Université Paris 1 Panthéon - Sorbonne

UFR 27 Mathématiques et Informatique

MIAGE RÉSEAU DES MIAGE DE FRANCE Sorbonne

Mémoire de MASTER 1 MIAGE

Soutenu le : 02 septembre 2021

LE ROUX Corentin

Protection des données personnelles : Impact du RGPD sur les blockchains dans le secteur de la santé

Sous la direction de : Nicolas HERBAUT

Année d'étude : 2020/2021

Jury : Rebecca DENECKERE, Nicolas HERBAUT

Remerciements

Je tiens à remercier chaleureusement les enseignants de Paris 1 Panthéon-Sorbonne qui, au cours de ma première année de master, et ce malgré un contexte particulièrement compliqué qu'a été celui de la pandémie de la covid-19, ont su me transmettre des enseignements de qualité, faisant appel à notre travail d'équipe, à notre rigueur mais aussi à notre curiosité. C'est grâce aux connaissances et aux compétences qu'ils ont su faire grandir chez moi que j'ai pu réaliser le présent état de l'art ainsi qu'évoluer professionnellement au cours du stage effectué dans le département des Systèmes d'Information et de Télécommunications de RATP GROUP.

Je remercie également mon équipe qui a su, au cours des 5 mois passés, me faire découvrir avec une grande bienveillance et beaucoup de professionnalisme l'univers de la gestion de projet.

« la technologie n'est jamais neutre, c'est un terrain de conflit
influencé par les imaginaires et les intérêts
des personnes en charge de son design »

Michel Bauwens

Résumé

L'objectif de cet état de l'art est de présenter comment la blockchain peut trouver des utilités dans le secteur de la santé et en quoi l'entrée en vigueur du RGPD peut impacter ces cas d'usage, notamment avec la nécessité de permettre le droit à l'oubli. Nous concentrons cette étude sur ce secteur bien précis puisqu'il s'agit d'un domaine où de nombreuses données à caractère personnel sont impliquées et où il existe un réel enjeu de sécurisation, d'autant plus dans un contexte où les cyberattaques sont de plus en plus sophistiquées, se professionnalisent et ne craignent pas de prendre en otage les données – et potentiellement la vie – de patients.

Mots-clés : blockchain, rgpd, santé, technologies, loi, protection des données, droit à l'oubli, vie privée, consentement

Abstract

The objective of this state of the art is to present how blockchain can find uses in the healthcare and how the entry into force of the RGPD can influence these use cases, especially with the need to allow the right to be forgotten. We focus this study on this specific sector since it is a field where many personal data are involved and where there is a real challenge of security, especially in a context where cyber attacks are becoming increasingly sophisticated, professionalized and not afraid to take hostage the data - and potentially the lives - of patients.

Keywords : blockchain, data, gdpr, law, data protection, right to be forgotten, healthcare, privacy, consent

Table des matières

Liste des tableaux

Liste des figures

Liste des annexes

I. Introduction

Alors que la loi peine à donner un cadre légal à un écosystème en constante évolution, Internet, les utilisateurs sont de plus en plus sensibilisés à la nécessité de se réapproprier ce que certains qualifient d'ores et déjà d'or noir du XXIe siècle[1] : les données. A l'image du Big Brother que dépeignait George Orwell[2] dans son roman « 1984 », les États-Unis ont essuyé en 2013 les accusations de surveillance de masse, mise en lumière par le lanceur d'alerte Edward Snowden. Ces accusations sont lourdes de conséquences tandis que les propos alarmistes sont dignes d'Orwell, à la différence près que le réel a pris le pas sur la fiction. Pour rappel, voici un résumé de la surveillance de masse en quelques données[3] :

- Budget noir de 2013 : **68% du budget** revenait aux services de renseignement (*page 129*)
- 320 millions d'américains concernés
- 90% du trafic mondial s'effectue grâce à des technologies développées, possédées et/ou mises en œuvre par les autorités et les entreprises américaines
- Vœu le plus cher des services secrets : **la permanence** (stocker une fois pour toute, pour toujours et à jamais, l'ensemble des fichiers afin de constituer une mémoire parfaite). Autrement dit, l'archivage permanent. *« Un recensement continu qui se souvient de tout et ne pardonne rien »*
- *« J'ai donc aidé à rendre techniquement possible, pour un gouvernement, de recueillir l'ensemble des données numériques qui circulent dans le monde, de les conserver indéfiniment et de s'y reporter quand il le désire » - Edward Snowden*

Ce scandale précède un autre tristement célèbre, celui de Cambridge Analytica[4] en 2018 où près de 90 millions d'utilisateurs ont vus leurs données personnelles collectées et exploitées à des fins politiques. Ces évènements – suivis des révélations de la part de grandes entreprises telles que

[1] « La donnée… L'or noir du 21ème siècle », 20/12/18, https://www.linkedin.com/pulse/la-donnée-lor-noir-du-21ème-siècle-tarek-mansour/
[2] ORWELL, George, *1984*. Gallimard, 8 juin 1949.
[3] SNOWDEN, Edward. *Mémoires Vives*. SEUIL, 19 septembre 2019, 384 p.
[4] WYLIE Christopher. *Mindfuck, le complot Cambridge Analytica pour s'emparer de nos cerveaux*. Grasset, 11 mars 2020

Facebook sur la façon dont sont collectées, traitées et échangées les données – ont permis d'alarmer les utilisateurs sur ce qu'est réellement la gratuité sur Internet : une façade.

C'est dans ce contexte sensible que la loi, tentant péniblement de rattraper son retard dans ce système à deux vitesses, a fait entrer en application le Règlement Général sur la Protection des Données (RGPD) le 25 mai 2018. Son objectif est simple : recentrer le débat, définir et sensibiliser les acteurs et ainsi donner aux utilisateurs une plus grande transparence concernant leurs données à caractère personnel.

Dans cet état de l'art, nous centrerons notre propos sur les données personnelles du secteur de la santé, et ce pour plusieurs raisons :

- Le secteur de la santé est connu pour être celui souffrant le plus des cyberattaques, qui se font de plus en plus nombreuses et qui sont de plus en plus sophistiquées (Hamid Jahankhani 2019)
- Dès 2015, selon une étude[5] les utilisateurs plaçaient la sécurité de leurs données médicales dans leurs plus grandes préoccupations.

Nous nous focaliserons également sur une technologie directement liée aux données : la blockchain.

Par notre état de l'art nous tenterons d'apporter des éléments concrets de réponse quant aux défis et conséquences de l'entrée en vigueur du RGPD dans le secteur de la santé sur la technologie des blockchains.

[5] Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers, mars 2015

II. Méthodologie de recherche de littérature

L'objectif de ce mémoire de M1 était de s'intéresser à un sujet de recherche scientifique afin de produire une synthèse visant à mettre en exergue l'état des connaissances dans ce secteur au moment de la rédaction du présent mémoire.

Nous avons décidé d'orienter notre étude vers une tri-disciplinarité avec d'un côté le cœur même de notre formation à savoir l'informatique, d'un autre la notion légale et éthique qu'apporte le Règlement Général sur la Protection des Données (RGPD) et enfin d'un côté applicatif en s'intéressant spécifiquement au secteur de la santé. Depuis notre deuxième année de licence, nous apportons un regard particulièrement attentif à tout ce qui a trait aux problèmes relatifs à la protection des données à caractères personnels et, d'une manière plus globale, aux notions d'éthique et de cybernétique qui, de nos jours, prennent de plus en plus de place.

Avant d'en arriver au sujet sous sa formulation actuelle, nous nous étions orientés vers un champ plus large, sans nous restreindre à l'unique application au secteur de la santé. C'est en trouvant, lors de nos recherches, un mémoire traitant du même thème que nous avons décidé de recentrer la recherche sur un secteur donné.

Nos canaux de recherches ont été dans un premier temps Google Scholar et Arxiv. Nous avons également été amené à effectuer des recherches sur Semantic Scholar ainsi que sur Springer Link. Pour se faire, nous nous sommes demandé quels mots-clés définiraient au mieux le thème de notre recherche. Les plus évident étant « *blockchain* », « *gdpr* », « *law* », « *healthcare* » et « *data privacy* ». Etant donné l'aspect plus que brûlant de cette problématique qui est aujourd'hui au cœur d'un débat sociétal – où l'importance de penser sécurité et éthique se fait de plus en plus vif – il nous est arrivé à plusieurs reprises de tomber sur des articles encore à l'état de pré-print. Nous nous sommes alors concentrés sur l'idée globale de ces articles avant d'en extraire les sources et de nous focaliser sur celles-ci. Les résultats étant nombreux, nous avons fait le choix de filtrer sur les études les plus récentes. En effet, il s'agit d'un secteur évoluant grandement (le RGPD étant lui-même

encore très récent) et il nous a semblé plus pertinent de s'intéresser à des articles dont la potentielle obsolescence est minime.

Une fois une première sélection d'articles effectuées, nous avons regroupé les informations obtenues pour les divisés en sous-catégories afin de déterminer ce que chaque article pouvait apporter à cet état de l'art, dans quelle(s) partie(s) et dans quelles mesures. Cela nous a permis d'épurer les sources, certaines donnant plus un cadre de recherche que de réelles informations pouvant être réutilisées.

III. Background

Dans cette partie, nous tenterons d'apporter une définition aux deux grands axes majeurs de notre étude, afin de donner à celle-ci un cadre faisant consensus.

A. Le RGPD

1. Définition

Le Règlement Général de Protection des Données (RGPD) est un texte entré en vigueur le 25 mai 2018. Il s'inscrit dans la continuité de la loi de 1978 relative à l'informatique et aux libertés et vise à encadrer le traitement des données personnelles sur le territoire européen. De ce fait, le RGPD a comme objectif de :

- Définir la notion de données personnelles
- Impliquer l'utilisateur en le rendant acteur du système et propriétaire de ses données
- Définir des acteurs responsables du traitement de ces données
- Assurer une continuité de l'information
- Rétablir la confiance entre les utilisateurs et les professionnels

Cette réappropriation des données par les utilisateurs a vu ses effets se faire ressentir très rapidement. Ainsi, selon un sondage IFOP, 70% des Français auraient eu une prise de conscience concernant les problématiques de protection des données et s'y préoccupe plus qu'auparavant. De plus, après seulement un an d'activité, le RGPD a entrainé 144 376 plaintes adressées à la CNIL au niveau européen (CNIL 2019).

