Gramchain : améliorer les protocoles de suivi des patients porteurs de BHRe en utilisant la blockchain

Gramchain : improve the follow-up protocols for patients with eHRB bacteria using blockchain

Doriane PERARD[1]

[1] Innovacs, Université Grenoble Alpes, Grenoble, France, doriane.perard@univ-grenoble-alpes.fr

RÉSUMÉ. Les bactéries hautement résistantes émergentes (BHRe) réprésentent une menaces importantes à l'échelle internationale. Actuellement, le statut de porteur de BHRe n'est pas partagé automatiquement entre les différents établissements de santé. Le patient n'est alors pas correctement traité et les précautions d'hygiène appliquées ne sont pas suffisantes, pouvant entraîner des épidémies. Plusieurs projets, internes aux hôpitaux ou étatiques, ont vu le jour pour proposer un accès simplifié à cette information et limiter le risque de contamination. Mais ils comportent des problèmes limitant leurs impacts : non interopérabilité, données insuffisamment sécurisées, non respect des différents règlements sur la protection des données... Cet article présente Gramchain, un outil permettant d'améliorer les protocoles de suivi des patients porteurs de BHRe en utilisant une blockchain à permission. Cette solution, conçue en privacy by design, est conforme au RGPD. Le patient joue un rôle majeur dans le partage de ses données, grâce à un contrôle d'accès à granularité fine se faisant avec son autorisation.

ABSTRACT. Emerging highly resistant bacteria are a major international threat. Currently, the status of a carrier is not automatically shared between different health care institutions. The patient is then not properly treated, and the hygiene precautions applied are not sufficient, which can lead to epidemics. Several projects, both internal to hospitals and state-run, have been developed to provide simplified access to this information and limit the risk of contamination. But they have problems that limit their impact : non-interoperability, insufficiently secure data, non-compliance with various regulations on data protection, etc. This article presents Gramchain, a tool to improve the monitoring protocols of patients with BHRe by using a permssion blockchain. This solution, designed in privacy by design, is GDPR compliant. The patients play a major role in the sharing of their data, thanks to a fine-grained access control with his authorization.

MOTS-CLÉS. BHRe, blockchain, RGPD, patient souverain, données de santé.

KEYWORDS. HRB, blockchain, GDPR, sovereign patient, medical data.

Introduction

Les bactéries hautement résistantes émergentes (BHRe) constituent un problème international majeur de santé publique [1]. Elles sont de plus en plus présentes à travers le monde, alors que le développement de nouvelles molécules antibiotiques stagne, ce qui peut conduire à un risque d'impasse thérapeutique.

Quelques projets de traçabilité des patients atteints de BHRe sont apparus à l'échelle locale. Par exemple, certains pays ont rendu obligatoire la déclaration des incidents liés à ce type de bactérie. Pourtant, les informations sur le statut du patient en tant que porteur ne sont pas suffisamment accessibles, et la méconnaissance de ces informations a des conséquences :

— Sur le plan strictement sanitaire, le patient n'est pas traité correctement, pouvant entrainer des conséquences directes graves sur sa santé. Les précautions d'hygiène prises ne sont pas suffisantes, amenant à des contaminations et un risque de transmission croisée.

— Sur le plan de la recherche scientifique, il existe très peu de données précises sur les BHRe. Des données existent pour certains pays [2], ou pour l'Europe [3], mais pas à l'échelle mondiale.

Plusieurs groupes de travail plaident pour sauvegarder et partager ces informations de manière fiable et rapide [4]. Il en ressort que le stockage doit se faire sur le long terme, car un porteur de BRHe l'est

pour une très longue période, voir à vie. Le partage doit être réparti sur tous les différents acteurs pour assurer la disponibilité de l'information. Enfin, comme il s'agit de données de santé, la solution doit être conforme aux différentes réglementations.

Cet article décrit notre proposition de solution technologique utilisant une *blockchain* privée pour résoudre le stockage et le partage des données entre les institutions de santé.

Notre solution conserve toutes les données dans un outil unique : Gramchain. Les données sont numérisées et moins éparpillées, ce qui permet d'avoir une vision plus précise de la présence ou de l'absence de patients atteints de BHRe au sein d'un établissement, mais aussi à plus grande échelle. Grâce à la *blockchain*, les données sont chainées par des procédés cryptographiques. Il est alors impossible de modifier le contenu d'un enregistrement antérieur. Cette propriété d'immuabilité renforce l'intégrité du système, et est essentielle dans les systèmes d'information médicaux. Grâce à la cryptographie asymétrique, les *blockchains* proposent nativement un mécanisme d'authentification permettant de savoir qui est l'auteur d'une donnée.

La *blockchain* est conçue de manière résiliente, la chaine d'enregistrement des événements est répliquée sur tous les nœuds du système, c'est-à-dire tous les établissements de santé participant au projet. La disponibilité des données est proportionnellement augmentée par le nombre d'acteurs dans le réseau. Le choix d'une blockchain privée se justifie par le fait que seuls des établissements partenaires ont une place légitime dans le système. Chaque hôpital participant à Gramchain stocke la chaine, donc toutes les données de façon chiffrée. Lorsqu'un patient porteur de BHRe se présente dans l'établissement de santé, il fournit des informations à l'établissement afin de permettre à l'équipe médicale d'accéder à ses données.

L'accès aux données doit être géré à une échelle fine, pour respecter la confidentialité des données médicales et placer le patient au coeur du système. Les transactions, contenant les données liées aux BHRe, sont stockées sous forme chiffrée, protégées par un système de gestion des clés. Une clé maitresse secrète est détenue par le patient. Il génère à partir de celle-ci une clé dérivée. En fournissant cette clé, il choisit d'autoriser spécifiquement un établissement de santé à accéder à certaines données précises. Il est reste ainsi maître de ses données.

Afin d'être compatible avec les différentes réglementations sur la protection des données, le projet est mené selon le principe du *Privacy by Design*. Cela se traduit par la prise en compte de la protection des données dès la conception de la solution technique. L'objectif à court terme du projet est d'être utilisé en France, puis en Europe. Un effort particulier a été fait pour respecter le règlement général sur la protection des données (RGPD). Des consultations avec la Commission Nationale de l'Informatique et des Libertés (CNIL) [5] sont menées pour obtenir leur validation à tous les niveaux.

Ce document est organisé de la façon suivante : dans la première partie nous fournissons un état de l'art sur les BHRe, les bases de données BHRe existantes, les *blockchains* ainsi que les fonctions de dérivation de clés cryptographiques. La proposition de Gramchain est présentée dans la section 2 et les détails quant à son fonctionnement dans la section 3 Dans la section 4, nous présentons l'intérêt de la solution Gramchain puis nous discutons en section 5 des points restant à développer et des ouvertures. L'article se termine par une conclusion dans la section 6

1. État de l'art

1.1. *Bactéries hautement résistantes émergentes (BHRe)*

La résistance aux antibiotiques est l'une des plus grandes menaces auxquelles l'humanité devra faire face dans les deux prochaines décennies. Selon The Lancet [1], en 2019, 1 270 000 décès dans le monde étaient attribuables à la résistance aux antimicrobiens, soit autant que le sida et le paludisme réunis.

Les bactéries hautement résistantes émergentes (BHRe) sont un type de résistance aux antibiotiques, déjà classé comme un problème majeur de santé publique. Cette résistance correspond à l'acquisition par les bactéries de la capacité à neutraliser les agents chimiques des antibiotiques agissant contre la croissance des colonies bactériennes. Le gène de résistance peut ensuite être transmis aux autres bactéries présentes. Selon [6], les BHRe pourraient entraîner plus de dix millions de décès chaque année en 2050. En France, la déclaration obligatoire des épisodes d'infection liés aux BHRe à l'agence régionale de santé permet d'avoir une vision assez réaliste de la situation. Le nombre de nouveaux cas augmente chaque année de manière exponentielle, avec 2500 nouveaux patients porteurs en 2019 [2]. Bien qu'un biais de déclaration ne puisse être exclu, l'augmentation des épisodes déclarés au cours des trois dernières années est évidente.

Lors de l'utilisation d'un antibiotique sur un patient porteur de BHRe, les bactéries normales sont détruites, et seules les bactéries résistantes demeurent. La proportionnalité de BHRe augmente alors considérablement. Pour éviter cette situation, il est important de connaître le statut de porteur du patient. Bien que de nombreuses recherches médicales soient en cours dans ce domaine, l'utilisation et le développement des antibiotiques se poursuivent, et de nouvelles bactéries résistantes apparaissent. L'émergence de la résistance soulève le risque d'une impasse thérapeutique et d'une pandémie mondiale [7]. Une solution efficace pour contenir l'épidémie est de limiter la transmission croisée des sources d'infection connues et inconnues pendant les soins. Ces dispositions permettent de protéger les patients ainsi que le personnel médical. Une piste d'amélioration consiste à renforcer la traçabilité des patients porteurs de ces bactéries. La surveillance reste un axe majeur de la prise en charge des maladies infectieuses, pourtant elle a été jusqu'à récemment, souvent ignorée dans la lutte contre les BHRe.

En France, 40% des cas sont directement liés à un voyage à l'étranger [2]. Ce pourcentage a pu être sous-estimé compte tenu du nombre d'épisodes pour lesquels les détails ne sont pas disponibles. A plus grande échelle, dans le rapport annuel 2019 sur la résistance aux antimicrobiens en Europe [3], le Centre européen de prévention et de contrôle des maladies note "Une évolution particulièrement préoccupante a été l'augmentation du pourcentage d'isolats d'E. faecium résistants à la vancomycine dans l'UE/EEE, passant de 10,5% en 2015 à 18,3% en 2019 [...] aucun schéma géographique distinct n'était évident.". La traçabilité des patients porteurs doit se faire non seulement entre établissements de santé d'un même pays, mais à plus grande échelle, européenne et mondiale.

