstruire une grande partie de la chaîne. Cela demanderait une grande puissance de calcul et surtout que tous les mineurs se synchronisent.

Consciente de cette limite, la Commission propose de rendre la donnée inaccessible, notamment en supprimant la clé privée qui permettrait le déchiffrage de la donnée.
Cela ne supprimerait pas au sens propre la donnée de la blockchain mais permettrait de se « *rapprocher de l'exercice effectif de son droit à l'effacement pour la personne concernée* ». (63)
Si une personne souhaite modifier une information inscrite sur la chaîne, le responsable du traitement devra inscrit un nouveau bloc qui « annulera » l'information précédente. Celle-ci sera toujours visible mais sera « effacée » par la nouvelle information, ce qui permet d'être au plus près du droit de rectification d'une personne.

Droit à l'information :

L'article 7 du chapitre III indique que « *le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale*. » (66)
La blockchain est ici conforme au RGPD puisque chaque utilisateur vérifie et valide la donnée avant son ajout dans la chaîne ; l'historique des transactions servant comme preuve du consentement.
Le responsable du traitement devra en plus fournir une information concise, accessible et avec des termes clairs à une personne avant l'ajout d'une information, afin d'être totalement conforme.

La blockchain est une technologie qui présente certains enjeux au niveau du respect des droits et des libertés fondamentales de la personne.
La CNIL souhaite ainsi porter la réflexion au niveau européen afin de poser les bases d'une réglementation universelle et ainsi donner une meilleure lisibilité aux utilisateurs de la blockchain.

4.3 Ethique et partage des données

La mise en place d'une blockchain permettant la gestion et l'échange de dossiers offrirait des possibilités formidables en terme d'analyse de données.
Imaginons que toutes les données enregistrées soient accessibles de manière totalement anonyme et confidentielle, sans aucun moyen de relier une personne physique à ces informations.
Cela permettrait de réaliser des analyses, d'en extraire des tendances, de perfectionner les statistiques voire même de favoriser la recherche sur certaines pathologies ou d'élaborer des politiques de prévention. L'accès à ces données pourrait être particulièrement prolifique pour les industriels et les institutions publiques.

Cet accès ne pourra se faire qu'avec le consentement des patients et la garantie de l'anonymat. Or la plupart des experts qui travaillent sur la mise en place d'une blockchain pour les dossiers médicaux préconisent de monétiser ces données.
Le patient peut décider qui aura accès ou non à ses informations médicales, et de ce fait pourrait décider de donner accès aux chercheurs ou au laboratoire avec contrepartie financière. La blockchain autorise le patient à « reprendre contrôle » sur ses données et permettrait même d'en tirer profit.

En France, la loi interdit strictement tout « *acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée* » sous peine de sanctions. (36) Les sanctions encourues peuvent aller jusqu'à 5 ans de prison et 300 000 euros d'amende.

La réflexion portée sur la monétisation de ses données personnelles amène à se poser plusieurs questions :

- D'un point de vue financier, comment définir la valeur d'une donnée de santé ?
- Une donnée totalement anonymisée est-t-elle vraiment une donnée personnelle ? Est-on alors vraiment légitime pour vendre ses données ?
- Est-ce vraiment « éthique » de vouloir vendre ses données alors qu'elles pourraient faire avancer la science et bénéficier à tous ?

4.4 La blockchain et l'écologie

L'un des grands points qui fait débat autour de la blockchain est son empreinte écologique.

En effet, le minage, indispensable au fonctionnement d'une blockchain, demande une puissance de calcul conséquente. Cela demande des ordinateurs puissants, qui consomment beaucoup d'énergie et pousse même les mineurs à aller s'installer dans des zones plus reculées où l'électricité est moins chère.

Un rapport publié en 2014 montre l'empreinte énergétique du Bitcoin : son réseau de minage consomme chaque année l'équivalent de la consommation de l'Irlande. (67) En Asie, le gouvernement chinois a du intervenir pour demander la réduction ou la disparition de fermes de minage, le poids énergétique étant devenu trop lourd.