La prise de conscience ne se limite pas uniquement aux utilisateurs mais également aux acteurs professionnels qui s'approprie rapidement ce nouveau cadre légal et qui sont nombreux à remonter les violations de données, qui s'élèvent à 89 271 sur la même période.

2. Principes généraux du RGPD

Dans le chapitre 1 article 4 du RGPD, 26 termes sont définis clairement pour éviter toute ambiguïté. Parmi eux se trouvent des termes déjà employés mais dont la définition ne faisait pas toujours consensus comme :

- Les données à caractère personnel qui sont définies comme étant « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (CNIL 2018)[6]

- Le consentement qui explicite la nécessité pour la personne de donner, de manière « libre, spécifique, éclairée et univoque »[5] l'autorisation, par un acte clair (l'absence d'acte ne pouvant être un consentement) , au traitement de données à caractère personnel la concernant dans le seul cadre du traitement pour lequel elle y a consenti.

En plus de ces anciennes terminologies reprécisées, de nouvelles viennent enrichir le vocabulaire des droits relatifs aux données :

- Un traitement : Il désigne la ou les opérations appliquées par quelque moyen que ce soit sur une ou des données à caractères personnelles. Est notamment considéré comme un traitement : « la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »[5]

[6] « CHAPITRE I - Dispositions générales», CNIL, consulté le 14 mai 2021, https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1

- Le «responsable du traitement» qui est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » [5]

3. Les données au cœur des mesures

Au-delà de l'aspect organisationnelle et juridique, le chapitre 3 du RGPD reprécise les différents droits d'un individu concernant ses données. Ils sont au nombre de 6 (CNIL 2018) :

- Droit d'accès (article 15) : chaque individu est libre de savoir si ses données à caractère personnel sont traitées ou non et, dans la positive, à obtenir de plus amples informations quant à : la nature des données concernées, les finalités du traitement, les destinataires présents ou futurs de ces traitements, …

- Droit de rectification (article 16) : chaque individu est en droit de demander auprès du responsable du traitement la correction de toute donnée à caractère personnel erronée le concernant, et ce dans les plus brefs délais.

- Droit à l'oubli (article 17) : chaque individu est libre de demander auprès du responsable du traitement la suppression des données à caractère personnel le concernant, et ce dans les plus brefs délais. Ce droit peut toutefois être restreint par l'intérêt public (à des fins médicales ou archivistes), par le droit à la liberté d'expression et d'information ou encore par le droit de l'Union ou de l'Etat membre auquel appartient ledit responsable du traitement.

- Droit à la limitation du traitement (article 18) : chaque individu peut, selon certains critères, demander la limitation du traitement de ses données à caractère personnel auprès du responsable du traitement.

- Droit à la portabilité des données (article 20) : chaque individu est libre de demander de recevoir, dans un format lisible par machine, l'ensemble des données à caractère personnel

le concernant dont dispose le responsable du traitement sans que celui-ci s'oppose au transfert de ces données à un autre responsable du traitement.

- Droit d'opposition (article 21) : chaque individu est en droit de s'opposer, pour des raisons qui lui sont propre, au traitement de ses données à caractère personnel. Le responsable du traitement sera alors tenu d'arrêter tout traitement de ces données sauf s'il peut prouver qu'un motif légitime et impérieux requiert ce traitement.

Avec l'arrivée du RGPD, un questionnement sur la capacité de la blockchain à assurer les droits évoqués ci-dessus a été sujette à de nombreuses études.

B. Blockchain

1. Définition

Dans son article paru peu de temps après l'entrée en vigueur du RGPD, la CNIL définie la Blockchain comme étant *« une base de données dans laquelle les données sont stockées et distribuées sur un grand nombre d'ordinateurs et dans laquelle toutes les écritures effectuées dans ce registre, appelées « transactions », sont visibles de l'ensemble des utilisateurs, depuis sa création. La Blockchain n'est pas, par elle-même, un traitement de données ayant une finalité à part entière : il s'agit d'une technologie, qui peut servir de support à des traitements variés »* (CNIL 2018) [7] . Cette technologie est assez récente sur l'échelle des nouvelles technologies mais touche de nombreux secteurs d'activités, en particulier les finances, l'agroalimentaire ainsi que le secteur de la santé. Les blockchains ont permis l'essor des cryptomonnaies tels que le Bitcoin ou encore l'Ethereum.

2. Les caractéristiques de la Blockchain

Les caractéristiques de la blockchain peuvent être définies selon trois axes : le type de blockchain, ses acteurs et ses propriétés.

Commençons par le type. Il en existe trois distincts :

- La blockchain dite publique : tout le monde peut y accéder et ce depuis n'importe où. Elle est à la fois visible et modifiable par tous. Il est ainsi possible d'en observer le registre ou d'en devenir validateur sous certaines conditions (preuve de travail ou preuve d'enjeu). La blockchain publique la plus connu n'est autre que le Bitcoin, la première à la fois en terme historique mais également en termes d'importance sur le marché (Lars 2018).

- La blockchain à permission : aussi qualifiée de blockchain de consortium, elles sont à mi-chemin entre la publique et la privée. Des règles peuvent y être définie pour restreindre les autorisations de transactions et/ou d'approbation de celles-ci. Ce système est notamment

[7] « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », CNIL, consulté le 14 mai 2021, https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

utilisé par les institutions financières. La blockchain R3 regroupe près de 100 institutions financières dont BPN Paribas. Cet écosystème leur est propice puisque le secteur de la finance évolue dans un univers fortement réglementé et contrôlé, où l'anonymat peut constituer un danger. Plus récemment, en Avril 2021, la Blockchain « Aura Blockchain Consortium » a été créée par LVMH, Prada et Cartier pour permettre à leurs clients d'obtenir un certificat numérique de leurs achats, permettant ainsi de prouver son authenticité et de retracer son parcours de la conception à la livraison.

- La blockchain privée : elle est soumise à l'unique contrôle d'un gestionnaire qui gère à la fois la participation et l'approbation.

Intéressons-nous maintenant aux acteurs de la blockchain d'après le RGPD. 3 rôles sont définis :

- Les accédants qui peuvent consulter et copier la blockchain
- Les participants qui peuvent soumettre à approbation des transactions.
- Les mineurs qui peuvent approuver une transaction et créer un bloc conformément aux règles de la blockchain.

De manière générale, toute blockchain doit s'assurer que l'ensemble des participants peut visualiser l'intégralité des données figurant dans la blockchain, que plusieurs copies de la blockchain existent de manière simultanée et décentralisée. Une fois inscrite, aucune donnée ne doit pouvoir être modifiée et/ou supprimée de la blockchain. Enfin, chacune des décisions se fait par consensus sans intervention d'un arbitre centralisé omnipotent.

3. Le fonctionnement

Pour résumé simplement le fonctionnement d'une blockchain, considérons le schéma ci-dessous :

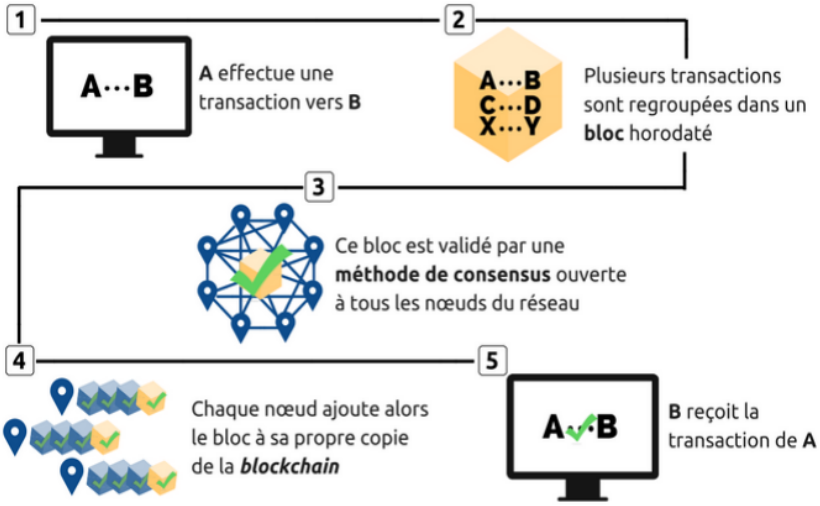

Figure 1: Exemple d'enregistrement d'une transaction sur une blockchain (Julien Aubert 2018) [8]

où chacune des étapes (début de transaction, saisi du bloc, validation, mise à jour et fin de transaction) est représentée. La partie 2 de ce schéma peut se détailler comme suit :

[8] « Rapport de la mission d'information commune sur la blockchain (chaîne de blocs) et ses usages : un enjeu de souveraineté », Assemblée Nationale, consulté le 14 mai 2021, https://www2.assemblee-nationale.fr/static/15/commissions/CFinances/blockchain-synthese.pdf

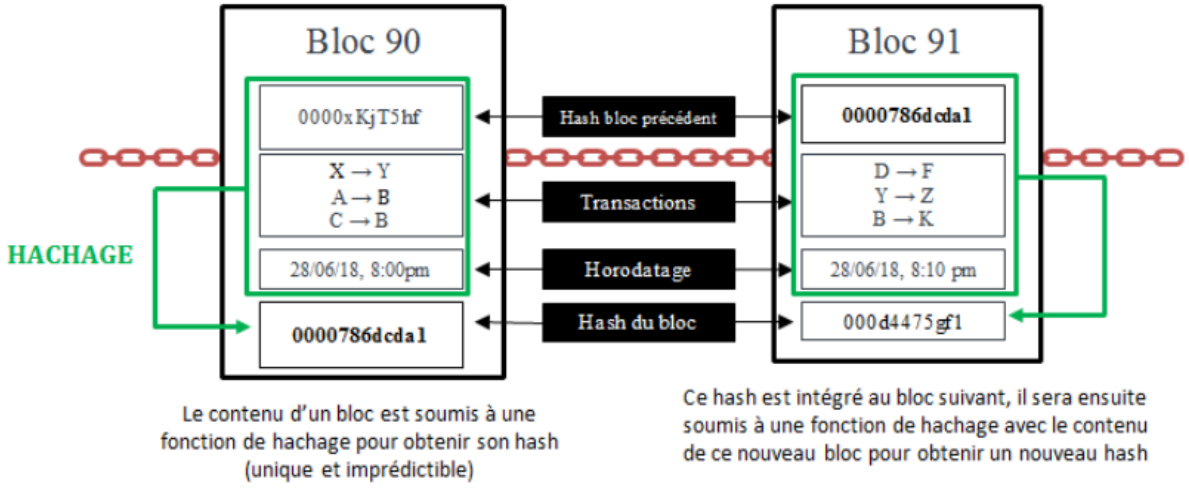

Figure 2: Le rôle du hachage dans l'intégrité de la chaîne de blocs [9]

Ainsi représenté, il est mis en évidence qu'une modification dans les transactions du bloc 90 à des fins malveillantes aurait un impact sur le hachage de ce bloc et, de ce fait, une conséquence sur le hachage de l'ensemble des blocs suivants.