1.2. *Base de données BHRe existantes*

Les données concernant les patients porteurs ou contacts de BHRe sont collectées de façon variable en fonction des établissements. Au sein des hôpitaux, la gestion des BHRe est à la charge des équipes opérationnelles d'hygiène, composées d'infirmiers et de médecins, spécialisés dans la lutte et la prévention des épidémies au sein de l'hôpital. Les équipes médicales possèdent de nombreuses données sur

les BHRe, sous différentes formes : documents Excel, documents papier, logiciels internes, documents détenus par les patients...

Les outils permettant leur enregistrement sont souvent développés en interne, sans prendre en compte les aspects de fiabilité, de sécurité et d'interopérabilité. En conséquence, il n'existe pas de véritable système de partage des informations entre les établissements et les demandes sont traitées manuellement, ce qui nécessite du temps et du personnel. Ponctuellement, dans certaines situations précises et avec l'accord des médecins concernés par le patient, les données peuvent être transférées entre deux établissements. Mais cet échange pose des problèmes concernant la confidentialité et la sécurité du transfert, souvent réalisé par mail.

Cette hétérogénéité présente de nombreux inconvénients. Tout d'abord, les données sont la plupart du temps stockées en clair (c'est-à-dire non chiffrées) dans le système d'information. Elles peuvent être lues par toute personne ayant accès au réseau de l'hôpital. Ceci est incompatible avec le respect du RGPD.

Il n'y a aucun contrôle sur l'intégrité des données qui peuvent être modifiées ou supprimées sans garantie, car les tableurs, les logiciels non professionnels et les documents papier ne disposent pas de protection par défaut. Cette absence de contrôle est problématique car l'intégrité des données est un point essentiel au bon fonctionnement d'un système d'information de santé.

Les données sont éparpillées, tant sous forme numérique que physique. Comme elles ne sont pas répliquées, leur disponibilité dépend entièrement de l'hôpital qui les possède. Elles sont sensibles à la perte physique pour les documents papier et à la perte numérique pour les informations numériques, par exemple en cas d'incendie ou d'attaque par *ransomware*.

Au niveau national, le signalement sur e-sin [1] est obligatoire et permet de collecter un certain nombre d'informations relatives aux patients identifiés BHRe. Mais les données des patients sont anonymisées, ce qui ne permet pas de suivi individuel. C'est en effet un outil de santé publique qui sert de support épidémiologique dans la constitution de statistiques.

Dans ces conditions, il semble difficile d'imaginer la mise en œuvre d'un partage efficace de l'information, alors qu'il s'agit d'une des solutions les plus pertinentes pour limiter le risque d'épidémies. Le Haut Conseil de la Santé Publique [4] insiste sur le fait qu'une communication entre établissements de santé est indispensable et non discutable. L'information concernant le statut d'un patient porteur de BHRe doit être indiquée dans le dossier médical partagé, dès qu'elle est disponible.

En France, les précautions lors de l'admission d'un nouveau patient sont insuffisantes car l'information sur le statut de porteur de la bactérie BHRe est inconnue. 48% des admissions de patients porteurs se font avec des précautions standards, qui sont insuffisantes [2]. Le risque de transmission croisée est donc important.

1.3. *Blockchain*

Le concept de *blockchain* est introduit en 2008 par Nakamoto Satoshi [8]. Une *blockchain* est une séquence de blocs de taille variable stockés dans un grand livre distribué, lui-même répliqué sur l'ensemble

1. https ://esin.santepubliquefrance.fr/appli_esin

des participants, appelés nœuds. Ceux-ci interagissent avec le réseau, en *peer-to-peer* pour ajouter des événements à la *blockchain*, sans autorité centrale.

Un registre de la *blockchain* se présente sous la forme de blocs contenant les transactions soumises par les utilisateurs. Chaque bloc est chaine au précédent par le stockage dans le bloc courant, d'une signature d'intégrité du bloc précédant (*hash*), d'où le terme *blockchain*.

La *blockchain* assure la sécurité et la confidentialité des données stockées selon différents critères [9]. Les blocs sont chaines entre eux ce qui permet de rendre la chaine immuable. L'ajout, la suppression ou la modification du contenu d'un ancien bloc est tout simplement impossible. Chaque nœud participant stocke les anciens blocs, écoute les nouveaux blocs annoncés et vérifie l'intégrité de la chaine.

Chaque nœud du système possède sa propre copie, identique à celle des autres, ce qui augmente la disponibilité et la résilience. En cas de panne ou de perte de ses données, il les récupère en les téléchargeant depuis les autres nœuds du système. Les données relatives BHRe sont des données valables à long terme, car un patient est porteur à vie. Chaque hôpital dispose de toutes les données BHRe chiffrées et participe à l'effort de réplication.

Il existe deux grandes familles de *blockchains* : les *blockchains* sans permission et les *blockchains* avec permissions.

Les *blockchains* publiques sont sans permission, c'est-à-dire que n'importe quel noeud peut rejoindre le réseau pour lire et/ou écrire des transactions. Elles sont donc ouvertes et décentralisées, ce qui signifie qu'aucune autorité centrale ne contrôle le réseau. Les *blockchains* publiques sont conçues pour être ouvertes et accessibles à tous. Elles sont donc bien adaptées aux applications qui exigent transparence et confiance, comme les applications décentralisées.

Les *blockchains* privées sont basées sur des autorisations, ce qui signifie que seul un nombre limité de nœuds peut accéder à la chaine, en écrivant ou en lisant des transactions. Les participants doivent être validés et autorisés par un ou plusieurs pairs avant de rejoindre le réseau. Les *blockchains* privées sont plus centralisées, car tout nouveau participant doit être validé, de sorte que certains nœuds disposent de ce droit supplémentaire. Elles offrent plusieurs avantages par rapport aux réseaux publics, notamment l'augmentation de la sécurité et de la confidentialité, un meilleur contrôle du participant, des transactions plus rapides, des coûts de transaction plus faibles et un passage à l'échelle plus efficace.

Ces deux types de *blockchains* ont donc chacun leurs spécificités avec des avantages et des inconvénients, et le choix ne doit pas être pris à la légère. Bitcoin et Ethereum sont des exemples de *blockchains* publiques, tandis que Hyperledger Fabric, R3 Corda et Quorum sont des exemples de *blockchains* privées.

Dans [10], les auteurs proposent une méthode pour déterminer le meilleur choix entre les cinq principales blockchains, selon différents critères. Dans [11], les auteurs établissent une méthode d'aide à la décision sur le choix de la technologie : sans blockchain, avec une *blockchain* sans permission ou avec une *blockchain* avec permissions.

1.4. *Blockchain dans les applications médicales*

La recherche de cas d'usage des *blockchains* est un sujet d'actualité, de nombreux travaux ont été réalisés sur son utilisation avec des applications médicales. Selon [12], les avantages de l'utilisation des

blockchains dans un contexte médical sont en faveur du patient, qui est placé au cœur du système, avec des soins plus appropriés grâce au partage et à la réplication des informations. Concernant les points bloquants, un effort est nécessaire pour respecter la réglementation (RGPD), et certains risques existent concernant l'interopérabilité et l'acceptation de cette nouvelle technologie à grande échelle.

Dans [13], les auteurs utilisent une *blockchain* pour collecter des données microbiennes en raison de la rareté des données et de la nécessité de traçabilité pour l'évaluation ou la médecine légale. Dans [14], les auteurs proposent une étude de preuve de concept pour la *blockchain* HealthChain afin de renforcer l'engagement des patients et la conservation des données dans un environnement sécurisé et interopérable. Une revue systématique menée par [15] montre l'intérêt, les comparaisons entre les solutions et les orientations des dossiers médicaux personnels basés sur les *blockchains*. Dans [16], les auteurs attestent que la *blockchain* peut être utilisée pour identifier les problèmes de sécurité sanitaire, analyser les mesures préventives et faciliter le processus de décision pour agir rapidement. Dans [17], les auteurs se concentrent sur les principales limites d'une solution de dossiers médicaux centralisés comme celle de la France, et comment une solution basée sur la *blockchain* peut les éviter.

De nombreux projets mêlant *blockchain* et données de santé émergent, dans le but de mettre le patient au centre du système et de fournir de meilleurs soins. La plupart d'entre eux sont confrontés à des problèmes de compatibilité et d'évolutivité avec le RGPD, ainsi qu'à l'hétérogénéité excessive des données stockées.

1.5. *Cryptographic key derivation functions*

Pour assurer une confidentialité avec une granularité fine, il peut intéressant d'autoriser la lecture de chaque jeu de donnée de façon indépendante.

Pour cela, la solution optimale serait de chiffrer chaque nouvelle donnée avec une clé unique et aléatoire. L'entité qui souhaite accéder à des données particulières recevrait la clé associée. Les clés aléatoires sont intéressantes car il n'existe pas de processus de calcul permettant de deviner une valeur aléatoire : l'unique solution est de tester toutes les valeurs possibles jusqu'à obtenir la bonne. Pour des valeurs aléatoires suffisamment grandes, il devient alors impossible de deviner la clé dans un temps acceptable. Le problème avec cette solution est de générer une demande de création d'une nouvelle clé pour chaque nouvelle transaction, et de stocker toutes les clés sur le portefeuille du patient et le cloud externe.

Une autre solution consiste à utiliser une clé dérivée, calculée à l'aide d'une "fonction de dérivation de clé" (*cryptographic key derivation functions*, KDF) sécurisée.

Une fonction de dérivation de clés permet de dériver une clé K' à partir d'une clé K et d'un identifiant non secret. La connaissance de K permet de dériver K', mais la connaissance de K' ne permet pas de retrouver K. Ce mécanisme permet de dériver plusieurs clés à partir d'un même secret initial pour différents usages. Le principal avantage des clés uniques dérivées par transaction est que si une clé dérivée est compromise, les données des transactions futures et passées sont toujours protégées [18, 19]. Ils rendent beaucoup moins coûteux l'achat, l'utilisation et la maintenance des systèmes qui les emploient.