Pour les mêmes raisons qu'évoquées précédemment, l'empreinte énergétique concerne essentiellement les chaînes publiques en raison de leur mode de minage. Une chaîne privée devrait nécessiter des dépenses énergétiques moindres. De plus, l'évolution des technologies devrait permettre de naturellement faire baisser le besoin en énergie des calculateurs.

Plusieurs entreprises proposent d'utiliser des sources d'énergies alternatives, comme Envion qui se base sur les panneaux solaires, Hydrominer sur l'hydro-électricité ou encore Wind Energy Mining qui utilise l'énergie éolienne. Ces initiatives montrent la volonté qu'ont les acteurs de la blockchain à vouloir améliorer la technologie afin de préserver l'environnement.

CONCLUSION

La gestion et le partage des données de santé est un enjeu majeur au regard de l'évolution du monde médical, tant d'un point de vue d'efficacité opérationnelle, de rapidité de prise en charge et de suivi du patient, que d'un point de vue financier.
Dans un monde hyper-connecté où l'interopérabilité est une composante cruciale, le dossier médical numérique, unique et partagé entre tous les professionnels de santé apparaît indispensable pour assurer la bonne continuité des soins. Cela permettrait de réduire le nombre d'erreurs médicales, qu'elles soient liées à l'identification du patient ou dues à des interactions médicamenteuse. Le dossier médical partagé permettrait également de réduire les coûts liés aux actes médicaux redondants ainsi qu'à la mauvaise transmission voire la perte d'informations.

Un des principaux freins au déploiement d'un dossier médical partagé réside dans les craintes liées à la sécurité et à l'intégrité des données, ainsi qu'au respect de la vie privée du patient. La technologie blockchain est capable de lever ces craintes, notamment par son caractère infalsifiable, garant de la pertinence et de la traçabilité des données qui y sont inscrites, mais aussi grâce à son caractère décentralisé, réduisant sensiblement le risque de perte ou de vol de données. La notion de confiance, essentielle pour le partage des données, sera ainsi renforcée par la technologie mise en œuvre et non par un organisme dépositaire des données.

Si cet aspect est sans conteste significatif, le déploiement d'un dossier médical partagé reste aujourd'hui contraint par les caractéristiques propres au système de santé. C'est un système compartimenté, organisé en silo, sans réelle capacité de communiquer de manière efficace. La blockchain est une opportunité pour améliorer l'interopérabilité des systèmes informatiques de santé, facilitant ainsi l'échange entre professionnels de santé et accélérer la mutation nécessaire de l'organisation du système de santé.
Toute évolution majeure repose sur une remise en cause des pratiques actuelles, qui sera progressive mais dont la mise en œuvre peut être accélérée par l'adoption d'une nouvelle technologie et par la perception des avantages qu'elle apporte. La numérisation de l'ensemble des documents médicaux, préalable indispensable au partage des données, apparaît demain comme étant essentiel aux professionnels de santé qui en retireront un avantage certain.
L'exemple de mises en pratiques réussies de blockchains, pour la traçabilité des médicaments ou la gestion de la supply-chain, pourra être un levier pour la conduite du changement. La technologie est récente et devra prouver son efficacité et sa capacité à faire face à certains défis comme la mise à l'échelle et la conformité aux droits des patients, notamment au droit à l'oubli.

Au-delà de ces seuls aspects, la technologie blockchain, par la généralisation des données de santé pouvant être partagées, recoupées et analysées, pourra permettre une meilleure appréhension globale de l'état de santé d'une population donnée, profitable à la fois aux professionnels de santé mais surtout aux patients. L'approche collaborative et intégrée, sur laquelle repose la blockchain, constitue sans conteste un atout majeur sur lequel s'appuyer pour développer un système de santé encore plus performant.