La blockchain appartient à la plus grande famille des registres distribués (digital ledger technologies, DLT), dont les principales caractéristiques[10] sont :

- Distribuée : tous les participants du réseau disposent d'une copie intégrale du registre, pour une transparence totale
- Horodatage : l'horodatage de la transaction est enregistré sur un bloc.
- Unanimité : tous les participants du réseau sont d'accord sur la validité de chacun des enregistrements.
- Immuable : tout enregistrement validé est irréversible sauvegardé et ne peut pas être modifié
- Sécurisé : tous les enregistrements sont cryptés individuellement
- Programmable : une blockchain est programmable via les « smart contracts »

[9] « LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS)», Senat, consulté le 14 mai 2021, http://www.senat.fr/rap/r17-584/r17-5841.pdf

[10] MyHealthMyData (MHMD): Deliverable 2.6 - Privacy-by-design and compliance assessment | Zenodo

Un smart contract (contrat intelligent), est un programme informatique qui repose sur l'idée du « code is law » (Lawrence Lessig). L'obligation reliant les partis prenantes du contrat n'est plus régit par la loi mais par le code. Au cours de l'exécution du contrat, chacune des instructions inscrite au préalable dans le contrat donne lieu à des enregistrement dans la blockchain, ce qui permet de pérenniser les données et ainsi empêcher toute modification ou suppression à posteriori. [11]

Maintenant que nous avons posé les bases techniques et légale du sujet, nous allons réaliser l'état de l'art de la problématique évoquée précédemment : *Blockchain : quels défis et conséquences de l'entrée en vigueur du RGPD dans le secteur de la santé ?*

[11] Le fonctionnement d'un smart contract, consulté le 22/07/21, Smart Contract : Qu'est-ce qu'un contrat intelligent ? • BitConseil

IV. Blockchain et Healthcare

Une étude a été réalisée sur 1 752 enregistrements dans la base de données de Web of Science (il s'agit d'une base de données bibliographique et bibliométrique multidisciplinaire). Cette étude résulte en différents graphiques de type réseau qui permet ainsi de visualiser les sujets émergents dans le secteur de la santé. (Javad POOL 2020)

La figure ci-dessous présentent les sujets émergents de la recherche sur la confidentialité des données dans le secteur de la santé. Les sujets sont colorés selon les années. Ainsi, les sujets brûlants (qui émergent depuis 2018) sont colorés en jaune.

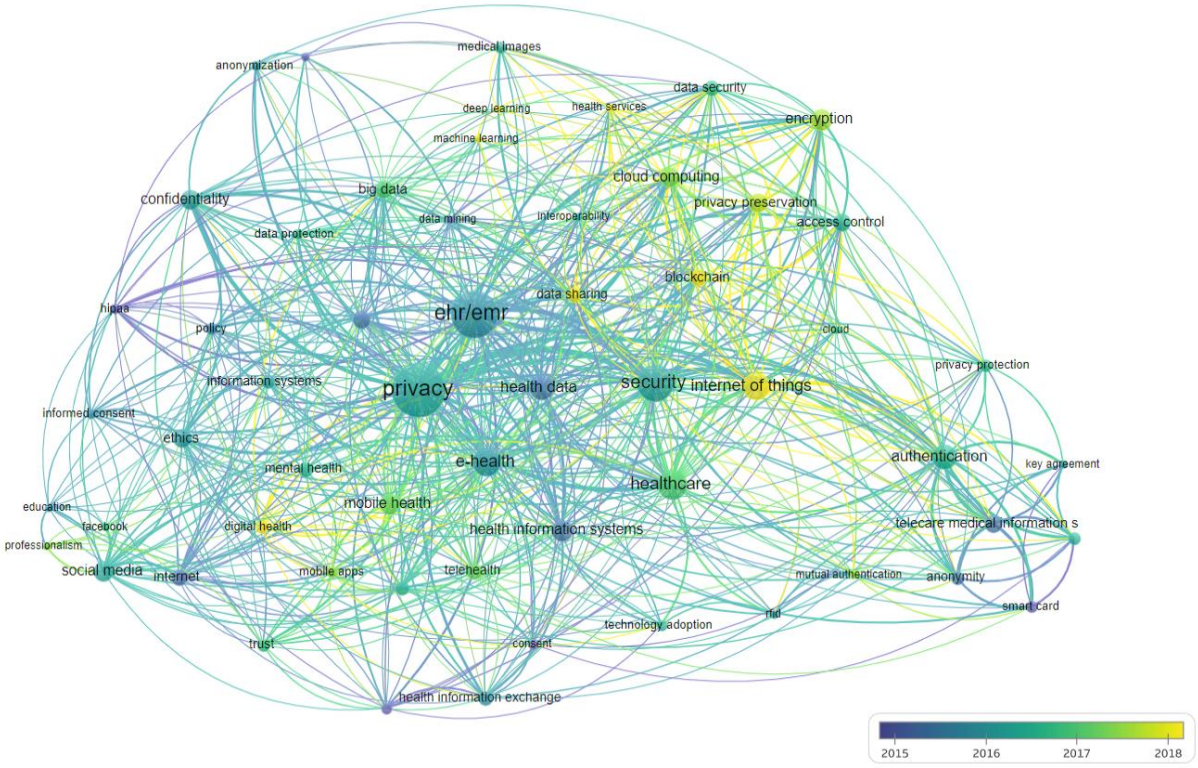

Figure 3 : Thèmes émergents de la recherche sur la confidentialité des données de santé accessible en *version web* (Javad POOL 2020)

Parmi les sujets d'actualité, nous relevons notamment l'IoT (Internet of things – les objets connectés), le data sharing, le digital health et la blockchain. Concernant les sujets les plus

représentés, nous retrouvons « privacy », « security » et « ehr/emr ». L'étude suggère ensuite que, selon son analyse, les sujets concernant notre état de l'art sont et seront :

	Thématique	Problématiques
Sujets émergents	Blockchain	*- Comment les blockchains peuvent influencer les pratiques de protection des données dans le secteur des soins de santé ?* *- Quels sont les risques et les opportunités en matière de protection de la vie privée concernant l'utilisation de blockchain dans le secteur de la santé ?*
Sujets à surveiller	RGPD	*- Comment les concepteurs de dispositifs médicaux prennent-ils en considération les impératifs du RGPD dans le processus de conception des outils numériques ?* *- A quels défis sont confrontés les DPD (délégués à la protection des données) pour protéger les données de santé en pratique ? Comment ces défis peuvent-ils être relevés ?*

Tableau 1 : Tableau récapitulatif des sujets (Javad POOL 2020)

L'intégralité du tableau des résultats est accessible en Annexe 1.

Cette étude conclue par un constat simple : le secteur de la santé se digitalise de plus en plus pour améliorer ses performances et co-créer de la valeur, mais il ne faut pas négliger la question de la protection de la vie privée des utilisateurs et de ses données. La blockchain fait partie des nouvelles tendances vers lesquelles s'orientent la littérature scientifique dans le secteur de la santé. D'autres sujets comme la protection des données à caractère personnel sont plus que jamais d'actualité avec l'entrée en vigueur du RGPD. (Javad POOL 2020).

Dans le secteur de la santé, le système de transactions porté par la technologie de la blockchain peut permettre de réglementer électroniquement le partage des dossiers médicaux des patients avec d'autres entités du secteur. Ainsi, nous pouvons imaginer que chaque entité qui serait impliquée dans la collecte, le stockage et/ou le traitement des données à caractère personnel d'un patient aura accès à un registre distribué privé et transparent. (Gregory Epiphaniou 2019)

Nous allons donner quelques exemples d'applications des blockchains dans le secteur de la santé :

- Suivi des processus de production de médicament pour éviter la contrefaçon : d'après l'Organisation Mondiale de la Santé (OMS) le nombre de contrefaçon à l'échelle mondiale varie entre 10 à plus de 30% selon les pays.[12] C'est dans cet objectif qu'Hyperledger ("*une plateforme open source, « une communauté ouverte, centrée sur le développement d'un ensemble de frameworks, d'outils et de librairies permettant de déployer des blockchains orientées entreprises. Il fait office de terrain neutre pour plusieurs framework de registre distribué »*[13]*)* a lancé un projet visant à vérifier la propriété et la qualité des médicaments au sein de la chaîne d'approvisionnement.

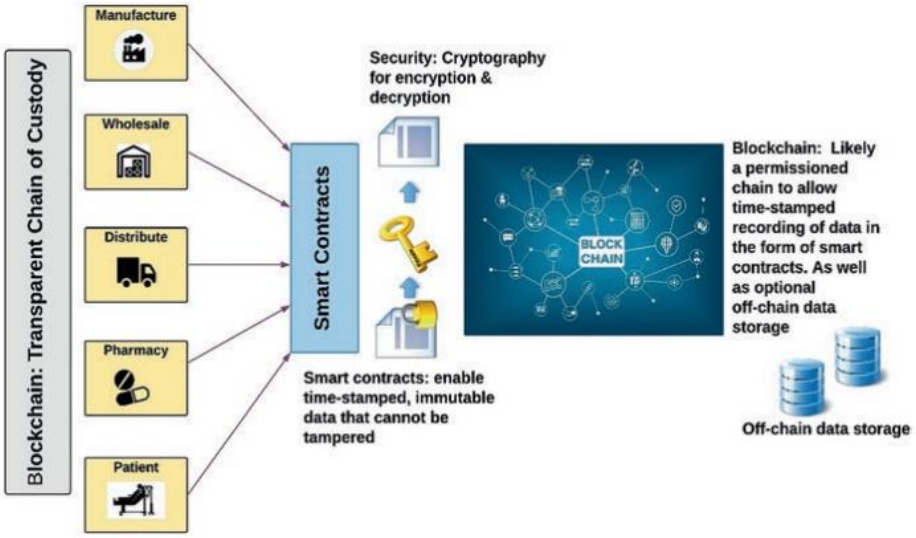

Figure 4 : La blockchain au service de la transparence de la supplychain

- Nous pouvons imaginer un « réseau dans lequel un hôpital, une clinique spécialisée et une compagnie d'assurance sont impliqués dans le diagnostic et le traitement des patients avec l'approbation du paiement respectivement. Les contrats intelligents peuvent être utilisés pour coordonner les étapes de la prise en charge du patient au fur et à mesure qu'elles se produisent.