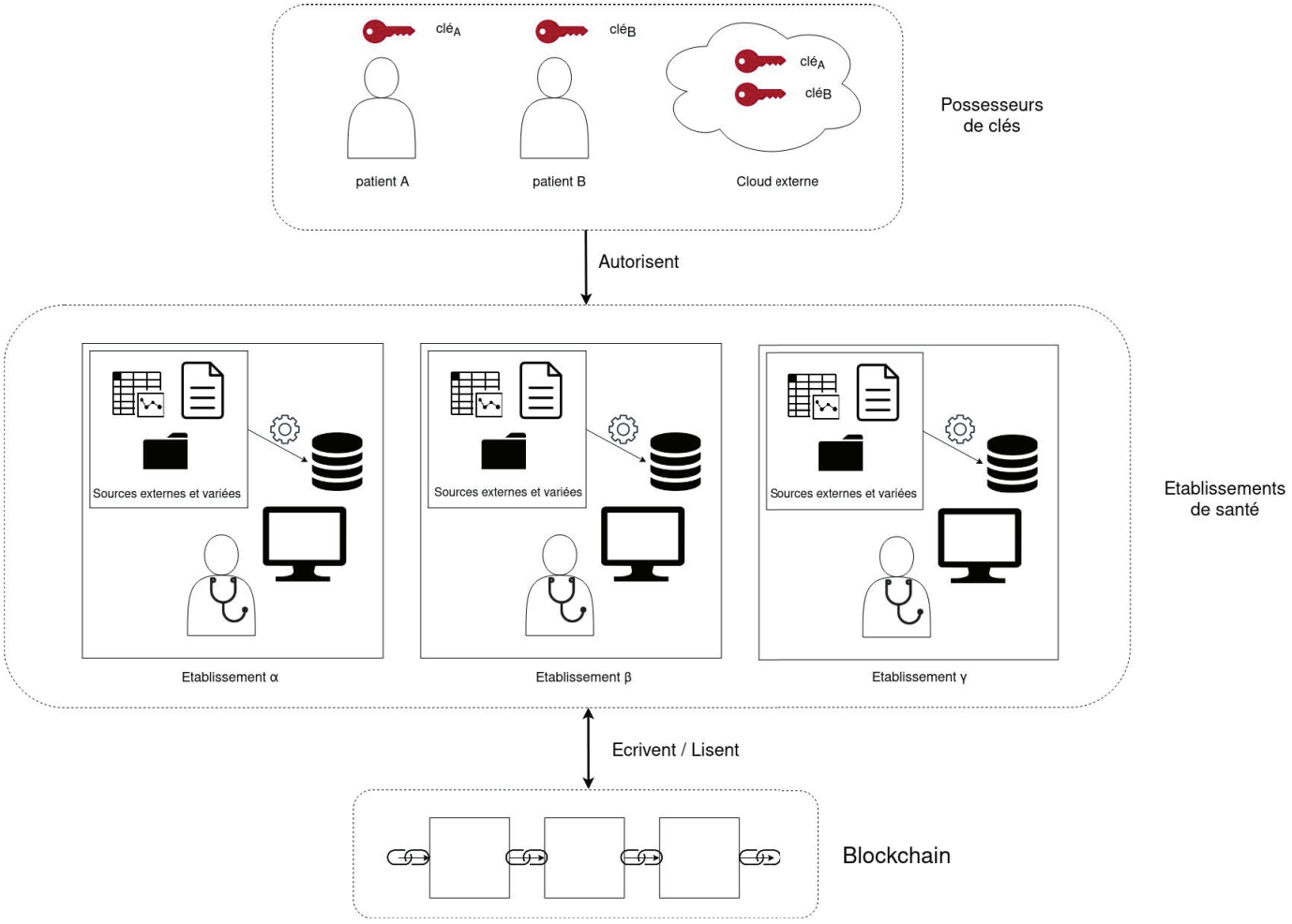

FIGURE 1. *Vue haut niveau de la solution*

Il existe de nombreuses propositions de KDF, avec une ou plusieurs phases. Pour en choisir une, des guides proposent des états de l'art sur les algorithmes recommandés et dépréciés à utiliser [19]. Les détails et caractéristiques exacts dépendent du KDF choisi, mais le fonctionnement général est le suivant :

Soit D un identifiant public, soit S un secret, la clé dérivée k est calculée par : $K' = KDF(D||S)$.

2. Description générale de Gramchain

Notre proposition, Gramchain, a pour but de faciliter la communication de données liées aux BHRe entre les établissements de santé. Dans cette section nous présentons les différents acteurs de Gramchain, qui sont représentés sur la figure 1. Ils peuvent être séparés selon trois grands rôles :

— Les patients et le serveur externe, qui autorisent l'accès aux données grâce à la cryptographie.
— Les établissements de santé, qui utilisent et génèrent les données médicales.
— La blockchain, qui est la technologie sur laquelle repose Gramchain, et stockée sur les serveurs des établissements de santé.

2.1. *Les patients*

Dans cet article, un patient est une personne qui se rend dans un établissement de santé participant au projet, et va être déclarée porteur d'une BHRe après avoir subi des examens médicaux. Il lui est alors

proposé de s'inscrire et rejoindre Gramchain, pour un partage plus efficace de ses informations liées à sa BHRe.

Une fois que celui-ci accepte, il reçoit un portefeuille électronique permettant de gérer les accès à ses données. Lorsqu'il se rend dans un hopital pour des examens, il peut donc choisir d'autoriser le personne de santé à lire les informations qu'ils jugeront pertinentes. Ce système de droit d'accès contrôlé par le patient lui rend la propriété et la maitrise de ses données, et augmente son implication dans son parcours de santé.

2.2. *Le serveur externe*

Parallèlement aux patients, le serveur externe a également un rôle lui permettant d'autoriser la lecture et l'écriture d'informations sur les patients.

Le but est de permettre à l'équipe médical d'accéder aux données de santé du patient dans une situation où ce dernier n'est pas en mesure de l'autoriser lui-même. Cette procédure est appelée "bris de glace" et est particulièrement utile en cas d'urgence où le patient est inconscient ou ne dispose pas de son portefeuille électronique sur lui.

De plus, si le patient ne possède plus son portefeuille électronique, en cas de vol ou de perte par exemple, il ne peut plus autoriser l'accès aux données, qui deviennent alors illisibles et perdues. En disposant de ce serveur de secours, il peut le régénérer.

Comme le serveur externe permet la récupération des données de santé, il doit présenter un haut niveau de sécurité, et en Francec doit être certifié "hébergeur de données de santé". Il pourrait être hebergé par un acteur privé ou public. L'espace de santé numérique [2] proposée en France depuis 2022 pourrait remplir ce rôle.

Malgré les avantages énoncés au dessus, le fait de doter un autre acteur du droit à disposer des données diminue la capacité du patient à être maître de ses données. Son utilisation peut donc ne pas systématique, et être à la discrétion du patient concerné. Ce sujet est abordé plus en détail dans la sous section 5.1.

2.3. *Les établissements de santé*

Les établissements médicaux partenaires sont des hopitaux, des cliniques, des cabinets de professionnels de santé,... qui procèdent à des soins liés directement ou indirectement aux BHRe. Pour éviter des contaminations patients-patients ou patients-soignants et pour améliorer la qualité des soins, il est important que le personnel ait accès au statut de porteur du patient, ainsi qu'à un certain nombre de détails.

Les établissements décidant de rejoindre Gramchain ont un rôle de noeud *blockchain*. Ils stockent en conséquence une copie de la chaine, contenant les données de l'ensemble des acteurs du réseau. Lorsqu'un patient porteur de BHRe se rend dans un des établissements, son équipe médicale accède à ses données avec son autorisation. Ces établissements peuvent également écrire dans la *blockchain* de nouvelles informations sur le patient et la BHRe, pour maintenir le dossier à jour.

2. https ://www.monespacesante.fr

2.4. *La blockchain*

Le fonctionnement des blockchains a été expliqué dans la section 1.3 Contrairement à une architecture serveur-clients, dans un tel réseau chaque nœud participant maintient en permanence sa propre copie de la chaine et la vérifie sans accorder de confiance aux autres. La solution Gramchain vise à interconnecter les établissements de santé à travers l'Europe et même le monde, cette propriété de décentralisation est donc particulièrement intéressante.

De plus, comme chaque nœud du système possède sa propre copie, identique à celle des autres, la disponibilité est augmentée. Chaque hôpital dispose de toutes les données BHRe et participe à l'effort de réplication. En cas de panne ou de perte de ses données, il les récupère en les téléchargeant depuis les autres nœuds du système. Les données relatives aux BHRe sont des données valables à long terme, car un patient est porteur pendant une longue durée. Il est intéressant de conserver toutes les données depuis son premier examen, pour pouvoir disposer d'une vision globale de l'évolution de sa maladie mais également pour à des fins statistiques ou pour alimenter la recherche autour de cette thématique. Cependant, ces données étant de nature sensible, leur accès doit être suffisamment protégé pour respecter le secret médical et être conforme aux différentes réglementations en vigueur, comme le RGPD. Un travail a donc été mené sur les autorisations d'accès, en utilisant un système de clés cryptographiques expliqué en 3.2.1

Dans [10], les auteurs proposent une méthode pour déterminer le meilleur choix entre les cinq principales *blockchains* différentes, selon différents critères. Dans [11], les auteurs établissent une méthode d'aide à la décision sur le choix de la technologie : sans blockchain, avec une *blockchain* sans permission ou avec une *blockchain* avec permissions.

Dans le projet Gramchain, les acteurs du système sont connus et en nombre limité, puisqu'il s'agit des établissements de santé partenaires. Cette chaine n'a pas à être vérifiable publiquement. Nous avons également besoin d'un système évolutif pour avoir une faible latence, une faible puissance de calcul requise et un faible coût par transaction. Notre choix penche pour une *blockchain* à permission, et les deux articles cités dans l'état de l'art [10, 11] confirment cette décision.

