Medwish : Ecosystème de santé décentralisé

Version de référence : Version française 2.1.6 (pre-print)

contact@medwish.io

DEC 2020

Abstract

Un système qui permettrait la valorisation des données de santé optimiserait l'accès aux soins.

La gestion des données de santé contrôlée par les patients apporte une partie de la solution à cette valorisation, mais les bénéfices de ce contrôle sont perdus dès lors qu'il est possible de rompre avec le secret médical.

Nous proposons une solution de gestion décentralisée et sécurisée des données de santé qui, associée à des échanges de valeurs plus confidentiels, permet de garantir le secret médical.

Les données sont anonymisées et chiffrées unitairement côté client. Les données sont ensuite envoyées sur un réseau de stockage décentralisé et sécurisé. Le réseau est constitué de nœuds qui gèrent le stockage et valident les échanges de valeurs (transactions). L'accès aux données (lecture et en écriture) est contrôlé par les patients. Les patients peuvent monétiser ou non cet accès. La monétisation ou tout autre échange de valeur sur le réseau s'opère sur un serveur d'horodatage latéral à bitcoin dont les transactions, confidentielles par défaut, sont validées par les nœuds de réseau.

Nous proposons une solution qui incite à rediriger la valeur des données de santé vers le financement des soins ce qui permet de garantir un meilleur accès aux soins.

La valeur des données de santé, soutenue par une collatéralisation, est stabilisée pour les acteurs de soins (patients et professionnels).
Des incitations à financer les soins sont mises en place comme par exemple une fonte monétaire modérée qui intervient si les acteurs de soin n'effectuent aucune action durant une période de temps donnée. Il existe deux types d'action, les dépenses pour des soins immédiats ou les placements. Il existe deux types de placements, ceux pour des dépenses de soins futures (générateurs d'intérêts) et ceux dans les entreprises fournissant des produits ou services de soins sur le réseau.

Enfin nous proposons une gouvernance communautaire avec démocratie liquide et un vote quadratique.

Pour devenir nœud du réseau il faut satisfaire deux conditions, la réussite d'un test différenciant les humains des robots et le séquestre de cryptomonnaie sur une adresse multi-signatures gérée par la gouvernance. La participation à la gouvernance se fait par un second séquestre. La fin des séquestres est décidée par le participant. La valeur sortante, dépend du travail de sécurité, de stockage et de l'implication dans la gouvernance.

1 Introduction

L'espérance de vie augmente mais l'espérance de vie en bonne santé tend à stagner depuis 10 ans [1]. Ce Gap grandissant traduit une augmentation du besoin de soins passé l'âge de l'espérance de vie en bonne santé et une augmentation des coûts associés aux soins (devenant insupportables à l'horizon 2050 [2]). La baisse prévue du nombre de médecins dans la population mondiale [3] crée mécaniquement une diminution de l'accès aux soins, sans distinction d'âge, par manque de professionnels de santé et ou par manque de capacité de financement des soins.

Nous savons que les progrès technologiques des dispositifs médicaux ou de l'algorithmie médicale améliorent nettement la qualité des soins. Ces progrès sont notamment permis par la collecte de données de santé. Mais cette collecte reste entièrement à la charge des patients qui financent leurs créations, leurs stockages, leurs utilisations et leurs résultats. Si l'amélioration de la qualité des soins dépend des données de santé et si la collecte des données de santé dépend du financement des patients alors les données de santé revêtent une valeur financière non négligeable pour l'amélioration de la qualité des soins.

Nous savons que le secret médical fait partie intégrante du droit au respect et la protection de la vie privée, droit inscrit dans la Déclaration universelle des droits de l'homme des Nations unies [4]. Nous savons que le secret médical ne peut pas être révélé sans consentement. Or si le secret médical inclut toutes les interactions avec un professionnel de santé, la connaissance par un tiers d'un paiement envers un médecin rompt le secret médical. Dès lors, les données de transactions à destination de soins doivent être traitées avec autant de précaution que les données de santé. Elles doivent alors être soumises au secret médical et aucun tiers de confiance ne doit avoir la capacité de pouvoir identifier un patient ou les pathologies dont il souffre sans consentement.

Si l'on s'accorde à dire que la qualité des soins et les besoins de soins sont croissants et que la démographie médicale est décroissante alors les leviers d'accessibilité aux soins sont l'augmentation de la population de soignants et ou l'augmentation des capacités de financement des soins par individu. Or la formation de plus de professionnels de santé demande des moyens humains et financiers trop importants à court terme. Moyens dont nous ne disposons pas.