[12] FIGHTING FALSIFIED MEDICAL PRODUCTS – Sanofi, mars 2021, Fighting Falsified Medical Products (sanofi.com)
[13] Qu'est-ce qu'Hyperledger, Hyperledger – Open Source Blockchain Technologies

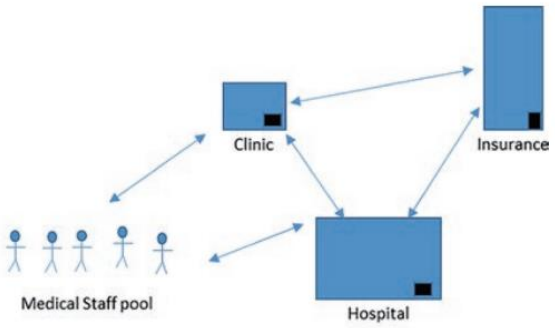

Figure 5 : Utilisation des contrats intelligents dans le secteur de la santé (Gregory Epiphaniou 2019)

Le site diagnostic de l'hôpital fixe automatiquement un rendez-vous à la clinique spécialisée, et l'approbation du paiement est vérifiée par rapport aux dossiers d'assurance. L'état global du registre de comptes permet de détecter rapidement les litiges et les anomalies et de traiter automatiquement les cas en utilisant la base de données de l'entreprise. les cas peuvent être traités automatiquement en utilisant le contrat. Une extension de ce système pourrait même inclure l'attribution du travail au personnel médical. Les contrats intelligents pourraient interroger les dossiers sur l'expérience du personnel pour attribuer le travail à ceux qui sont à la fois qualifiés et disponibles » [traduction libre] (Gregory Epiphaniou 2019).

- Le framework de blockchain Hyperledger Indy est utilisé afin de permettre l'accréditation du personnel médical (Figure 6). Grâce à cette organisation, les hôpitaux peuvent s'assurer que le personnel médical est à la fois qualifié (1) et compétent (2).

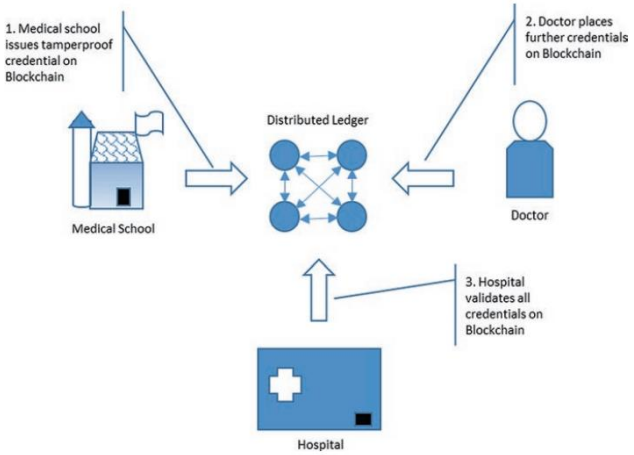

Figure 6 : Accréditation du personnel médical via le framework Indy

- Enfin, un dernier cas d'usage mais pas des moindres : sécuriser et permettre un meilleur suivi de la chaîne d'approvisionnement d'organes. Ce processus, qui représente 34 000 transplantations et 60 000 personnes en attente de trouver un donneur en 2017 selon les chiffres de la commission européenne, est un domaine critique du secteur de la santé, car il implique énormément de données sur le donneur, le receveur, l'organe, les médecins, les hôpitaux, … Une mauvaise gestion de cet amas de donnée peut entrainer des pertes, des duplications, des altérations voire des erreurs. Au-delà des risques que représentent de telles données s'ajoutent celui des chaînes d'approvisionnement parallèle (trafic illégal). Certains de ces organes obtenus de manière non-éthique peuvent se retrouver sur la chaîne d'approvisionnement initiale. Ce trafic parallèle implique directement les populations les plus pauvres où, d'après une étude, le prix d'un rein serait de 1000$. Dans ce contexte, la blockchain pourrait jouer un rôle essentiel par sa capacité à sécuriser et maintenir l'exactitude des données, dissuader les procédures illégales, protéger les patients en leur évitant de s'exposer à des greffes de mauvaise qualité, ou encore pour retracer le parcours d'un organe au cas où la greffe se serait mal passée (organe contaminé ou rejet). (Nicanor Chavez 18/07/20)

Ainsi, nous avons vu que la technologie blockchain possède un grand potentiel dans le secteur des soins de santé où son spectre applicatif peut être très vaste. Par ailleurs, il a été estimé que près de 55% des applications médicales auront adopté la blockchain pour un déploiement commercial d'ici 2025. Par ailleurs, cela pourrait représenter un réel retour sur investissement puisque, rappelons-le, le secteur des soins de santé est celui qui subit le plus grand nombre de violations de données avec en moyenne 2,5 fois plus que les autres industries, soit environ 380 $ par dossier de patient unique compromis en 2017. (Nicanor Chavez 18/07/20)

Même si la blockchain apporte des avantages d'un point de vue protection des données, elle soulève également des interrogations concernant sa compatibilité avec le RGPD. A l'origine, le RGPD avait pour cible les bases de données conventionnelles mais ne prévoyait pas de cadre légal spécifique pour les nouvelles technologies émergentes comme l'est la blockchain. (Nicanor Chavez 18/07/20)

Maintenant que nous avons vu comment la blockchain peut trouver des applications dans le secteur de la santé (notamment en termes de traçabilité, de fiabilité des informations et en travail collaboratif), nous allons nous intéresser à la question des interactions existantes entre le RGPD et la blockchain.

V. Les impacts du RGPD sur les Blockchains

Seulement deux mois après l'entrée en vigueur du RGPD, un rapport public[14] a été publié avec comme acteurs moraux notables l'Assemblée nationale et le Sénat. Celui-ci traite des enjeux technologiques de la blockchain et évoque à plusieurs reprises sa capacité à être conforme avec le RGPD.

En effet, l'entrée en vigueur du RGPD représente un réel enjeu juridique, notamment en termes de protection des données à caractère personnel dans les blockchains. Cette problématique y est dépeinte comme particulièrement « complexe à traiter » (p.92) et la question suivante y est posée : « la blockchain est-elle compatible avec le RGPD ? » .

D'après Mmes Amandine Jambert (ingénieure experte à la CNIL) Guilda Rostama (juriste) et Tiphaine Havel (conseillère parlementaire) la technologie de « la blockchain, en particulier publique, pourra difficilement être pleinement compatible avec le RGPD ».

Il y a deux raisons principales à cette réserve quant à la position de la CNIL à affirmer ou réfuter l'éventuelle capacité de la blockchain à se conformer au RGPD :

- La première raison est que le RGPD interdit les transferts de données en dehors de l'Union européenne en dehors de certains conditions bien spécifiques. Or, dans une technologie où les mineurs peuvent éventuellement se trouver n'importe où dans le monde et ne sont pas nécessairement connus, cette exigence législative peut être un réel défi bloquant la conformité.

- La seconde raison concerne l'un des droits de l'utilisateur porté par le règlement : le droit à l'oubli.

[14] LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS), 20 juin 2018, r17-5841.pdf (senat.fr)

Daniel Augot évoque « l'opposition classique entre la préservation de la vie privée et les préoccupations sécuritaires des Etats (qui veulent contrôler les flux) ».

Dans un second rapport[15], la CNIL reprend les grandes lignes de l'interaction entre la blockchain et le RGPD. Son objectif est de donner une base de travail et de compréhension de quel acteur est responsable de quoi, mais également d'éclaircir quelles sont les zones d'ombres en ce qui concerne la compatibilité.

Ainsi, le rapport suggère que le responsable de traitement soit le participant ayant soumis une donnée à la validation des mineurs si celui-ci le fait dans le cadre de l'exertion de son activité professionnelle.

En ce qui concerne les sous-traitants, ils peuvent être :

- Des développeurs de contrats intelligents qui traitent de données à caractère personnel
- Des mineurs qui valident l'enregistrement dans la blockchain de données à caractère personnel

Parmi les 6 droits portés par le RGPD, seulement trois ne semblent pas poser de problème de conformité (le droit à l'information, le droit d'accès et le droit à la portabilité). En revanche, le droit de rectification, le droit d'opposition et le droit à l'oubli nécessite une analyse plus poussée pour s'assurer de leur respect.

Prenons l'exemple du droit à la rectification. Il est techniquement impossible de modifier un bloc dans une chaîne et, par conséquent, de faire appliquer ce droit. Afin de palier à cette lacune, il est suggéré de stocker sous la forme d'un engagement cryptographique («un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de le retrouver ou de la reconnaître à partir de cette seule version engagée » [14]) et d'adapter le processus, en remplaçant le principe de rectification par une mise à jour via la création d'un nouveau bloc dans la chaîne : « en effet, une transaction ultérieure

[15] Premiers éléments d'analyse de la CNIL : BLOCKCHAIN, septembre 2018, La blockchain (cnil.fr)

peut toujours annuler la première transaction, même si la première transaction apparaîtra toujours dans la chaîne. » [14]

Concernant le droit à l'effacement, qui est également techniquement impossible, la CNIL suggère l'inscription des données sous la forme de l'un des procédés cryptographiques suivants :

- Un engagement
- Une empreinte issue d'une fonction de hachage à clé
- Un chiffé utilisant un algorithme et des clés conformes à l'état de l'art

De sorte que l'accès à la donnée puisse être rendu impossible par le responsable du traitement et permettre ainsi de reproduire un comportement similaire à celui d'un effacement.

Nous allons maintenant nous intéresser aux articles du RGPD pouvant impacter le secteur de la santé. En effet, l'entrée en vigueur de cette nouvelle réglementation représente un réel enjeux pour les HI qui doivent légitimer tout traitement de données à caractère personnel et pouvoir prouver que les données sont utilisées uniquement pour ce traitement spécifique. Une étude (Annexe 4) résume ce que les HI doivent considérer lorsqu'ils utilisent des DLT afin de protéger les PHI et minimiser les risques et les coûts que représenteraient une non-conformité au RGPD.

Maintenant que nous avons étudié quels aspects portés par le RGPD pouvaient éventuellement affecter les blockchains, nous allons nous concentrer sur les articles cherchant à démontrer la faisabilité de l'application de cette nouvelle législation à la technologie de la blockchain.