Afin de déterminer quelle blockchain privée utiliser, nous avons lu les différents *white papers* et les avons manipulées localement sur un ordinateur afin de déterminer celle qui semble la plus appropriée pour notre projet. Quorum a été écartée pour des raisons de licence, car elle n'est pas assez permissive. Corda et Hyperledger ont des licences identiques qui conviennent, et les deux tests local se sont avérés concluant. Notre choix final s'est porté sur Hyperledger, qui dispose d'une communauté forte et d'un financement solide, ce qui semble être une solution plus durable.

3. Fonctionnement détaillé de Gramchain

3.1. *Scénario*

Afin d'expliquer le plus clairement possible le fonctionnement de Gramchain, prenons un exemple réaliste. Un patient, nommé Bob, a besoin de consulter un professionnel de santé et se rend à l'hôpital de Pontoise. Lors d'examens, Bob est diagnostiqué comme porteur d'une BHRe et décide de rejoindre le programme de Gramchain pour faciliter le partage de ses informations médicales pour ses prochaines futures consultations. Il fournit les renseignements nécessaires ainsi que son accord à l'équipe

opérationnelle d'hygiène de Pontoise, qui réalise la procédure d'enregistrement de Bob. Ces étapes sont expliqués dans la sous-section 3.2 A l'issu de son enregistrement, Bob reçoit un portefeuille électronique lui permettant d'autoriser l'accès à ses données.

Une fois que Bob est enregistré, il devient alors possible pour les établissements de santé partenaires d'inscrire dans Gramchain les données de santé jugées utiles, avec l'accord de Bob. L'hôpital de Pontoise y écrit dans la chaine les détails des résultats positifs des examens de détection de la BHRe de Bob. La procédure d'écriture est détaillée dans la sous-section 3.3

Dans le futur, Bob doit réaliser de nouveau examen et se rend cette fois-ci au CHU de Grenoble. Pour mettre en place des précautions d'hygiène suffisantes et adapter les soins, l'équipe médicale souhaite obtenir les informations des précédents examens. Bob donne son accord et rend possible la lecture des données souhaitées. Ces dernières sont stockées dans la chaine, qui est répliquée sur tous les acteurs du réseau donc entre autre sur les serveurs de l'hôpital. La lecture depuis la blockchain est expliquée dans la sous-section 3.4.1

Bob se retrouve aux services des Urgences, dans un état physique ou mental ne lui permettant pas d'autoriser lui-même l'équipe médicale à accéder à ses données. Bob ayant donné son consentement préalable relatif à cette situation d'urgence, les praticiens peuvent se passer de son autorisation et contacter directement le serveur externe. Celui-ci leur permet de réaliser une procédure "bris de glace" et d'accéder aux données. La sous-section 3.4.2 présente cette procédure.

3.2. *Enregistrement dans le système d'un nouveau patient porteur d'une BHRe*

3.2.1. Clés cryptographiques

Lorsqu'un patient est testé sur sa contamination à une BHRe pour la première fois, l'hôpital émet une demande de création d'une clé maitresse secrète cryptographique pour le patient concerné. Cette procédure est expliquée dans la figure 2.

L'accès aux données du patient doit être limité et contrôlé autant que possible pour garantir la confidentialité et respecter la vie privée du patient. Cette limitation permet également d'être cohérent avec les principes du RGPD, comme précisé dans la section 4.3

Lorsqu'un hôpital souhaite chiffrer des données, il génère l'identifiant D. Il l'envoie à l'application mettant en œuvre le KDF, sur le dispositif du patient ou du serveur cloud externe. L'application calcule la clé K' comme $K' = KDF(D||S)$, et renvoie la valeur K', la clé dérivée, à l'établissement ayant effectué la demande, avec une date de validité. Ce mécanisme permet à l'hôpital d'écrire sur la *blockchain* pendant une période limitée, correspondant à l'hospitalisation. Mais il ne peut pas accéder aux autres données du patient et n'a pas besoin de demander la clé du patient pour chaque nouvelle écriture durant son hospitalisation. Lorsque la date de validité est atteinte, l'hôpital détruit sa copie de la clé dérivée.

L'identifiant doit être public et unique pour chaque nouvel enregistrement du patient. Il est par exemple possible d'utiliser une combinaison de l'identifiant unique de l'hôpital sur la *blockchain* et du numéro de consultation du patient, ou toute autre information pouvant être facilement générée et récupérée. Cette dernière propriété est particulièrement intéressante, car cet identifiant sera à nouveau utilisé à l'avenir pour régénérer la clé dérivée et lire les anciennes données. Ces identifiants peuvent être stockés dans le portefeuille du patient et dans le cloud externe, afin d'être sûr de les retrouver à l'avenir.

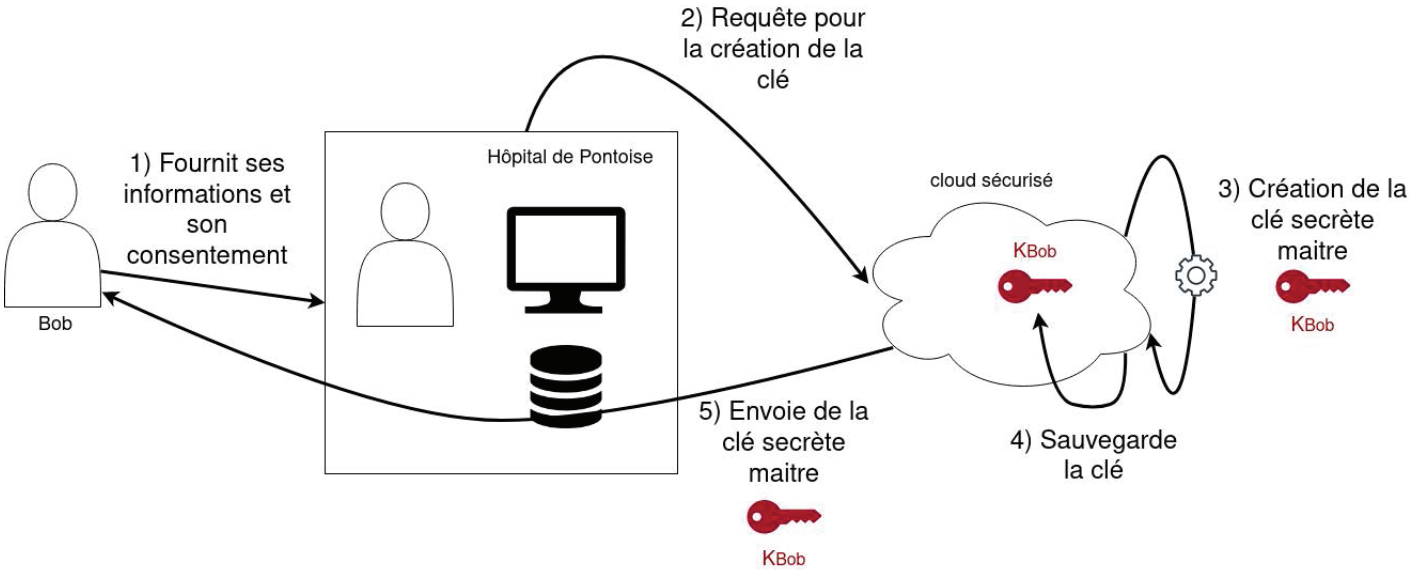

FIGURE 2. *Procédure de génération de la clé maitresse secrète du patient Bob*

Dans les différents schémas, les clés maitresses secrètes sont en rouge et les clés dérivées en vert.

3.2.2. Protocole

Les clés maitresses secrètes sont créées la première fois qu'un patient est confronté à un examen positif lié aux BHRe. Elles sont créées sur un logiciel spécifique fonctionnant sur le serveur externe, à la demande d'un établissement de santé.

La procédure est expliquée dans la figure 2.

Bob se rend à l'hôpital de Pontoise pour passer des examens médicaux. Au cours de ceux-ci, Bob est diagnostiqué comme porteur d'une BHRe. Il accepte de rejoindre le programme Gramchain, pour partager ses données liées aux BHRe. L'équipe opérationnelle d'hygiène de Pontoise lui demande ses informations administratives et différents consentements, en 1). Ces consentements sont au nombre de trois : pour permettre la collecte, la consultation et le stockage de ses données dans la blockchain, pour autoriser le partage avec d'autres établissements de santé et pour permettre l'utilisation du serveur externe stockant des copies de clés.

L'équipe d'hygiène fait une demande de création de la clé maitresse secrète auprès du cloud externe (2). Grâce à un logiciel spécifique, le cloud crée la clé à l'étape 3), puis la sauvegarde sur son propre système de stockage à l'étape 4). Enfin, à l'étape 5), la clé maitresse secrète est envoyée au portefeuille de Bob.

Les procédures de déclaration déjà en place, comme par exemple la déclaration sur e-sin pour l'agence régionale de santé en France, restent valables, afin de maximiser la transmission des informations.

3.3. *Écriture dans la blockchain*

Bob a maintenant sa clé maitresse secrète. Ses données BRHe peuvent être écrites dans la blockchain. La procédure d'écriture est représentée dans la figure 3.