BIBLIOGRAPHIE

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. :9.

2. Distributed Ledger Technology: beyond block chain. :88.

3. Qu'est-ce que la blockchain ? [Internet]. Blockchain France. 2015 [cité 13 nov 2018]. Disponible sur: https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

4. Delahaye J-P. La puissance de la blockchain | Complexités [Internet]. Pour la Science. [cité 14 nov 2018]. Disponible sur: http://www.scilogs.fr/complexites/la-puissance-de-la-blockchain/

5. Dash P. Crypto Thoughts — Does it matter who came first Blockchain or Bitcoin? [Internet]. Medium. 2018 [cité 1 déc 2018]. Disponible sur: https://medium.com/crypt-bytes-tech/crypto-thoughts-does-it-matter-who-came-first-blockchain-or-bitcoin-fcdc0268f8f9

6. Quénetain S de. Blockchain Privée vs Blockchain Publique [Internet]. Blockchains Expert. 2018 [cité 14 nov 2018]. Disponible sur: https://www.blockchains-expert.com/blockchain-privee-vs-blockchain-publique/

7. Bitcoin - Argent P2P libre et ouvert [Internet]. [cité 14 nov 2018]. Disponible sur: https://bitcoin.org/fr/

8. Ethereum Project [Internet]. [cité 14 nov 2018]. Disponible sur: https://www.ethereum.org/

9. La blockchain : nouvelle plateforme numérique du secteur biopharmaceutique - Sanofi [Internet]. [cité 15 nov 2018]. Disponible sur: https://www.sanofi.com/fr/science-et-innovation/la-blockchain-nouvelle-plateforme-numerique-du-secteur

10. Blockchain in healthcare: Patient benefits and more [Internet]. Blockchain Unleashed: IBM Blockchain Blog. 2017 [cité 16 nov 2018]. Disponible sur: https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/

11. PwC Report: The disruption of blockchain and healthcare [Internet]. Digital Pulse. 2018 [cité 15 nov 2018]. Disponible sur: https://www.digitalpulse.pwc.com.au/report-blockchain-healthcare-disruption/

12. PricewaterhouseCoopers. Blockchain is here. What's your next move? [Internet]. PwC. [cité 15 nov 2018]. Disponible sur: https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

13. Research Briefing: Blockchain in Healthcare [Internet]. CB Insights Research.

[cité 15 nov 2018]. Disponible sur: https://www.cbinsights.com/research/briefing/blockchain-in-healthcare/

14. Santé, industrie pharmaceutique et blockchain [Internet]. Blockchain Partner. [cité 15 nov 2018]. Disponible sur: http://blockchainpartner.fr/sante-industrie-pharmaceutique-et-blockchain-notre-etude/

15. Nouvelle L. La blockchain, une technologie à fort potentiel dans la santé - L'Usine Santé. 30 mars 2018 [cité 15 nov 2018]; Disponible sur: https://www.usinenouvelle.com/editorial/la-blockchain-une-technologie-a-fort-potentiel-dans-la-sante.N673619

16. Substandard and falsified medical products [Internet]. World Health Organization. [cité 15 nov 2018]. Disponible sur: http://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products

17. Gulland A. Fake drugs: Why Governments must tackle global scourge. The Telegraph [Internet]. 29 mars 2018 [cité 15 nov 2018]; Disponible sur: https://www.telegraph.co.uk/news/2018/03/29/governments-urged-tackle-scourge-fake-drugs/

18. Thoma A, Farrokhyar F, McKnight L, Bhandari M. How to optimize patient recruitment. Can J Surg. juin 2010;53(3):205-10.