VI. Assurer la conformité RGPD des Blockchains

Dans cette partie, nous allons essayer de montrer comment les blockchains peuvent se conformer au RGPD.

A. Rappel sur le droit à l'oubli

Comme nous l'avons évoqué précédemment, le droit à l'oubli est par design incompatible avec la blockchain qui, par sa conception, est immuable : rien ne peut être supprimé du registre. Toutefois, il faut garder à l'esprit que le droit à l'oubli n'est pas absolu : il existe de nombreuses exceptions qui figurent dans l'article 17 du RGPD :

> *« Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:*
>
> *a) à l'exercice du droit à la liberté d'expression et d'information;*
>
> *b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;*
>
> *c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;*
>
> *d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou*

e) à la constatation, à l'exercice ou à la défense de droits en justice. » [16]

C'est pourquoi les solutions proposées ne permettent pas de « supprimer » à proprement parler les données de la blockchain mais permettent, via un moyen de contournement, d'obtenir les mêmes effets.

B. BCdiploma

La première solution que nous allons présenter est celle proposée par BCdiploma, un projet français qui a vu le jour début 2018 et qui repose sur l'Ethereum. « BCdiploma permet aux institutions, via une application SaaS, de générer des documents dématérialisés accessibles sous forme de liens sécurisés utilisables gratuitement par leurs porteurs. Le diplômé, par exemple, peut transmettre son lien à un recruteur ou l'insérer sur son profil LinkedIn : un simple clic permet de consulter des données infalsifiables. La solution permet de mener des projets de transformation digitale à grande échelle. L'institution paramètre des "modèles des documents" et n'a plus qu'à fournir les données correspondantes (fichier Excel ou API) pour automatiser la délivrance des documents en ligne sous forme de liens. Les données sont authentifiées et stockées sur une blockchain, elles ne sont pas conservées par BCdiploma. Les liens délivrés permettent leur affichage en temps réel. » [17]

Ce projet a été construit pour être compliant by design. Après avoir été diplômé, chaque étudiant recevra, de manière sécurisé, un lien pour accéder à son diplôme. Ce lien ne peut pas être retracé à partir de la transaction Ethereum mais celle-ci est nécessaire pour accéder au diplôme. En tant que seul accesseur à ce lien, il en est responsable en cas de partage. S'il souhaite faire valoir son droit de retrait, l'école aura pour impératif de vérifier son identité puis de détruire la clé de persistence. Dès lors, plus aucune application ne sera en mesure de décrypter le diplôme. (Aurelie Bayle 2018)

[16] Article 17 du RGPD, consulté le 10/07/21 Article 17 EU règlement général sur la protection des données (EU-RGPD). Privacy/Privazy according to plan. (privacy-regulation.eu)
[17] BCdiploma, consulté le 20/07/21, BCdiploma - Catalogue GouvTech (numerique.gouv.fr)

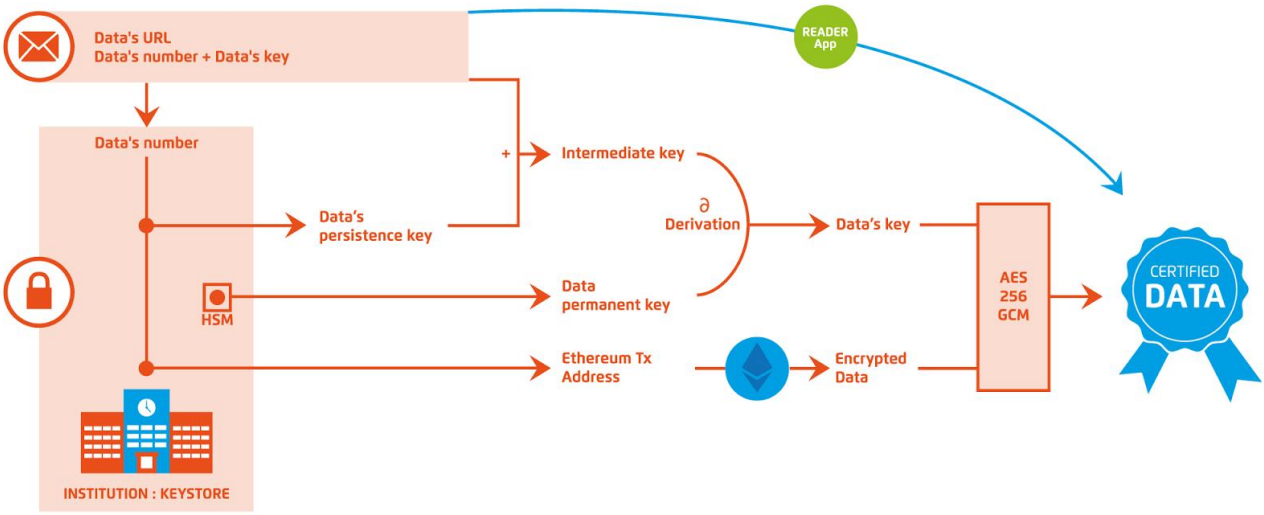

Figure 7 : Architecture de BCdiploma[18]

Ainsi, BCdiploma répond à la double problématique de permettre à l'utilisateur d'exercé son droit à l'oubli tout en traitant également l'enjeu de clarification des acteurs et des responsabilités autour du traitement des données à caractère personnel au sein de la blockchain.

Cette solution pourrait être transposée dans le secteur de la santé comme présenté avec le cas Hyperledger Indy pour protéger les informations médicales d'un patient, ou pour certifier le personnel médical.

C. MyHealthMyData (MHMD)

D'autres projets proposent une solution technique à cette problématique du droit à l'oubli. Nous pouvons citer MHMD, une plateforme de recherche et d'innovation ayant pour but de changer fondamentalement la façon dont sont traitées et échangées les données sensibles. MHMD se décrit comme étant en passe d'être « le premier réseau ouvert d'informations biomédicales centré sur la connexion entre les organisations et les individus, encourageant les hôpitaux à commencer à mettre à disposition des données anonymes pour la recherche ouverte, tout en incitant les citoyens à devenir les propriétaires et contrôleurs ultimes de leurs données de santé »[19]. MHMD met

[18] BCdiploma – White Paper – Avril 2018, BCD-WhitePaper_last.pdf (evidenz.io)
[19] NEW PARADIGM IN HEALTHCARE DATA PRIVACY AND SECURITY, My Health My Data

également à disposition son DPIA (Data protection impact assessment) dans lequel est notamment décrit comment chaque droit porté par le RGPD est respecté (Annexe 5).

« MHMD utilise une blockchain comme un système décentralisé permettant de contrôler, surveiller et appliquer les directives du RGPD tout au long du cycle de vie du partage des données. Dans sa conception, MHMD enregistre les données privées à l'intérieur d'un serveur central dans les installations du contrôleur de données. Une fonction de correspondance entre les métadonnées et les données privées permet la traçabilité et la logique métier. La fonction de mappage est également stockée en dehors de la blockchain. Ainsi, pour exercer le droit à l'oubli, il suffit de briser le lien entre la blockchain et les données privées dans la fonction de mappage. » (Aurelie Bayle 2018)

D'après son site[20], MHMD est en conformité au RGPD car :

- « Chacun des membres du réseau MHMD est un nœud de la blockchain qui interagit avec les serveurs du contrôleur de données/du consommateur de données par le biais d'un pilote de blockchain qui lance la transaction et écoute les évènements de la blockchain.

- Les données ne sont jamais stockées directement sur la blockchain : elles sont stockées dans le contrôleur de données

- Chaque nouvelle action (requête on injection) est enregistrée dans la blockchain en utilisant une valeur de hachage de l'élément de donnée. Cette valeur est ensuite mappée en utilisant une base de données de mappage en dehors de la chaîne dans le contrôleur de données, qui sert de pont entre la valeur de hachage et l'élément de donnée.

- Chaque élément de données est indexé puis référencé dans la blockchain en stockant la valeur de hachage de l'élément de données indexé : de cette façon, la blockchain conserve l'enregistrement des données disponibles et de l'historique associé sans qu'il soit nécessaire d'enregistrer les données privées.
- Pour faire correspondre les études et les éléments de données, un modèle bitmap est utilisé : le bitmap est stocké dans la base de données de mappage hors chaîne. Cela permet de

[20] MHMD, consulté le 23/07, Blockchain – My Health My Data

supprimer le lien entre la donnée utilisée dans une étude et la valeur stockée dans la blockchain en modifiant le bitmap directement dans la base de données cartographique. Avec cette méthode, nous atteignons le droit à l'oubli imposé par le GDPR. »

Dans un autre article publié par les mêmes auteurs, ceux-ci décrivent de manière plus approfondie la solution. Dans un premier temps, est expliqué comment l'auditabilité du système représente un enjeu majeur concernant la capacité à être conforme au RGPD. Grâce au design du système mis en place, MHMD répond aux droits d'accès ainsi qu'au droit à l'oubli. Ainsi, tout utilisateur désireux de connaître où sont passées toutes ses données et à qui elles ont été partagées pourra faire une demande, tout comme il pourra faire une demande de les rendre inaccessible. Cela s'explique par ce qui semblait initialement être un frein à la conformité du RGPD : l'immuabilité de la blockchain. En effet, ce principe permet d'auditer les pistes de données et la gestion des données avec la certitude que la base n'a pas été altérée. (Mirko Koscina 2019)

MHMD décrit son système comme étant, à sa connaissance, la première solution de blockchain entièrement compatible au RGPD dans le domaine de la santé. Il repose sur :

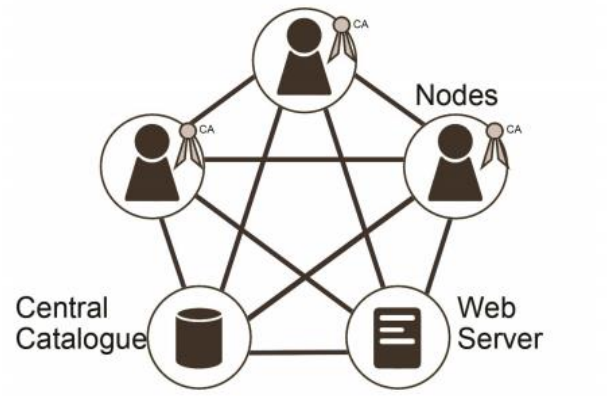

Figure 8 : Architecture MHMD

- Catalogues : l'architecture est divisée en deux types de catalogues :
    - Catalogues locaux : Normalise les données (génère des métadonnées à partir de données réelles) et les enregistres dans le catalogue central.
    - Catalogue central : version agrégée des données disponibles. Il permet aux utilisateurs du système de rechercher des données de manière consolidée. Les

responsables du traitement des données doivent appliquer au minimum un niveau d'anonymisation avant le partage des données. L'utilisateur ne saura pas qui fournit les données.