Afin de sauvegarder et de partager les données BRHe, l'équipe médicale de Pontoise enregistre ces

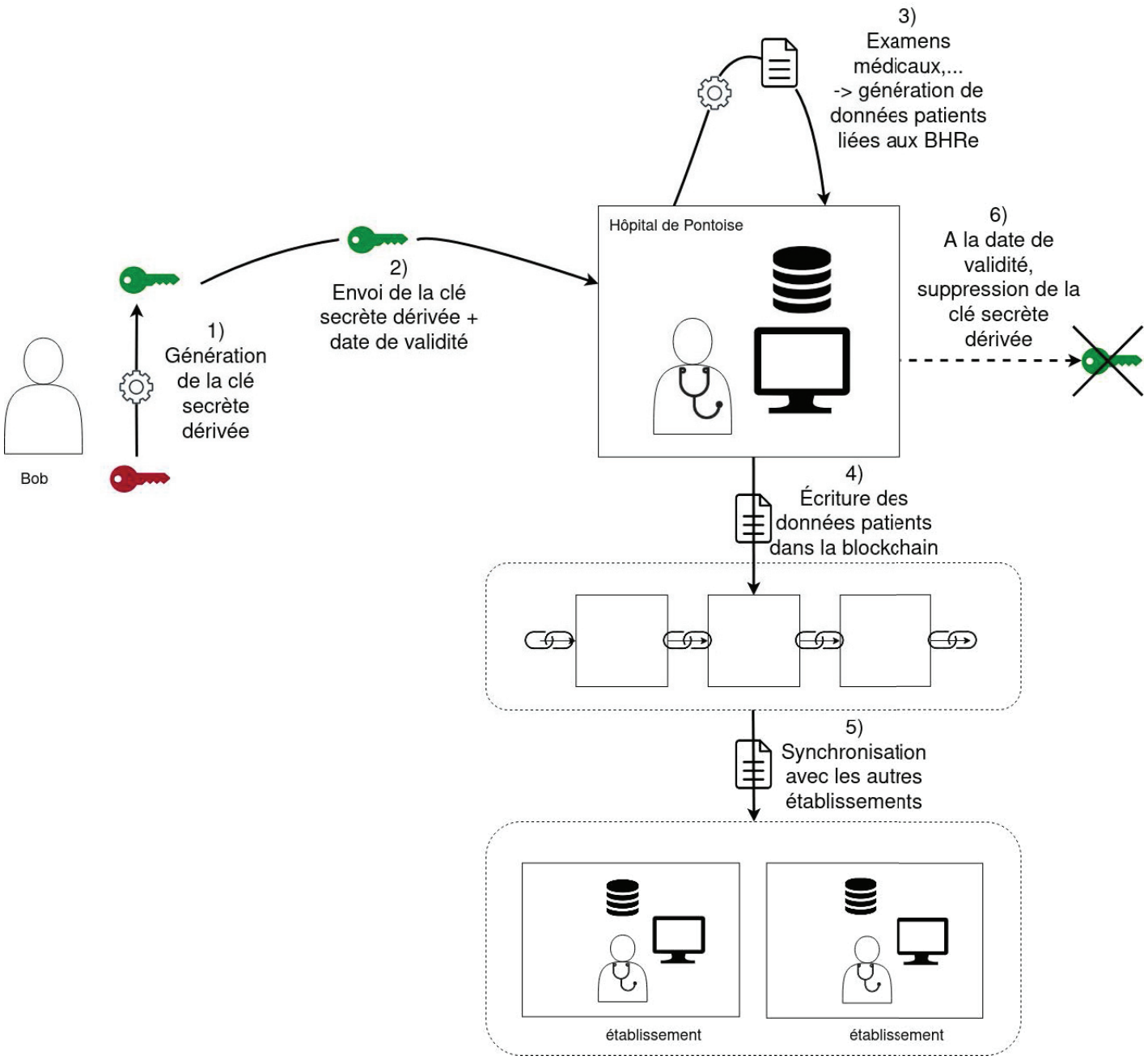

FIGURE 3. *Procédure d'écriture des informations BHRe du patient Bob*

résultats dans la chaine, sous une forme chiffrée. Pour ce faire, ils ont besoin d'une clé dérivée fournie par Bob. Cette étape est la première sur la figure 3. Cette clé est générée par Bob, grâce à sa clé maitresse secrète. Le protocole précis de génération de la clé dérivée est expliqué dans la section 3.2.1

Une fois la clé générée, Bob la fournit à l'hôpital avec une date de validité. Cette date de validité autorise l'hôpital à l'utiliser uniquement pendant une période limitée correspondant à l'hospitalisation de Bob (étape 2).

Pendant la phase d'hospitalisation, l'hôpital effectue des examens médicaux sur Bob et génère certaines données liées aux BRHe (3). Ces données sont variées, comme des informations sur le patient (nom, prénom, numéro d'identification,...), des données d'hospitalisation (date d'entrée, département, référence du service,...) et des informations BRHe (niveau de risque, résultats, procédure pour contacter les patients, type de BRHe,...). Ces données sont chiffrées avec la clé dérivée de Bob, et envoyées sous

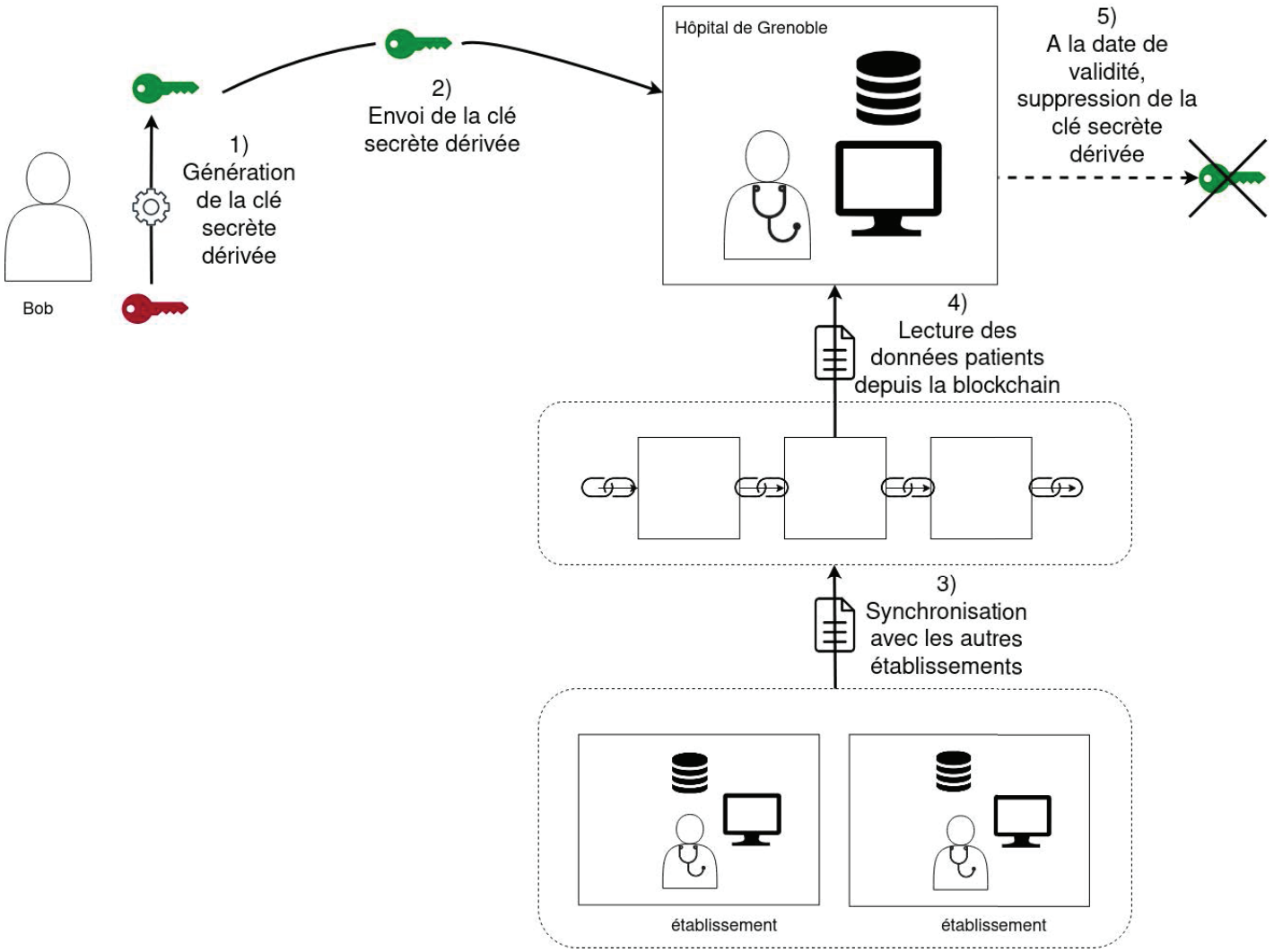

FIGURE 4. *Procédure de lecture des informations BHRe du patient Bob*

forme de transaction sur la *blockchain* en phase 4. Une fois la transaction acceptée et insérée dans un nouveau bloc, les autres nœuds, et les institutions médicales partenaires, acceptent ce bloc et ses transactions et le sauvegardent sur leur propre copie locale de la *blockchain* (5).

Les étapes 3 - 4 - 5 sont répétées un certain nombre de fois, en fonction de la durée du séjour de Bob et des examens qu'il reçoit. À la fin de cette période, lorsque Bob quitte l'hôpital, celui-ci supprime sa copie de la clé dérivée (6).

3.4. *Lecture depuis la blockchain*

3.4.1. Procédure classique

Le même patient, Bob, doit consulter un cardiologue et se rend à l'hôpital de Grenoble. Pour adapter les soins et prendre les précautions d'hygiène suffisantes, le service de cardiologie souhaite accéder aux informations de sa BRHe. L'hôpital stocke sa propre copie de la *blockchain* et dispose des données de Bob sous forme chiffrée. Il a besoin de la clé dérivée associée pour les obtenir en clair et pouvoir les utiliser. Dans cette situation classique, Bob est en mesure de donner lui-même la clé à l'établissement de santé. La figure 4 présente cette procédure.