19. CHAPITRE I - Dispositions générales | CNIL [Internet]. [cité 16 nov 2018]. Disponible sur: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

20. Qu'est-ce ce qu'une donnée de santé ? | CNIL [Internet]. [cité 16 nov 2018]. Disponible sur: https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

21. Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

22. DMP : Dossier Médical Partagé [Internet]. [cité 18 nov 2018]. Disponible sur: https://www.dmp.fr/

23. Dossiers législatifs - LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé | Legifrance [Internet]. [cité 18 nov 2018]. Disponible sur: https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000029589477&type=general&legislature=14

24. Dossier médical personnel : un demi-milliard pour rien [Internet]. leparisien.fr. 2014 [cité 18 nov 2018]. Disponible sur: http://www.leparisien.fr/societe/dossier-medical-personnel-un-demi-milliard-pour-rien-04-01-2014-3461831.php

25. Le carnet de santé numérique va devoir faire ses preuves. 6 nov 2018 [cité 18 nov 2018]; Disponible sur: https://www.lemonde.fr/sante/article/2018/11/06/le-carnet-de-sante-numerique-va-devoir-faire-ses-preuves_5379433_1651302.html

26. Kohn LT, Corrigan J, Donaldson MS, éditeurs. To err is human: building a safer health system. Washington, D.C: National Academy Press; 2000. 287 p.

27. Brennan TA, Leape LL, Laird NM, Hebert L, Localio AR, Lawthers AG, et al. Incidence of Adverse Events and Negligence in Hospitalized Patients [Internet]. http://dx.doi.org/10.1056/NEJM199102073240604. 2010 [cité 18 nov 2018]. Disponible sur: https://www.nejm.org/doi/10.1056/NEJM199102073240604?url_ver=Z39.88-2003&rfr_id=ori%3Arid%3Acrossref.org&rfr_dat=cr_pub%3Dwww.ncbi.nlm.nih.gov

28. Les événements indésirables graves liés aux soins observés dans les établissements de santé : premiers résultats d'une étude nationale. 2005;16.

29. Shaw R, Drever F, Hughes H, Osborn S, Williams S. Adverse events and near miss reporting in the NHS. Qual Saf Health Care. août 2005;14(4):279-83.

30. Haute Autorité de Santé - Pertinence des soins – Les professionnels en action [Internet]. [cité 18 nov 2018]. Disponible sur: https://www.has-sante.fr/portail/jcms/c_2818625/fr/pertinence-des-soins-les-professionnels-en-action

31. Vos données personnelles sur internet peuvent valoir de l'or [Internet]. Challenges. [cité 19 nov 2018]. Disponible sur: https://www.challenges.fr/high-tech/vos-donnees-personnelles-sur-internet-peuvent-valoir-de-l-or_57690

32. McAfee Labs. Health Warning Report. :13.

33. BVA_VF_Mutations du système de santé_Les contrepoints de la santé_08.02.18_visu.pdf [Internet]. Dropbox. [cité 19 nov 2018]. Disponible sur: https://www.dropbox.com/s/c5w2cbvdy5vgldg/BVA_VF_Mutations%20du%20syst%C3%A8me%20de%20sant%C3%A9_Les%20contrepoints%20de%20la%20sant%C3%A9_08.02.18_visu.pdf?dl=0

34. Japaud M. Données de santé : les Français sont prêts à les partager. 2017;5.

35. Infographie sur les données de santé [Internet]. Faire avancer la santé numérique. 2017 [cité 19 nov 2018]. Disponible sur: http://www.faireavancerlasantenumerique.com/infographie-des-resultats-du-sondage-fasn-sur-les-donnees-de-sante/

36. Code de la santé publique - Article L1111-8. Code de la santé publique.

37. Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.