On conclut donc ici que le meilleur levier d'accès aux soins est l'augmentation des capacités financières de chaque individu. Et comme on sait que les données de santé possèdent une valeur alors l'accès aux soins doit pouvoir être financé par l'accès aux données de santé.

Une telle politique économique de santé doit présenter, dans le cadre d'un consensus social, des mesures de sorte à inciter à rediriger les recettes de l'accès aux données de santé vers l'accès aux soins.

Or nous savons que d'un point de vue psychologique, les incitations financières sont puissantes pour modifier des comportements. Actuellement les seules incitations proposées le sont au travers des assurances santé. Mais elles restent des investissements à pertes pour les patients tant que le besoin de soins n'est pas présent. Il serait plus profitable pour les patients que leurs investissements en santé deviennent un capital disponible et rémunérateur tant que le besoin de soins n'est pas présent.

Si actuellement les assurances santé dictent les règles quant à l'utilisation des fonds d'un patient,

émettre un nouveau modèle d'assurance santé suppose un nouveau modèle décisionnaire. Nous savons que les expériences scientifiques qui étudient l'homme dans une situation d'exercice de pouvoir concluent toutes au besoin de partage du pouvoir [5]. La traduction de ces expériences est que si l'intérêt est le bien commun alors il est nécessaire de se mettre à l'abri d'une centralisation du pouvoir en le partageant.

Dans ce livre blanc nous proposons une solution au problème de l'accès aux soins sous forme d'un écosystème de santé décentralisé et communautaire. L'écosystème permet la valorisation des données de santé en préservant le secret médical, et incite à utiliser cette valeur pour le financement des soins.

2 Les données de santé

Tout commence par la définition d'une donnée de santé.

Il est établi que les données de santé sont des extensions immatérielles du corps humain, elles sont parties intégrantes de ce qui définit un individu en termes de santé physique ou mentale, passée, présente ou future. Elles peuvent présenter un caractère personnel si elles sont relatives à une personne physique ou si elles présentent un lien direct vers une personne physique. Si aucune information menant à une identification d'une personne physique n'est présente alors la donnée de santé est dite anonyme et si un lien peut être établi elle est dite pseudonyme.

Nous savons que certaines données de santé ne permettent pas l'anonymisation. En effet, une radiographie et un résultat de prise de tension artérielle sont toutes deux des données de santé mais l'une permet une anonymisation alors que l'autre non. Dans le cas de la tension artérielle, celle-ci se présente sous le résultat de deux chiffres (pression systolique + pression diastolique) qu'il faut lier à un patient, un jour, une heure, un état de santé. Par exemple, l'anonymisation pourrait consister à supprimer l'identité du patient. Le résultat pourrait être écrit sous une forme clé/valeur TaSys = 12 TaDia = 8. Dès lors, sans lien reliant cette donnée avec un patient, il n'est pas possible d'identifier un patient autrement qu'en opérant des croisements de données. Pour une radiographie, une simple triangulation de points permettrait la réidentification d'un patient, ce qui ne prendrait techniquement que quelques secondes par comparaison de points avec une base de données de clichés non anonymisés.

Le besoin est de mettre en place des procédures de préservation des personnes physiques différentes suivant le niveau d'anonymisation initiale possible d'une donnée.

Par ailleurs nous savons qu'une donnée de santé est une extension de soi. Or si les travaux de recherche sur des données de santé engendrent une nouvelle donnée relative à la santé, alors toute donnée issue d'un traitement de données de santé est aussi une extension de soi. Nous considérons toutes données issues d'un traitement de données de santé comme une donnée de santé relative à un patient ou un groupe de patients.

A ce stade, se pose la problématique de la notion de propriété des données de santé.

3 Droit de propriété des données de santé

Le droit à la propriété est un droit fondamental inscrit, et adopté par les États membres des Nations unies, dans la Déclaration universelle des droits de l'homme [4].

Le droit de propriété se définit par les droits de jouir et disposer d'une chose de la façon la plus absolue quel que soit le mode d'acquisition légale de ce droit. Un droit de propriété appliqué aux données de santé à caractère personnel reviendrait à avoir la capacité de les vendre, de les louer et même de les détruire. Notons que sur les données de santé ne présentant pas de caractère personnel, un droit de propriété peut être établi quel que soit le mode d'acquisition légal de ce droit de propriété.

On peut alors se poser la question suivante :
Est-on, en tant que personne physique (patient), propriétaire de son corps et par extension de ses données de santé ?