- Central Web Server : Sert de point d'entrée aux utilisateurs pour interagir avec l'ensemble du système. Ce serveur ne détient aucune donnée autre que celles d'authentification. Cette dernière s'effectue via la saisie d'un nom d'utilisateur, d'un mot de passe et d'une organisation (qui aura la charge de valider ces données). En cas de faille du côté de l'organisation, seuls ses utilisateurs seront impactés (et pas le système tout entier).

- Certificate authorities : Chaque organisation possède sa propre autorité de certification via une API (CA API) qui est intégrée au serveur web.

- Nodes : Un nœud se caractérise par :
    - L'appairage d'une blockchain
    - Un pilote qui met en œuvre la logique commerciale principale (traitement des demandes émanant du Central Web Server et communique aux pairs locaux pour exécuter et traiter les transactions).
    - Une base de données de mappage locale qui permet de garder une trace de chaque référence à un élément de donnée dans la blockchain.
    - Un CA en charge d'émettre des certificats dans l'organisation
    - Une CA API qui relie le Central Web Server au CA afin d'assurer l'authentification

D. CUREX

CUREX est un projet qui a vu le jour en décembre 2018. Son objectif est double :

- sécuriser les données confidentielles des patients
- accroître la confiance des patients dans les infrastructures du secteur de la santé

Ce dernier besoin est à son paroxysme dans un univers où les données sont sensibles et partagées entre des parties prenantes transfrontaliers.

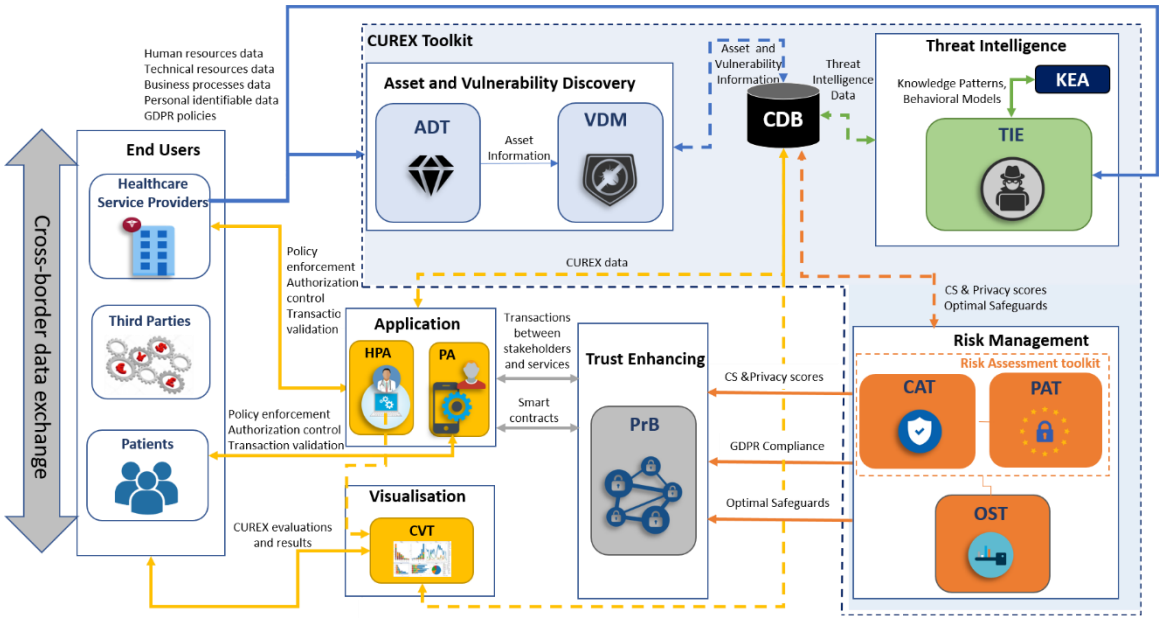

Figure 9 : Architecture de CUREX[21]

Le workflow de la plateforme CUREX est le suivant [19] :

1. l'ADT détectent les assets et récupèrent les informations nécessaires au processus d'évaluation des risques et les transmets au VDM
2. Le VDM recherche des vulnérabilités puis les partages au TIE et au KEA afin d'effectuer des analyses plus approfondies.
3. Le résultat de cette analyse est partagé à la boîte à outil d'évaluation des risques :
    a. CAT évalue les risques de cybersécurité
    b. PAT évalue les risques de confidentialité
    c. OST effectue une analyse coûts/avantages et propose des mesures de protection optimale à exécuter en fonction des risques calculés par les deux autres outils
4. Les scores d'évaluation des risques de cybersécurité et de confidentialité ainsi que certaines informations relatives aux métadonnées et la stratégie de sécurité optimale sont stockés dans la blockchain privée.
5. La blockchain gère les relations entre les différentes parties prenantes et les applications en générant des contrats intelligents.

[21] Curex Project, consulté le 21/07/21. CUREX Platform | CUREX (curex-project.eu)

Ainsi, la plateforme CUREX permet des échanges de données de santé respectant les normes de cybersécurité et de vie privée, en se basant sur trois axes stratégiques :

1. Une meilleure sécurité des services, des données et des infrastructures du secteur de la santé
2. Un risque amoindrie de cyberattaques engendrant une violation de la confidentialité des données
3. Une confiance et une sécurisation accrue des patients

et se repose sur une multitude d'outils. (Farnaz Mohammadi 2019)

Enfin, une étude plus récente propose un arbre décisionnel (Annexe 6) afin de déterminer, selon le cas dans lequel nous nous situons, (blockchain publique sans permission, blockchain publique avec permission, blockchain de consortium avec permission ou blockchain privée avec permission) et redirige vers les bonnes références. **(Pavlenkova 2020)**

VII. Conclusion

Au cours de cet état de l'art, nous avons tenté de résumer et de mettre en cohérence des articles de recherche scientifique ainsi que des livre blanc afin d'apporter une réponse à la problématique suivante : *Blockchain : quels défis et conséquences de l'entrée en vigueur du RGPD dans le secteur de la santé ?*

D'abord, nous avons posé les bases en rappelant ce que représente le règlement général sur la protection des données et en quoi consiste la blockchain avant de montrer que les thématiques liées aux nouvelles technologies (blockchain, IoT, cloud computing, …) ont le vent en poupe dans la littérature scientifique et côtoient des sujets déjà bien ancré dans le débat tel que la vie privée et les enregistrements de données médicaux. Cette première analyse nous a permis de mettre en exergue la pertinence du sujet de l'état de l'art, montrant que la problématique s'inscrivait bel et bien dans un enjeu contemporain.

Ensuite, nous nous sommes intéressés aux applications de la blockchain dans le secteur de la santé. Nous avons notamment pu évoquer des projets tels que l'utilisation dans la traçabilité des médicaments pour lutter contre la propagation de faux sur le marché ou encore dans la gestion des accréditations du personnel soignant.

Une fois cette première étude de l'existant réalisé, nous nous sommes concentrés sur la relation entre RGPD et blockchain, pour s'avoir s'il s'agissait d'un « faux problème » [22] comme certains articles de presse peuvent laisser entendre. En effet, au cours de nos recherche nous avons constaté que le soucis majeur entre ces deux thématiques concernait particulièrement la blockchain publique. Toutefois, même si ces articles pointent du doigt un véritable sujet qu'est celui de l'identification des acteurs et des responsabilités inhérents aux données, ils omettent généralement d'évoquer un autre défi conceptuel et architectural, à savoir permettre aux utilisateurs d'exercer leur droit de rectification ou encore leur droit à l'oubli. Ces deux droits, par nature, semble en total contradiction avec le principe même de la blockchain qui se veut immuable.

[22] « Blockchain et RGPD, un faux débat ! », consulté le 05/08/21, Blockchain et RGPD, un faux problème ! (siecledigital.fr)

Enfin, nous avons étudié comment la lecture scientifique répondait à cette problématique de conformité des blockchains au RGPD. Nous avons ainsi évoqué différentes solutions telles que la création d'une clé de persistence ou encore d'une fonction de hachage ce qui permet aux utilisateurs d'exercer leur droit à l'oubli.

Cette étude nous aura permis de prendre conscience des nombreux cas d'usage que peut trouver la blockchain, qui semble en être à ses balbutiement dans le secteur de la santé. Il semble clair que ce sujet est et restera encore d'actualité pour les prochaines recherches à venir, d'autant plus dans un contexte de pandémie internationale qui aura été propice aux cyberattaques visant le secteur de la santé. Nous pouvons notamment citer[23] :

- 05/2017 : Malware sur le système de santé britannique ayant impacté 16 centres de santé, 200 000 ordinateurs et 1200 appareils de diagnostic.
- 03/2019 : Hameçonnage sur le CHU de Montpellier ayant permis le déploiement d'un virus sur plus de 600 postes.
- 06/2019 : Rançongiciel sur le groupe français Eurofins ayant entrainé une potentiellement perte de 62€M de chiffre d'affaires [24]
- 03/2020 : Attaque par déni de service du groupe AP-HP ayant impacté 39 établissements
- 07/2020 : Fuite de plus de plus de 6 000 données de rendez-vous de la plateforme Doctolib, aujourd'hui fer de lance de la campagne vaccinale française.

En plus des frais engendrés par la cyberattaque, par son traitement et par l'audit des infrastructures s'ajoutent d'éventuels sanctions en cas de non-conformité au RGPD. Celles-ci peuvent atteindre le montant le plus élevé entre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. A titre indicatif, en 2018 l'hôpital de Barreiro[25] en Espagne a été condamné à 400 000€ d'amende pour :

[23] «Cyberattaques dans le secteur de la santé », consulté le 05/08/2021, Avant de Cliquer Cyberattaques dans le secteur de la santé

[24] « Ransomware : Eurofins montre que même en payant, ça coûte cher », consulté le 05/08/2021, Ransomware : Eurofins montre que même en payant, ça coûte cher (lemagit.fr)

[25] « Sécurité des données hospitalières : un hôpital condamné ! », consulté le 05/08/2021, Sécurité des données hospitalières : un hôpital condamné ! | Dijon Santé - La Web TV santé de Bourgogne Franche-Comté (dijon-sante.fr)

- violation des principes d'intégrité/de confidentialité des données des patients
- violation du principe de limitation d'accès aux données des patients
- incapacité du responsable du traitement des données à garantir l'intégrité des données à caractère personnel des patients

Pour aller plus loin dans cette étude, il serait intéressant d'étudier l'impact financier et environnemental que représente la digitalisation d'un secteur à l'allure vieillissante qu'est celui de la santé.