38. Zorabedian J. This infographic shows the state of encryption today [Internet]. Sophos News. 2016 [cité 19 nov 2018]. Disponible sur: https://news.sophos.com/en-us/2016/01/28/this-infographic-shows-the-state-of-encryption-today/

39. Piratage de données médicales : la France n'est pas prête [Internet]. L'Obs. [cité 19 nov 2018]. Disponible sur: https://www.nouvelobs.com/rue89/rue89-internet/20160405.RUE2568/piratage-de-donnees-medicales-la-france-n-est-pas-prete.html

40. Writer DH. York Hospital reports data breach affecting its employees [Internet]. Press Herald. 2016 [cité 19 nov 2018]. Disponible sur: https://www.pressherald.com/2016/02/24/york-hospital-reports-data-breach-affecting-its-employees/

41. A snapshot of data breaches in California: 6 key points [Internet]. [cité 19 nov 2018]. Disponible sur: https://www.beckershospitalreview.com/healthcare-information-technology/a-snapshot-of-data-breaches-in-california-6-key-points.html

42. PricewaterhouseCoopers. Global Economic Crime Survey 2016 [Internet]. PwC. [cité 19 nov 2018]. Disponible sur: https://www.pwc.fr/fr/publications/fraude-et-criminalite/global-economic-crime-survey-2016.html

43. IBM. IBM | Ponemon Cost of Data Breach 2017 [Internet]. 2017 [cité 19 nov 2018]. Disponible sur: https://www.ibm.com/security/infographics/data-breach/

44. DGOS. Atlas des systèmes d'information hospitaliers [Internet]. Ministère des Solidarités et de la Santé. 2016 [cité 19 nov 2018]. Disponible sur: https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/atlas-des-systemes-d-information-hospitaliers

45. L'interopérabilité : la clé de voûte de la e-santé | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 20 nov 2018]. Disponible sur: http://esante.gouv.fr/le-mag-numero-7/l-interoperabilite-la-cle-de-voute-de-la-e-sante

46. Fieschi PM. La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé. 2009;66.

47. Alliance PCH. Six gouvernements européens demandent un soutien pour la télésanté interopérable dans une lettre conjointe au réseau de santé en ligne [Internet]. [cité 20 nov 2018]. Disponible sur: https://www.prnewswire.com/fr/communiques-de-presse//fr/communiques-de-presse/six-gouvernements-europeens-demandent-un-soutien-pour-la-telesante-interoperable-dans-une-lettre-conjointe-au-reseau-de-sante-en-ligne-584089401.html.html

48. Fieschi PM. Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins. 2003;56.

49. Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS) | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 20 nov 2018]. Disponible sur: http://esante.gouv.fr/services/referentiels/referentiels-d-interoperabilite/cadre-d-interoperabilite-des-systemes-d

50. Coup de projecteur sur les rançongiciels : les modes de chiffrement [Internet]. Emsisoft | Security Blog. 2017 [cité 21 nov 2018]. Disponible sur: https://blog.emsisoft.com/fr/27699/rancongiciels-chiffrement/

51. Code de la santé publique - Article L1111-8-1. Code de la santé publique.

52. Quel identifiant pour le secteur de la santé ? La CNIL propose la création d'un numéro spécifique généré a partir du NIR mais anonymisé | CNIL [Internet]. [cité 22 nov 2018]. Disponible sur: https://www.cnil.fr/fr/quel-identifiant-pour-le-secteur-de-la-sante-la-cnil-propose-la-creation-dun-numero-specifique

53. L +Bastien. Data Lake : définition, avantages et inconvénients pour l'entreprise [Internet]. LeBigData.fr. 2017 [cité 22 nov 2018]. Disponible sur: https://www.lebigdata.fr/data-lake-definition

54. Linn LA, Koo MB. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. :10.

55. Cloud décentralisé : l'utilisateur devient fournisseur... et les prix chutent [Internet]. [cité 22 nov 2018]. Disponible sur: https://www.journaldunet.com/solutions/cloud-computing/1208437-cloud-decentralise-l-utilisateur-devient-fournisseur-et-les-prix-chutent/

56. France B. Les applications prometteuses des smart contracts [Internet]. Blockchain France. 2016 [cité 22 nov 2018]. Disponible sur: https://blockchainfrance.net/2016/01/28/applications-smart-contracts/