Lorsque Bob se rend à l'hôpital de Grenoble, et régénère la bonne clé dérivée lors de son inscription

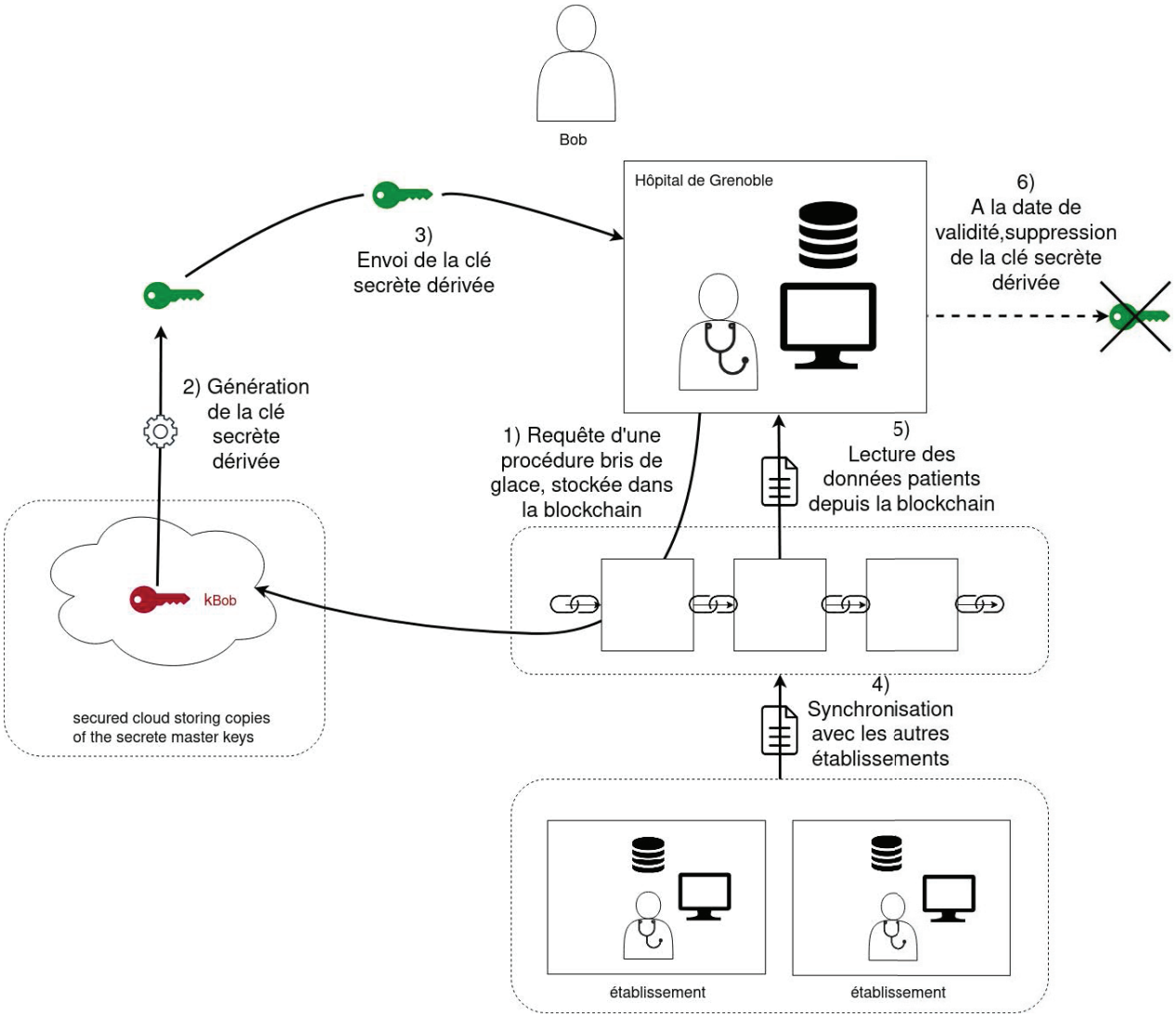

FIGURE 5. *Procédure de bris de glace pour la lecture des informations BHRe du patient Bob*

(1), correspondant aux données de la requête, à partir de sa clé maitresse secrète. Cette opération est effectuée en utilisant son porte-monnaie. Il fournit cette clé dérivée à l'hôpital (2). Ensuite, en 3), l'hôpital synchronise sa copie de la *blockchain* avec celle des autres établissements de santé du réseau. Cette opération est censée être effectuée automatiquement et régulièrement. Ensuite, il extrait les données BRHe de Bob en 4), et les déchiffre. Cela permet à l'hôpital de récupérer les dernières informations sur son statut de porteur, ainsi que le type de bactéries en cause, etc.

A la fin de la date de validité, à l'étape 5), l'hôpital supprime la clé.

3.4.2. Procédure d'urgence "bris de glace"

Un autre cas peut se présenter lorsque Bob n'est pas en mesure de donner son consentement en fournissant la clé dérivée. Cela peut arriver dans une situation d'urgence où Bob est inconscient, ou sans son portefeuille. Dans ce cas, une procédure de bris de glace est utilisée, consistant à contourner l'autorisation de Bob. Ce type de procédure, présentée dans la figure 5, est déjà couramment utilisée dans les hôpitaux et est déclenchée avec l'accord de l'équipe d'éthique médicale, dans des conditions spécifiques et en cas d'urgence uniquement.

Dans cette situation, le personnel médical émet une demande de bris de glace pour accéder aux données

de Bob, en enregistrant cette demande sur la *blockchain* (1). Le serveur cloud externe est informé de cette demande. Comme il stocke sa propre copie de la clé maitresse secrète de Bob, il génère la clé dérivée correspondant aux données demandées par Bob 2). À l'étape 3, il envoie cette clé à l'hôpital demandeur. Le reste de la procédure est similaire à celle du cas d'utilisation classique. L'hôpital se synchronise sur la *blockchain* (4) puis déchiffre les données de Bob en utilisant la clé dérivée (5). Enfin, lorsque la date de validité de la clé est atteinte ou lorsque Bob quitte l'hôpital, ce dernier supprime sa copie locale de la clé (6).

L'avantage de stocker la demande de procédure dans la *blockchain* est qu'elle est enregistrée de façon immuable, ce qui est notamment utile en cas de contrôle futur sur la légitimité de la demande. Ainsi, on espère limiter le risque d'abus.

4. Intérêts de Gramchain

L'objectif principal de notre système est d'améliorer le stockage et le partage des données sur les BHRe. Dans la section 1, nous avons expliqué le problème des BHRe et pourquoi les solutions actuelles de stockage des données des patients porteurs sont insuffisantes. Dans cette section, nous allons discuter des différents intérêts de notre système par rapport à ceux existant. Tout d'abord, nous expliquerons pourquoi le stockage des données est amélioré. Ensuite, nous verrons comment Gramchain peut améliorer le partage des données. Enfin, nous aborderons la conformité au RGPD.

4.1. *Stockage*

Comme présenté dans la section 1, la gestion des données sur les patients porteurs de BHRe est pour l'instant hétérogène. Chaque hôpital utilise son propre système, allant des documents papier aux feuilles de calcul Excel. Il n'y a pas de partage efficace des données entre les établissements de santé indépendants. Ce manque d'informations peut affecter le diagnostic et le traitement, avec des conséquences graves directes telles que le décès du patient, ou engendrer des épidémies.

Gramchain utilise une *blockchain* privée à permission offrant une gestion uniforme des données sur les BHRe, qui sont stockées dans un espace de stockage précis et unique. Cette solution étant interopérable, il est nécessaire d'utiliser des standards sur le format des données stockées.

Une *blockchain* est un registre numérique de toutes les transactions. Elle s'enrichit en permanence de nouveaux blocs ajoutés par les noeuds participants. Chaque bloc contient une empreinte cryptographique du bloc précédent, des données et quelques autres informations. Il est impossible de modifier le contenu d'un ancien bloc sans modifier tous les blocs qui viennent après lui, ce qui permet de réduire le risque de falsification des données et de garantir leur intégrité. Cette propriété d'immuabilité renforce l'intégrité du système. Elle est très intéressante dans les systèmes d'information médicaux, car les données de santé ne doivent pas être altérées.

La technologie *blockchain* propose nativement un mécanisme d'authentification qui permet de savoir qui a créé une donnée. Grâce à la cryptographie asymétrique, le créateur de la donnée la signe en utilisant sa clé privée.

Contrairement à de nombreuses solutions existantes présentées en 1, les données sont stockées dans

la chaine sous forme chiffrées, avec des algorithmes cryptographiques recommandés par des organismes spécialisés [19]. La solution impose un contrôle d'accès, car les clés cryptographiques sont fournies par le patient qui devient l'acteur principal de ses données. Dans la section 1, nous avons présenté les fonctions de dérivation de clés, un mécanisme cryptographique qui permet de générer des clés dérivées à partir d'une clé maitresse secrète et de données publiques. Le patient peut ainsi choisir précisément les informations qu'il souhaite donner aux établissements de santé qu'il visite. La confidentialité des données est améliorée, ainsi que le contrôle du patient sur ses données.

4.2. *Partage décentralisé des données*

En l'absence de dossier médical partagé à grande échelle, les données ne circulent pas automatiquement d'un établissement de santé à un autre. Or, dans le cas d'un patient porteur d'une BHRe, l'équipe médicale doit avoir accès à ces informations pour pouvoir adapter au mieux les soins et éviter de nouvelles contaminations. Cette demande se fait actuellement manuellement et sans protocole précis. Elle nécessite donc du temps et du personnel, et la sécurité des données qui transitent n'est pas garantie.

Comme expliqué dans la section 1, la *blockchain* est une base de données distribuée qui permet un partage sécurisé, transparent, préservant la confidentialité et inviolable des données entre plusieurs parties. C'est cette sécurité qui la rend bien adaptée au partage de données. La *blockchain* est construite sur un réseau peer-to-peer (ici basé sur des permissions), et les données sont partagées avec d'autres noeuds qui sont autorisés à y accéder, ici d'autres établissements de santé, plutôt qu'avec un seul serveur central. Grâce à cette réplication, les données ne sont plus sensibles à un point de défaillance et la perte des serveurs d'une institution devient moins importante. La disponibilité des données est améliorée, car chaque hôpital du réseau stocke l'ensemble de la chaine, c'est-à-dire toutes les données relatives aux patients porteurs de BHRe.