D'autre part, il existe un paradoxe dans cette problématique de conformité de la blockchain au RGPD car, si il peut être compliqué de se conformer à 100% au RGPD, il n'empêche que la blockchain pourrait représenter un réel outil pour permettre aux utilisateurs d'avoir un meilleur contrôle sur leurs données personnelles, avec par exemple le projet « d'identité auto-souveraine » qui vise à fournir aux individus "une identité numérique portable à vie qui ne dépend d'aucune autorité centrale et ne peut jamais être retirée" (The Sorvin Foundation 2018)[26].

[26] Decentralized identity improves the end-user experience and helps enterprises strengthen data privacy.https://www.citi.com/ventures/perspectives/opinion/digital-identity.html

Bibliographie

Anton Hasselgren, Paul Kengfai Wan, Paul Kengfai Wan, Katina Kralevska, Danilo Gligoroski, Arild Faxvaag. «GDPR Compliance for Blockchain Applications in Healthcare.» 2020.

Aurelie Bayle, Mirko Koscina, David Manset, Octavio Perez-Kempner. «When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry.» 2018.

CNIL. *1 an de RGPD : une prise de conscience inédite.* 23 05 2019. https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite (accès le 05 14, 2021).

—. *Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?* 24 09 2018. https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles (accès le 05 14, 2021).

—. *CHAPITRE I - Dispositions générales.* 25 05 2018. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1 (accès le 05 14, 2021).

—. *Chapitre III - Droits de la personne concernée.* 25 05 2018. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3 (accès le 05 14, 2021).

Farnaz Mohammadi, Angeliki Panou, Christoforos Ntantogian, Eirini Karapistoli, Emmanouil Panaousis,Christos Xenakis. «CUREX: seCUre and pRivate hEalth data eXchange.» 2019.

Gregory Epiphaniou, Herbert Daly, and Haider Al-Khateeb. «Blockchain and Healthcare.» *Blockchain and Clinical Trial*, 2019: 1-29.

Hamid Jahankhani, Stefan Kendzierskyj, Arshad Jamal, Gregory Epiphaniou, Haider Al-Khateeb. *Blockchain and Clinical Trial.* 2019. (accès le 08 09, 2021).

Javad POOL, Farhad FATEHI, Farkhondeh HASSANDOUST, Saeed AKHLAGHPOUR. «Health Data Privacy: Research Fronts, Hot.» *Studies in health technology and informatics*, 2020.

Julien Aubert, Laure de La Raudière, Jean-Michel Mis. *Rapport de la mission d'information commune sur la blockchain (chaîne de blocs) et ses usages.* 12 12 2018. https://www2.assemblee-nationale.fr/static/15/commissions/CFinances/blockchain-synthese.pdf (accès le 05 14, 2021).

Lars, Ludovic. *Blockchain publique et blockchain privée : quelles différences ?* 20 06 2018. https://cryptoast.fr/differences-blockchain-publique-blockchain-privee/#:~:text=Une%20blockchain%20priv%C3%A9e%20ou%20permissionn%C3%A9e%20

est%20un%20registre,des%20permissions%20pr%C3%A9%C3%A9tablies%20par%20une%20autorit%C3%A9%20%28preuve%20d%27autorit% (accès le 05 14, 2021).

Lorenzo Cristofaro, Rocco Panetta. «MHMD : Privacy by design and compliance assessment.» 2019.

Mirko Koscina, David Manset, Claudia Negri, Octavio Perez Kempner. «Enabling trust in healthcare data exchange with a federated blockchain-based architecture.» 2019.

Nicanor Chavez, Stefan Kendzierskyj, Hamid Jahankhani, Amin Hosseinian. «Securing Transparency and Governance of Organ Supply Chain Through Blockchain.» 18/07/20.

Pavlenkova, Ilona. «GDPR and Blockchain Solutions.» 2020.

Annexes

Annexe 1 : Health Data Privacy: Research Fronts, Hot Topics and Future Directions

Table 3. Future research opportunities in health data privacy

	Directions	Key Questions
Emerging Topics	IoT	How and why the introduction and use of IoT in healthcare can increase the risk of health data breaches? How care providers can address and mitigate the cybersecurity and privacy risks associated with the use of IoT in healthcare?
	Blockchain	How do blockchain implementations in healthcare can influence data protection practices? What are the privacy protection opportunities and risks associated with the use of blockchain in healthcare?
	Machine learning and deep learning	How do privacy rights (e.g. the right to restrict processing) can be considered in the use of machine learning and deep learning methods? How do privacy rights (e.g. the right to erasure) affect medical decision making based on these methods?
	Digital health	How can data protection be designed and included in digital health transformations and contribute to improved healthcare performance?
	Data sharing	How do care providers effectively use and implement privacy policies for data sharing in the telehealth context (i.e., GP-to-Specialist, GP-to-Nurse, Patient-to-GP)?

	Directions	Key Questions
		What are the impacts of data breaches on data sharing practices among providers and patients?
	Health services	How can general privacy frameworks (e.g., NIST) be contextually implemented in different health services (e.g., elderly home care)?
Boundary-breaking alternatives	GDPR	How do medical device manufacturers consider GDPR in their processes of designing of digital artefacts? What challenges do Data Protection Officers (DPO) face in protecting health data in practices and how can these data protection challenges be addressed?
	Artificial Intelligence (AI)	How can AI play a role in detecting unauthorized access to health data and facilitate response to health data breaches?
	5G Internet	How do privacy concerns related to health data will influence the adoption of 5G Internet in healthcare?
	Privacy protection value	How can healthcare providers plan and actualize business value from protecting patient data (e.g., innovation, agility)?
	Contact tracing apps	How can 'privacy concerns' and 'lack of data protection by design' trigger individuals' resistance to adopt and use contact tracing apps in the pandemic context such as COVID-19?

Annexe 2 : Lexique

- EMR : Enregistrement médicaux électroniques (antécédents médicaux, traitements du patient)
- EHR : Dossier de santé électronique (plus général que l'EMR, peut être partagé avec d'autres acteurs médicaux)
- IoT : Internet of Things
- HI : Healthcare Institution (sphtructure de santé)
- DLT : Distributed Ledger Technologies (technologies de registres distribués)
- PHI : Protected Health Information
- Keystore : Endroit sécurisé où sont stockées les clés cryptées
- HSM (Hardware Security Module) : boîtier matériel de chiffrement permettant de générer, stocker et protéger des clés cryptographiques.
- ADT (Asset Discovery Tool) : outil détectant tous les appareils connectés au réseau IP d'un établissement de santé (hôpital, centre de recherche, …)
- KEA (Knowledge Extraction and Analytics) : outil permettant de prédire les menaces
- VDM (Vulnerability Discovery Manager) : outil qui analyse toutes les vulnérabilités possibles qui peuvent être exploitées dans l'infrastructure.
- TIE (Threat Intelligence Engine) : outil permettant de transformer les données collectées afin de les rendre exploitable afin de mieux se protéger des cybermenaces.
- CAT (Cybersecurity Assessment Tool) : outil identifiant les menaces auxquelles l'organisme est exposé et évalue le risque causé par une grande variétés de menaces au cours d'un échange de données.
- PAT (Privacy Assessment Tool) : outil d'évaluation de la confidentialité. Il effectue une analyse des risques pour la vie privées afin de fournir les niveaux de confidentialité appropriés pour se conformer au RGPD.
- OST (Optimal Safeguards Tool) : outil majeur de la plateforme qui apporte les mesures de protection pour les organismes de santé
- PrB (Private Blockchain)
- HPA (Health professional Application) : application pour l'utilisateur final visant à aider le personnel hospitalier à échanger des informations de manière sécurisé.

- PA (Patient Application) : application final pour les patients afin d'échanger des informations de manière sécurisé.
- CVT (CUREX Visualization Tool)

Annexe 3 : Le RGPD dans les blockchains

Feature	GDPR article	Blockchain application			
		MedRec	EMRshare	FHIRchain	VerifyMed
Able to conduct information audit to demonstrate GDPR compliance	Art. 30 GDPR (Records of processing activities)	Yes	Yes	Yes	Yes
	Art. 35 GDPR (Data protection impact assessment)	N/A	N/A	N/A	N/A
Legal justification for processing health data	Art. 6 GDPR (Lawfulness of processing))	N/A	N/A	Yes	N/A
	Art. 7 GDPR (Conditions for consent)	N/A	Yes	Yes	N/A
Clear information about the data processing and legal justification in privacy policy	Art. 12 GDPR (Transparent information, communication and modalities for the exercise of the rights of the data subject)	Yes	Yes	Yes	Yes
Have a process to notify the authorities in the event of a data breach	Art. 33 GDPR (Notification of a personal data breach to the supervisory authority)	No	No	No	No
	Art. 34 GDPR (Communication of a personal data breach to the data subject)	No	No	No	No
Data protection is considered at all times, including at the beginning of developing a product	Art. 25 GDPR (Data protection by design and by default)	Yes	Yes	Yes	Yes
	Art. 5 GDPR (Principles relating to processing of personal data)	N/A	N/A	N/A	N/A
Encrypt, pseudonymize or anonymize personal data whenever possible	Art. 32 GDPR (Security of processing)	Yes	Yes	Yes	Yes
Designated person for ensuring GDPR compliance across the organization	Art. 25 GDPR (Data protection by design and by default)	No	No	No	No
Should be able to verify the patients identity.	Art. 15 GDPR (Right of access by the data subject)	Yes	Yes	Yes	No
Easy to delete personal data upon request	Art. 17 GDPR (Right to erasure/ right to be forgotten)	No	No	No	No
Easy to stop data processing upon request	Art. 18 GDPR (Right to restriction of processing)	N/A	No	N/A	No
Establish the responsibility and liability of the controller	Art. 24 GDPR (Responsibility of the controller)	No	No	No	No
Easy to receive a copy of your personal data and share with another in a simple format	Art. 20 GDPR (Right to data portability)	Yes	Yes	Yes	No

Source : (Anton Hasselgren 2020)