En tout état de cause, les juridictions s'accordent sur le fait que le droit de propriété n'est pas opposable au corps humain et par extension n'est pas opposable aux données de santé. En dehors de l'Iran, il n'est pas possible de monétiser tout ou partie de son corps. Cependant, toute personne possède un droit de jouissance. Ce droit est composé de l'usus (droit d'user, contrôler) et du fructus (droit aux profits). Dit autrement, un patient est en droit d'utiliser ses données de santé et d'en contrôler l'utilisation à son profit.

Nous savons que les données de santé ont une valeur marchande. Mais la valeur des données de santé d'un individu peut-elle être redirigée vers le patient ?

4 Valorisation des données de santé

Nous avons vu qu'aucun patient d'un pays signataire des Nations Unis ne peut vendre ses données de santé ou même les détruire. Cependant il est légal pour un tiers de faire commerce des données de santé si et seulement si, les données sont anonymisées (la conformité légale du recueil des données dépend de l'information faite au patient et du consentement de celui-ci). Les données de santé qui ne présentent ni de caractères personnels, ni de liens directs ou indirects, sont de fait commercialisables.

Selon cet état de fait, un patient ne peut donc pas profiter de la monétisation de ses données de santé à caractère personnel, alors qu'un tiers le peut. Mais un patient obtient cette possibilité si et seulement si aucun lien ne peut être établi entre les données et sa personne.

Le besoin pourrait consister à permettre aux patients de récupérer la valeur de leurs données de santé dans un environnement leur assurant l'absence de lien avec eux-mêmes. Mais toutes les données dites pseudonymes, comme les résultats d'imageries médicales ou encore les données génomiques, en seraient exclues.

Cependant il existe des modalités selon lesquelles un patient perçoit une indemnisation quant à l'utilisation de son corps et par extension ses données de santé. En effet, au niveau international, il est établi la possibilité de réaliser des recherches médicales amenant à la rémunération des patients. Cette rémunération

vient au titre d'une indemnisation pour la participation à une recherche médicale. Il existe différents types de recherches (interventionnelles ou non) mais quel que soit le type de recherche effectuée, la finalité est le développement des connaissances biologiques ou médicales suite à l'obtention de nouvelles données de santé.

On conclut donc que si la finalité de traitement est au bénéfice de la recherche médicale alors un patient peut percevoir un profit à l'utilisation de ses données de santé.

Le besoin consiste donc à permettre aux patients de percevoir une indemnisation quant à l'utilisation de leurs données de santé dans un environnement leur assurant l'absence de lien avec eux-même et dédié à la recherche médicale, quel que soit le niveau d'anonymisation de la donnée.

Pour un tiers, l'absence de liens entre une donnée de santé et un patient se traduit par l'existence du secret médical.

5 Le secret médical

Le secret médical représente un droit fondamental pour le patient et un des piliers de la médecine. Il représente l'ensemble des informations confiées, vues, entendues, comprises ou interprétées lors de l'exercice d'un professionnel de santé concernant un patient.

Le secret médical débute dès la première interaction pouvant conduire aux soins. Par exemple, une prise de rendez-vous, en ligne ou non, doit garantir le secret sur les informations transmises du patient vers le praticien de bout en bout, sans quoi le secret médical est rompu.

Les données de santé relèvent, de fait, du secret médical, dès lors tout traitement de ses données hors du contrôle du patient ou du professionnel de santé (réalisé par un tiers) est en rupture avec le secret médical.

Le besoin réside donc dans la mise en place d'une gestion des données de santé sans tiers de confiance qui garantit le secret médical.

6 Gestion des données de santé

6.1 Structure de stockage

Nous proposons un réseau composé de nœuds connectés les uns aux autres, formant ainsi un réseau de stockage décentralisé. Dans le cadre de la gestion des données, les nœuds de réseau sont des structures physiques d'accueil de base de données décentralisées.

Le stockage décentralisé permet de dépasser les limites du stockage centralisé. Il permet un stockage plus fiable, plus accessible, plus évolutif et résistant mieux à certains types d'attaques, comme le déni de service (DDOS).

6.2 Anonymisation et pseudonymisation

Avant d'être stockée sur le réseau, chaque donnée doit subir un processus empêchant la ré-identification directe ou indirecte des individus (anonymisation) ou à défaut un processus empêchant la ré-identification directe (pseudonymisation).