57. Blockchain, how SMART is your contract? [Internet]. IBM Government Industry Blog. 2016 [cité 22 nov 2018]. Disponible sur: https://www.ibm.com/blogs/insights-on-business/government/blockchain-smart-contract/

58. e-Estonia — We have built a digital society and so can you [Internet]. e-Estonia. [cité 22 nov 2018]. Disponible sur: https://e-estonia.com

59. Interoperability services [Internet]. e-Estonia. [cité 3 déc 2018]. Disponible sur: https://e-estonia.com/solutions/interoperability-services/

60. E-Estonia - Healthcare system [Internet]. e-Estonia. [cité 3 déc 2018]. Disponible sur: https://e-estonia.com/solutions/healthcare/

61. MedRec [Internet]. [cité 22 nov 2018]. Disponible sur: https://medrec.media.mit.edu/

62. Blockchain, pas si simple pour les grands groupes ! [Internet]. Siècle Digital. 2017 [cité 22 nov 2018]. Disponible sur: https://siecledigital.fr/2017/03/20/blockchain-pas-si-simple-pour-les-grands-groupes/

63. Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? | CNIL [Internet]. [cité 23 nov 2018]. Disponible sur: https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

64. CHAPITRE IV - Responsable du traitement et sous-traitant | CNIL [Internet]. [cité 23 nov 2018]. Disponible sur: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Section1

65. Limiter la conservation des données | CNIL [Internet]. [cité 23 nov 2018]. Disponible sur: https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

66. CHAPITRE III - Droits de la personne concernée | CNIL [Internet]. [cité 23 nov 2018]. Disponible sur: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article17

67. Malone D, O'Dwyer KJ. Bitcoin Mining and its Energy Footprint. In: 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014) [Internet]. Limerick, Ireland: Institution of Engineering and Technology; 2014 [cité 23 nov 2018]. p. 280-5. Disponible sur: http://digital-library.theiet.org/content/conferences/10.1049/cp.2014.0699

Université de Lille
FACULTE DE PHARMACIE DE LILLE
DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE
Année Universitaire 2022/2023

Nom : FACON
Prénom : Chloé

Titre de la thèse :
LA BLOCKCHAIN PEUT-ELLE RESOUDRE LES ENJEUX LIES A LA GESTION ET AU PARTAGE DES DONNEES DE SANTE ?

Mots-clés :

Gestion et partage des données de santé entre professionnels de santé et patients, dossiers patients, nouvelle technologie, blockchain, protection des données

---

Résumé :

Depuis quelques années, la révolution numérique bouleverse le monde tel que nous le connaissons. Le digital est devenu omniprésent, indispensable et touche tous les secteurs, de la politique à la culture, en passant par l'économie et la santé.
La blockchain fait partie de ces technologies qui promettent d'opérer un changement dans le monde de la santé. Technologie aussi disruptive qu'Internet, capable de renverser et de moderniser les structures de santé pour certains, simple illusion pour d'autres, la blockchain est une technologie qui fait débat et qui intéresse de plus en plus d'entreprises.
Grâce à son caractère décentralisé, sa transparence et garantissant l'intégrité et la sécurité des données, la blockchain promet de transformer la manière dont sont traitées, stockées et partagées les informations médicales, notamment grâce aux dossiers médicaux partagés.
Les données de santé sont des données sensibles qui doivent faire face à de nombreuses problématiques, notamment en terme de sécurité et d'interopérabilité. La blockchain peut-elle vraiment être une réponse à ces enjeux

---

Membres du jury :

Président : Serghereart, Eric, Professeur, Université de Lille, Lille

Assesseur(s) :
Grunewald, Alizée, Docteur en Pharmacie et Chef de Produit Senior Oncologie Thoracique, AstraZeneca, Paris
Olivier, Corentin, Pharmacien et Chef de Projet Digital Customer Engagement, Lundbeck, Paris