Annexe 4 : Le RGPD dans le Healthcare

Article in GDPR	Compliance	Impact in healthcare
Art. 30 (Records of processing activities), Art. 35 (Data protection impact assessment)	Able to conduct information audit to demonstrate GDPR compliance	HI is required to keep an up-to-date and detailed list of their processing activities using a data protection impact assessment. The list should include the purposes of the processing, what kind of data you process and who has access to it in the organization
Art. 6 (Lawfulness of processing), Art. 7 (Conditions for consent)	Legal justification for processing health data	HI can justify the purpose according to one of the six conditions. E.g Patients has given consent for the processing. Extra obligation such as the opportunity to revoke consent must be available to patients
Art. 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)	Clear information about the data processing and legal justification in privacy policy	HI is obligated to inform patients that health data is collected. HI should explain why this is collected, how it is processed, who has the access and how it is secured using clear and plain language, particularly when addressing specifically to a child.
Art. 33 (Notification of a personal data breach to the supervisory authority), Art. 34 GDPR (Communication of a personal data breach to the data subject)	Have a process to notify the authorities in the event of a data breach	HI is required to notify the supervisor authority in their jurisdiction within 72 hours learning of the health data breached or exposed. Patients should be notified without undue delay in plain language, if the breach is likely to put them at risk.
Art. 32 (Security of processing)	Encrypt, pseudonymize or anonymize personal data whenever possible	HI is to encrypt, pseudonymize or anonymize PHI whenever feasible.
Art. 25 (Data protection by design and by default), Art. 5 (Principles relating to processing of personal data)	Data protection is considered at all times, including at the beginning of developing a product	HI should implement appropriate technical (encryption) and organizational measures(deleting patients data that is no longer needed) to protect data. HI which adheres to data protection principles when processing of personal data is involved.
Art. 25 (Data protection by design and by default)	Designated person for ensuring GDPR compliance across the organization	HI should designate someone that is accountable for GDPR compliance which includes evaluation of data protection policies and the implementation of policies. HI should be able to verify the patient's identity.
Art. 15 (Right of access by the data subject)	Able to verify the patients' identity	HI is obligated to furnish patients with complete information when they request it and should be able to comply within a month. HI should be able to verify the patient's identity.
Art. 17 (Right to erasure/ right to be forgotten)	Easy to delete personal data upon request	Patients should have the right to request to delete all health data and HI should honour their request within a month. HI may have grounds to deny the request such as compliance with a legal obligation. HI should be able to verify the patient's identity.
Art. 18 (Right to restriction of processing)	Easy to stop data processing upon request	Patients can request HI to restrict or stop processing their health data if certain grounds apply, such as dispute about the lawfulness of the processing. HI may be allowed to keep storing their data although the processing is restricted.
Art. 24 (Responsibility of the controller)	Establish the responsibility and liability of the controller	Any processing of personal data carried out by HI or on HIs behalf, responsibilities should be established which includes implementing appropriate technical and organisational measures. This is to ensure and to be able to demonstrate that processing is performed lawfully
Art. 20 (Right to data portability)	Easy to receive a copy of your personal data and share with another in a simple format	From a privacy standpoint, GDPR offers higher patients autonomy over their data, instead of HI. This means patients should be able to receive health data in a readable format or share with other HI.

Source : (Anton Hasselgren 2020)

Annexe 5 : MHMD Privacy by design and compliance assessment

RIGHT	CONSEQUENT AUTOMATED ACTION
Access **(obtaining confirmation as to whether or not personal data concerning the data subject are being processed and, in case, access to such data and to all relevant information regarding the processing)**	A transaction is registered on the blockchain which indicates that access was requested for a specific data item. The extraction and delivery of the data will then take place off-chain (under the responsibility of the competent controller).
Rectification **(obtaining without undue delay the rectification of inaccurate personal data)**	A specific smart contract is activated in order to prevent any party to the Project, including particularly the Stakeholder, to access the inaccurate data, while allowing to collect and process only the amended Datasets.
Erasure **(obtaining from the controller, when certain conditions laid down by Art. 17 of the GDPR are met, the erasure of personal data concerning him or her without undue delay)**	The right to erasure is achieved by 'breaking the link', *i.e.* deleting the entries, in the Local mapping DB, so preventing anyone from being able to associate a data source identifier and the relevant blockchain identifier. As a result of this, a smart contract will forbid anyone from accessing the data on the Platform, thus guaranteeing a result whose effects are reasonably completely equivalent to those of material cancellation (which will obviously will be carried out off-chain with no delay, insofar at least one of the conditions set forth by Art. 17.1 is satisfied)
Restriction of processing	Where the processing is restricted in the cases set out by Art. 18.1, a specific smart contract will be executed to

(obtaining from the controller restriction of processing, meaning that the personal data shall, with the exception of storage, only be processed, *inter alia*, with the data subject's consent or for the establishment, exercise or defense of legal claims)	prevent all Stakeholders from carrying out any kind of processing, with the exception of storage, unless (i) the data subject has given his/her consent, or (ii) for the establishment, exercise or defence of legal claims.
Notification **(the controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it)**	The measures described above in regards of the request of rectification or erasure of personal data, or restriction of processing, ensure that the relevant legal effects are appropriately extended to any user of MHMD blockchain, thus meeting notification requirement which, however, shall apply only where this does not prove impossible or does not involve a disproportionate effort.
Portability **(receiving the personal data provided to the controller in a structured, commonly used and machine-readable format and, where requested, having such data directly transmitted to another controller)**	The same actions described above in regards of the right of access shall apply, mutatis mutandis, to the requests of portability. The duty to provide the data subject with the data in a structured, commonly used and machine-readable format lies exclusively with the controller (namely the Hospital for Clinical Data, or the Platform Operator for Individual data).

Withdrawal of consent **(revoking the consent(s) at any time, bearing in mind that it shall be as easy to withdraw as to give consent)**	At any time a Patient or User should withdraw one or more of the consents previously provided – as repeatedly explained above in detail – a smart contract will be run to definitively (at least until the data subjects provides the consent again) prevent Stakeholders from accessing the associated Datasets for purposes which do not meet the applicable usage requirements.
Automated decision-making process **(not being subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the data subjects, unless this processing is based on his/her specific consent and provided that suitable measures to safeguard the data subject's rights and freedoms are in place, with**	In no case the automated processing operations carried out through the Platform, as operationalized by both the blockchain and the associated smart contracts, may determine or result in a decision which produces legal effects for the data subjects, or which may in any case significantly affect them.
particular regard to the right to obtain human intervention, or to express the individual's point of view and to contest the decision)	Any such decision can be taken and is therefore exclusively left to the Stakeholders, without any chance that the Platform Operator carries out any fully automated individual decision-making as governed by Art. 22 of the GDPR.

Source : (Lorenzo Cristofaro 2019)

Annexe 6 : Arbre décisionnel Blockchain

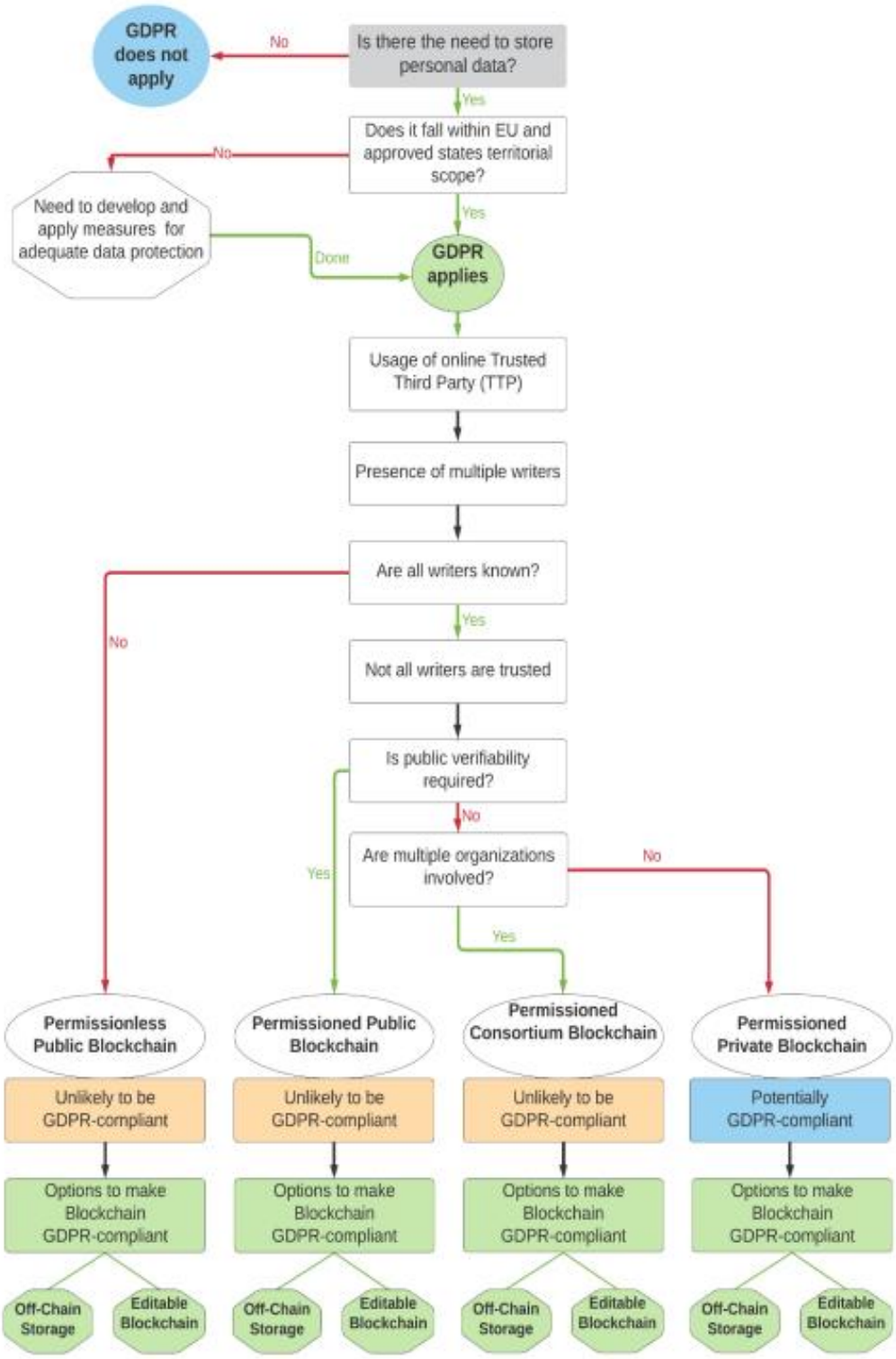

Figure 10 : Arbre décisionnel (Pavlenkova 2020)