Cependant le processus mis en place ne doit pas être un frein à la recherche médicale. Par exemple, la suppression du nom et du prénom du patient est évidente mais la date de naissance est souvent retirée en totalité. Effectivement s'il est facile de re-identifier les patients centenaires, remplacer une date de naissance par une tranche d'âge permet de mobiliser des jeux de données indisponibles jusqu'alors pour la recherche tout en préservant un niveau d'anonymisation ou de pseudonymisation par donnée performant.

Dans l'optique d'une préservation du secret médical, nous proposons que la réalisation de ce traitement, première étape de la gestion de données, soit réalisée côté client.

Mais l'anonymisation ou la pseudonymisation ne sont pas suffisantes pour garantir la sécurité des données.

6.3 Chiffrement

Le chiffrement est un procédé cryptographique selon lequel une donnée est rendue illisible par une personne ne possédant pas la clé de déchiffrement.

Dans le cadre du secret médical et de sa préservation ainsi que dans le cadre d'un ré-appropriement des données de santé par les patients, le choix du type de chiffrement devient un enjeu. Le chiffrement à appliquer dépend directement du type de données de santé. Il doit permettre de maintenir au maximum statique les données de santé (c'est-à-dire permettre que les données de santé transitent le moins possible d'un endroit à un autre).

Par ailleurs, il semble important de chiffrer les données avec des clefs uniques afin de réduire la profitabilité d'une attaque de type brute force (un attaque brute force est un principe d'analyse cryptographique consistant à tester toutes les possibilités de clefs de déchiffrement possible). En effet, si un ensemble de plusieurs données (jeu de données) dont la valeur est importante est chiffré avec une même clef de chiffrement, alors la profitabilité d'une attaque de type brute force peut être en faveur de l'attaquant.

Le chiffrement homomorphe apporte une partie de la solution mais son efficacité est fortement diminuée pour la recherche médicale si des données n'ont pas été chiffrées avec la même clef de chiffrement. En effet, le but du chiffrement homomorphe est de permettre la réalisation de calculs sur des données chiffrées (au travers de la couche de chiffrement) sans avoir accès aux données non chiffrées. Le chiffrement homomorphe se présentant comme une des meilleures alternatives pour des données statiques, contrôlée par les patients, et pour une externalisation des calculs. Mais dès lors qu'un calcul porte sur des données apportées par plusieurs patients présentant tous une clef de chiffrement différente alors la complexité est telle que le bénéfice du chiffrement homomorphe est perdu.

Une branche de la cryptographie s'intéresse aux calculs multi-parties sécurisés (MPC) [6]. L'Objectif est de concevoir des solutions permettant à plusieurs parties de calculer ensemble une fonction de leurs

données, tout en gardant ces données secrètes. Contrairement à la cryptographie classique, où l'on cherche à assurer la sécurité malgré la présence d'un adversaire extérieur, le MPC garantit la sécurité face à un adversaire interne contrôlant un ou plusieurs participants. Prendre avantage du MPC permettrait de devenir plus respectueux de la vie privée.

Cependant permettre de réaliser une fonction *f(x)* révèle un peu de x et s'il n'y a aucune autre sécurité supplémtentaire, on donne en théorie la possibilité de découvrir la donnée x.

Nous proposons la mise en place du système de MPC associé à un chiffrement unitaire des données et à l'ajout de bruit. Ainsi chaque donnée possède une clé de déchiffrement différente et n'est accessible qu'au patient. Le bruit, lui, se définit comme l'ajout de données dont la valeur est prise aléatoirement dans l'intervalle constituant la norme connue. Ces données présentent un impact non significatif sur le résultat final. Le chiffrement unitaire associé au bruit rendrait la profitabilité d'une attaque en défaveur de l'attaquant. Enfin ce système de chiffrement permet de garder les données statiques et un contrôle total par le patient.

Se pose alors la problématique du déchiffrement. Si le chiffrement est un enjeu, il est aussi nécessaire de prendre en compte le déchiffrement. Par exemple, le chiffrement homomorphe pose la problématique de la puissance de calcul et donc le temps nécessaire pour la réalisation des calculs au travers la couche de chiffrement. Mais les sommes de puissance de calcul que l'on peut solliciter aujourd'hui associées à la loi de Moore [7] permettent de minimiser cette problématique. De plus, si l'on prend en compte que la rentabilité à miner des cryptomonnaies devient de plus en plus faible pour un particulier, il serait profitable pour tous de permettre d'allouer cette puissance de calculs à des besoins de recherche médicale sur données chiffrées à l'instar de la puissance de calcul allouée au pliage de protéines [8].