Le problème des BHRe est un problème international. En effet, comme nous l'avons vu dans la section 1, plus d'un tiers des incidents liés à cette bactérie ont un lien direct avec l'étranger. Afin de limiter ces incidents, en France lors d'un rapatriement sanitaire depuis l'étranger, un formulaire de transfert contenant les données personnelles médicales est obligatoire, spécifiant la provenance du pays, la durée du séjour, la caractéristique de BHRe, les prélèvements effectués et à prévoir, et les résultats. Par conséquent, le partage des données relatives aux BHRe doit se faire entre les pays à un niveau mondial. La *blockchain* est basée sur un système décentralisé, qui permet à différentes entités d'échanger des données en se mettant d'accord sur le contenu de la chaine, sans avoir recours à une autorité centrale. Cette propriété est très intéressante ici, car chaque institution médicale dans chaque pays pourrait rejoindre le réseau, stocker et vérifier sa propre chaine, sans accorder plus de confiance ou de droits aux autres, ce qui signifie que la *blockchain* n'est pas contrôlée par une seule entité. Il semble plus cohérent d'imaginer une adoption à grande échelle si les différents pays conservent leur propre autorité et leurs propres données, plutôt qu'un seul serveur central.

4.3. *Conformité au RGPD*

Le règlement général sur la protection des données (RGPD) est entré en application dans toute l'Union Européenne en 2018. Son objectif principal est la protection des données personnelles des citoyens de l'UE. Son objectif secondaire est de favoriser le partage des données. Pour cela, il est nécessaire de

tracer et protéger les données, mais aussi de connaître tous les traitements qui peuvent être effectués sur celles-ci.

Blockchain et RGPD font l'objet de nombreux articles scientifiques et d'études par des comités d'État [20, 21, 5]. La Commission Nationale de l'Informatique et des Libertés a d'ailleurs mis en place un groupe de travail pour étudier la compatibilité entre *blockchain* et stockage des données de santé, en 2018. Ce document ne donne pas de réponse claire concernant l'incompatibilité, mais soulève des points potentiellement bloquants sur lesquels travailler. Plusieurs points d'attention ressortent de ces articles : comment fonctionne le droit à l'oubli dans un système immuable, comment les données sont stockées dans la chaine et comment assurer une confidentialité minimale et une anonymisation.

L'entrée en vigueur du RGPD marque un changement de paradigme dans la protection des données personnelles. Ce changement provient de deux concepts clés spécifiés par le règlement, à savoir le principe de responsabilité et le Privacy by Design.

La responsabilité impose au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées. En cas de contrôle par une autorité administrative compétente, il doit démontrer que les mesures sont conformes aux règles. Les mesures prises pour se conformer à ce principe sont détaillées dans la section suivante.

La compatibilité avec le RGPD impose de plus de respecter le principe de minimisation de la collecte. Les données personnelles stockées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leur traitement ultérieur. Gramchain ne stocke que des données directement liées aux BHRe, la minimisation est donc correcte.

Pour être compatible, il est nécessaire d'appliquer une méthode de travail prenant en compte la protection des données personnelles le plus tôt possible, dès la conception de la solution. Le Privacy by Design implique d'adopter un comportement proactif en matière de protection de la vie privée dès la conception de la solution technique. Nous avons choisi cette méthode, en intégrant ces problématiques dès le début du projet. Une consultation de la CNIL est également prévue, afin que le projet et ses méthodes soient validés. Un autre avantage est qu'elle est compatible avec d'autres réglementations : California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA),... Dans notre équipe, la personne en charge des aspects informatiques et libertés a été impliquée dans les étapes préalables au choix de l'architecture. Ces réflexions ont permis de mettre en évidence certains besoins, comme la nécessité de granularité dans l'accès aux données et la nécessité d'obtenir le consentement avant de créer toute clé.

La collecte de données médicales est théoriquement interdite. L'article 9 du RGPD exige une situation particulière pour passer outre cette interdiction. L'équipe médicale professionnelle est autorisée à exécuter ce traitement à des fins de médecine préventive, de diagnostic médical et de soins de santé. Dans le cadre du projet Gramchain, le traitement est réalisé conjointement avec une entreprise privée. Le consentement explicite du patient doit être obtenu pour permettre la collecte, la consultation et le stockage des données dans la blockchain. Un deuxième consentement est nécessaire pour autoriser le partage des données avec d'autres établissements de santé. Un troisième consentement du patient est nécessaire pour permettre l'utilisation d'un cloud externe stockant des copies de clés. Ces trois consentements sont donnés en même temps, lors de l'enregistrement du patient, comme expliqué dans la section 3.2.

L'évaluation d'impact sur la vie privée (PIA) est un document qui permet d'assurer un équilibre entre les finalités du traitement et les droits et libertés des personnes concernées. Au cours de ce processus, le Data Protection Office (DPO) et le responsable de la sécurité informatique évaluent si les mesures existantes et prévues sont conformes aux principes fondamentaux du RGPD et aux bonnes pratiques de sécurité. L'objectif est de réduire les risques résiduels lors de la mise en œuvre du traitement. L'article 35 du RGPD définit les cas dans lesquels la réalisation d'une PIA est obligatoire. Le critère 1, le traitement réalisé à grande échelle, et le critère 2, le traitement de données sensibles, rendent obligatoire la rédaction d'une PIA. Dans Gramchain, les principales difficultés sont l'utilisation de la technologie *blockchain* et la collecte des données de santé. Après avoir terminé la réalisation de cette évaluation interne pour le projet Gramchain, nous estimons que les risques résiduels sont suffisamment faibles pour pouvoir le soumettre à la CNIL pour validation.

5. Discussion

Des bases de données stockant des informations sur les patients porteurs de BHRe existent, mais sont confrontées à plusieurs problèmes importants, notamment les difficultés à les partager largement (entre hôpitaux et à l'international) et l'incompatibilité avec le RGPB. En outre, le patient ne participe pas au processus de décision et est totalement exclu du système. Dans cet article, nous avons présenté une solution de stockage et de partage de ce type de données, basée sur la blockchain, et permettant de répondre à ces problématiques.

L'architecture de la solution, son fonctionnement et ses avantages ont été détaillés dans les sections précédents. Nous allons aborder ici quelques pistes qui nous semblent intéressantes à travailler.

5.1. *Souveraineté patient VS disponibilité des données*

Comme expliqué dans la section 2, nous proposons une solution avec un serveur externe stockant une copie des clés secrètes maitresses des patients. Ce serveur doit donc répondre à des critères de sécurité spécifiques et être certifié hébergeur de données de santé pour la France.

Cette redondance permet à un patient qui perd sa clé maitresse secrète de la récupérer. Les données chiffrées avec cette clé restent accessibles, et la disponibilité augmente. La procédure d'urgence "bris de glace" permet au personnel soignant de pouvoir accéder aux informations nécessaires dans le cas où le patient n'est pas en mesure de fournir lui-même une clé dérivée, par exemple parce qu'il est inconscient. Mais cette amélioration de la disponibilité se fait au détriment de la souveraineté du patient, puisqu'il devient possible de se passer de son consentement direct, et qu'il n'est plus exactement au centre du système. Dans la version actuelle de Gramchain, nous choisissons la première solution, où une sauvegarde des clés secrètes maitresses est située sur un serveur externe. En effet, il est déjà courant dans le domaine de la santé de disposer de procédures de bris de glace pour accéder en urgence aux données de santé d'un patient, sans obtenir sa validation directe. C'est le cas, par exemple, du personnel médical d'urgence qui souhaite accéder au dossier médical partagé d'un groupe d'hôpitaux. Cette pratique est justifiée par le fait qu'elle permet une meilleure adaptation des soins, ce qui peut sauver la vie du patient et éviter l'émergence éventuelle d'une épidémie au sein d'un établissement.

La deuxième solution consiste à ne pas utiliser de cloud de secours, et à confier la gestion de la clé maitresse secrète entièrement au patient et à lui seul. Le patient est placé au cœur du système, seul son accord permet l'accès à ses données. Il a une réelle capacité à exercer son consentement et à contrôler le partage de ses données. Mais dans le cas où il ne peut fournir des clés dérivées à l'établissement de santé, par exemple en cas perte de son porte-feuille, d'un piratage, ou s'il n'est pas conscient, les données ne sont pas lisibles. L'équipe médicale n'est pas en mesure de savoir si le patient a une BHRe ou non, ni ses détails. Les soins ne sont pas adaptés et les conséquences restent alors inchangées : risque pour le patient et risque à plus grande échelle en cas de transmission croisée. La disponibilité des données est donc fortement impactée et réduite.

Le dilemme ici est de choisir le meilleur compromis entre l'augmentation de la disponibilité des données qui conduit à la diminution de la souveraineté du patient, et l'augmentation du risque de perte de données associé à l'augmentation du contrôle du patient sur ses données.

Une amélioration possible serait de laisser la possibilité au patient de choisir ou non cette redondance sur un serveur externe. Comme expliqué dans la sous-section 4.3, lors de son enregistrement dans le système, il fournit 3 consentement, dont un consentement pour autoriser l'accès à ses données dans une situation d'urgence. Si le patient ne souhaite pas autoriser cela, alors il n'y aura pas de copie de sa clé maitresse secrète sur le serveur externe. La procédure de bris de glace présentée en 3.4.2 n'est pas possible, mais le reste ne change pas.

5.2. *Blockchain et RGPD*

Comme indiqué précédemment, la mise en conformité RGPD est en cours, avec la création de certains documents spécifiques.

L'utilisation d'une *blockchain* soulève des questions sur l'exercice du droit de retrait pour les personnes concernées, les patients porteurs de BHRe. Le RGPD permet aux patients de disposer de leurs droits d'effacement, de rectification et d'archivage. La *blockchain* étant immuable, il n'est pas possible d'effacer simplement les données.

Dans le document [22], les auteurs notent que "le RGPD ne précise pas ce qu'est l'effacement". Dans ce contexte, la CNIL reconnaît que certaines techniques de chiffrement, couplées à la destruction des clés, peuvent potentiellement être considérées comme un effacement même s'il ne s'agit pas d'un effacement au "sens strict". Dans Gramchain, les données stockées dans la chaine sont chiffrées avec des algorithmes réputés solides et sûrs [19]. La destruction des clés maitresses secrètes, tant sur les portefeuilles des patients que sur ceux du serveur externe, peut être considérée comme un effacement, puisque les données sont par définition illisibles sans elles. Ce point n'est donc pas considéré comme bloquant.

5.3. *Élargissement du périmètre de Gramchain*

Même si la solution Gramchain est utilisée pour le stockage et le partage des données patients porteurs de BHRe, on peut imaginer l'étendre à un système plus large.

Dans l'état actuel des choses,la solution Gramchain peut être une solution complémentaire pour suivre une maladie spécifique à travers l'espace, le temps et les professions de santé, comme c'est le cas ici pour le suivi des BHRe. Ceci est particulièrement utile dans les zones frontalières où le suivi des patients est

complexes car les personnes peuvent se rendre dans des établissements de santé de différents pays, rendant le partage de ses données d'autant plus difficile. Un autre domaine d'application possible serait pour les maladies qui nécessitent un suivi sur le long terme, comme les cancers ou les maladies chroniques.

Gramchain peut également servir d'aide à la décision médicale. Couplée avec une formation spécifique ou d'outils faciles à prendre en main, le patient peut être réellement au cœur de son propre système d'information médicale en écrivant lui-même les informations utiles pour éviter l'aggravation de sa situation médicale. Ces inscriptions peuvent se faire directement sur la *blockchain* ou un espace associé comme l'espace de santé numérique [3] disponible en France depuis 2022. Cet outil, proposé par le Ministère de la santé et l'Assurance Maladie, a pour but de donner la main à l'usager dans la gestion de ses données. Il se présente sous la forme d'un portail web dans lequel le patient et le professionnel de santé vont stocker et partager des données de santé. Il est représentatif de la dynamique de placement du patient au centre du système.

Les informations fournis par le patient peuvent être diverses, et provenir de sources différentes. Dans notre cas d'étude, les BHRe, un exemple serait de savoir si le patient a voyagé dans un pays à haut risque de contamination, si des effets indésirables surviennent, etc. L'information est alors disponible pour tous les professionnels de santé concernés. D'autres sources peuvent venir compléter ces informations, pour permettre un suivi encore plus précis du patient. Les objets connectés génèrent un grand nombre de données, qui pourraient être utile dans le diagnostic : évolution du poids, de la tension, du rythme cardiaque, etc.

Une autre possibilité, explorée par plusieurs articles [23, 24], est de permettre à l'usager de partager ses données avec des acteurs externes, contre rémunération. Les données de santé peuvent être particulièrement utiles pour la recherche ou le data analytics et sont donc très demandées. Une économie numérique, reposant sur la blockchain et une cryptomonnaie, permet de mettre en relation le patient disposant de nombreuses données pertinentes et une entreprise ou un laboratoire ayant besoin de celles-ci pour améliorer produits et services.

6. Conclusion

Les BHRe posent un problème de santé publique à très large échelle, en partie dû au manque d'échange d'informations sur les patients porteurs. Cet article présente une solution ayant pour but d'améliorer le suivi des patients atteints de BHRe, en stockant ces informations sur une *blockchain* privée qui sera ensuite partagée entre les différents établissements de santé. Cette proposition se veut intéropérable à grande échelle et conforme au RGPD. Elle est articulé de façon à rendre le patient maitre de ses données, car son consentement est obligatoire pour autoriser une personnel de santé à accéder à ces données. Cette confidentialité et ce contrôle se fait avec un système de clé dérivée unique pour chaque examen, obtenues à partir d'une clé maitresse secrète appartenant au patient. En outre, nous proposons l'utilisation d'un système de serveur externe stockant une copie des clés maitresses secrètes, en cas de perte ou de procédure de bris de verre.

Dans une prochaine étape, nous souhaitons valider nos différents choix en développant des smart contracts d'écriture et de lecture sur la blockchain, afin de simuler son fonctionnement à plus grande

3. https ://www.monespacesante.fr

échelle, sur plusieurs dizaines puis centaines de nœuds. Des tests grandeur nature avec les hôpitaux de Grenoble et de Pontoise sont également prévus, lorsque le développement du logiciel le permettra. Ce premier retour d'expérience nous permettra d'ajuster la proposition et de la valider en conditions réelles.

Comme expliqué dans la section 4.3, nous sommes en attente d'une validation de la CNIL concernant notre conformité avec le RGPD. Mais nous avons travaillé en suivant les principes du Privacy by Design dès le début du projet, et nous avons pris soin de respecter les grands principes du RGPD, nous sommes donc relativement confiants sur ce sujet.

Comme mentionné dans l'introduction et dans la section 1, le problème majeur est la traçabilité des patients porteurs de BHRe au-delà des frontières. Bien que nous visions dans un premier temps le marché français, il serait pertinent d'utiliser cette solution à plus grande échelle, entre pays européens, voire dans le monde entier. L'une des propriétés de la *blockchain* est la décentralisation, ce qui est un avantage non négligeable dans la perspective d'ouvrir le système entre différents pays et continents.

Enfin, nous avons travaillé ici sur le cas d'utilisation précis des données BHRe. Cependant, ce système peut être étendu et reproduit sur d'autres types de données de santé nécessitant un suivi dans le temps et l'espace, comme les cancers ou les maladies chroniques.

Bibliographie

[1] C. J. Murray, K. S. Ikuta, F. Sharara, L. Swetschinski, G. R. Aguilar, A. Gray, C. Han, C. Bisignano, P. Rao, E. Wool *et al.*, "Global burden of bacterial antimicrobial resistance in 2019 : a systematic analysis," *The Lancet*, 2022.

[2] S. P. France, "Bilan des signalements bhre 2019," https ://www.santepubliquefrance.fr/content/download/304250/2857320, 2020.

[3] E. C. for Disease Prevention and Control, "Antimicrobial resistance in the eu/eea (ears-net)—annual epidemiological report 2019," *ECDC, Stockholm*, 2020.

[4] H. C. de la Santé Publique, "Prévention de la transmission croisée des bactéries hautement résistantes aux antibiotiques émergentes (bhre)," 2013.

[5] CNIL, "Blockchain : Premiers éléments d'analyse de la cnil," https ://www.cnil.fr/sites/default/files/atoms/files/la_blockchain 2018.

[6] R. on Antimicrobial Resistance, *Antimicrobial resistance : tackling a crisis for the health and wealth of nations*. Review on Antimicrobial Resistance, 2014.

[7] F. Baquer, E. Giraudon, and F. Jehl, "Bactéries multirésistantes et hautement résistantes émergentes : définition et mécanismes de résistance d'intérêt épidémiologique," *Revue Francophone des Laboratoires*, vol. 2021, no. 537, pp. 28–36, 2021.

[8] S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[9] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[10] N. Six, N. Herbaut, and C. Salinesi, "Quelle blockchain choisir ? un outil d'aide à la décision pour guider le choix de technologie blockchain," in *INFORSID 2020*, 2020, pp. 135–150.

[11] K. Wüst and A. Gervais, "Do you need a blockchain ?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 45–54.

[12] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare : A scoping review," *International Journal of Medical Informatics*, vol. 142, p. 104246, 2020.

[13] F. Mohammadipanah and H. Sajedi, "Potential of blockchain approach on development and security of microbial databases," *Biological Procedures Online*, vol. 23, no. 1, pp. 1–8, 2021.

[14] R. H. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (healthchain) : evaluation and proof-of-concept study," *J Med Internet Res*, vol. 21, no. 8, p. e13592, 2019.

[15] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain personal health records : systematic review," *Journal of medical Internet research*, vol. 23, no. 4, p. e25094, 2021.

[16] S. Bhattacharya, A. Singh, and M. M. Hossain, "Strengthening public health surveillance through blockchain technology," *AIMS public health*, vol. 6, no. 3, p. 326, 2019.

[17] O. E. Rifai, M. Biotteau, X. d. Boissezon, I. Megdiche, F. Ravat, and O. Teste, "Blockchain-based personal health records for patients' empowerment," in *International Conference on Research Challenges in Information Science*. Springer, 2020, pp. 455–471.

[18] C. W. Chuah, E. Dawson, and L. Simpson, "Key derivation function : the sckdf scheme," in *IFIP International Information Security Conference*. Springer, 2013, pp. 125–138.

[19] A. nationale de la sécurité des systèmes d'information, "Guide de sélection d'algorithmes cryptographiques," https ://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf, 2021.

[20] A. Hasselgren, P. K. Wan, M. Horn, K. Kralevska, D. Gligoroski, and A. Faxvaag, "Gdpr compliance for blockchain applications in healthcare," *arXiv preprint arXiv :2009.12913*, 2020.

[21] F. Fatehi, F. Hassandoust, R. K. Ko, and S. Akhlaghpour, "General data protection regulation (gdpr) in healthcare : Hot topics and research fronts," in *Digital Personalized Health and Medicine*. IOS Press, 2020, pp. 1118–1122.

[22] E. U. B. Observatory and Forum, "Blockchain and the gdpr," https ://www.eublockchainforum.eu/sites/default/files/reports/20 2019.

[23] M. Maher and I. Khan, "From sharing to selling : Challenges and opportunities of establishing a digital health data marketplace using blockchain technologies," *Blockchain in Healthcare Today*, 2022.

[24] S. Lawrenz, P. Sharma, and A. Rausch, "Blockchain technology as an approach for data marketplaces," in *Proceedings of the 2019 International Conference on Blockchain Technology*, 2019, pp. 55–59.