Nous avons proposé une solution au chiffrement. La donnée anonymisée et chiffrée est ensuite envoyée sur le réseau et dupliquée sur des nœuds aléatoirement, de manière à maintenir en permanence trois copies de celle-ci pour une question d'accessibilité.

Se pose maintenant la problématique du contrôle et de l'accès aux données.

6.4 Contrôle et accès aux données

Si seuls les patients possèdent le droit de jouissance de leurs données de santé, alors il convient qu'ils soient gestionnaire des droits d'accès aux données de santé.

Nous proposons que le contrôle des droits d'accès aux données en lecture et en écriture soit contrôlé par les patients ou tout autre personne définie par le patient lui-même (un ayant droit, la gouvernance du réseau pour une période limitée, autres). Le patient détient les clefs privées de ce gestionnaire d'accès et ces clefs privées sont transférables après chiffrement à un tiers de confiance choisi par le patient. Les échanges sont réalisés de façon purement pair à pair. Le patient peut à tout moment modifier les droits d'accès. Il peut donc autoriser l'accès en lecture à ses données ou même demander la suppression totale de ses données du réseau (après les avoir téléchargées).

Par ailleurs, les droits d'accès aux lieux de stockage sont contrôlés de façon non automatique, c'est-à-dire qu'une action volontaire de la part du patient est nécessaire.

Un contrôle des données ne définit pas leurs modalités de partage.

6.5 Partage des données

Entre acteurs de soins, aucune limitation n'est à prévoir. Les données de santé nécessaires au bon traitement du patient sont à la discrétion du patient et de son professionnel de santé.

Dans le cadre d'une demande d'accès aux données faite par un tiers, notamment pour la recherche médicale, il est nécessaire de limiter le nombre de données traitables par patient résolvant la problématique de la réidentification [9].

6.6 Cas d'usage

Un tiers, dans le cadre de la recherche médicale et de façon publique, s'identifie, énonce la finalité du traitement des données de façon claire et intelligible, spécifie sa recherche de données (critères d'inclusion et d'exclusion à l'étude), publie son protocole de recherche et informe le patient de ses droits et indemnités.

Cette déclaration d'intention et de recherche de données est postée sur le réseau sur un espace de stockage dédié. Les patients peuvent vérifier s'ils ont la capacité à satisfaire la demande de recherche médicale et ce sans interaction avec le tiers. Le patient ainsi éclairé, consent ou non à satisfaire la demande d'accès.

Le tiers identifié sollicitant le réseau s'oblige à mettre en parution open source le résultat de son travail, quel que soit l'état (finalisé ou non) et ses résultats (significatifs ou non) sur un espace dédié et résilient spécifique aux parutions scientifiques. Ils s'obligent, par ailleurs, à attribuer toutes nouvelles données créées à l'usufruit des patients. Dans le cas du non-respect de cette obligation, le tiers identifié se verra refuser l'accès au réseau par la gouvernance.

6.7 Technologie au lancement

Pour la gestion de donnée décentralisées nous utilisons les outils et services proposés par Protocol LAB dans le cadre de la création de l'IPFS [10] (InterPlanetary Files System) couplé à la solution proposée par Textile.io [11].

Toutefois, Nous savons que cette structure reste incomplète pour garantir le secret médical et qu'il convient d'assurer une confidentialité aux échanges de valeur.

7 Serveur d'horodatage latéral

Le secret médical, qui est une partie intégrante du droit à la vie privée, nous amène à identifier une problématique sérieuse :

L'opposition actuelle du droit à la vie privée et la surveillance accrue dans le cadre de la lutte anti-blanchissement et financement du terrorisme (LAB-FT).

En tout état de cause, et de manière généralisée en matière de finance, la LAB-FT est priorisée au détriment du droit à la vie privée.

La prise en compte de cet état de fait nous amène à nous orienter vers le protocole Bitcoin [12]. Ce dernier est un système de cash électronique où une pièce de monnaie y est définie comme une chaîne de signatures électroniques. Ce principe permet de suivre facilement les mouvements des pièces électroniques et répond au besoin de la LAB-FT. Cependant, à l'heure actuelle, la réalisation d'une transaction sur ce protocole est identificante et donc en rupture avec le secret médical si elle venait à être réalisée en règlement des soins. Notons, enfin, qu'il faut prendre aussi en compte que cet environnement reste limité en nombre de transactions par seconde.

Nous proposons donc la mise en place d'un serveur d'horodatage latéral à bitcoin, communément appelé *sidechain*, de tel sorte à profiter des bienfaits de la résilience de son réseau. Cette mise en place permet de résoudre la problématique de LAB-FT en concentrant les acteurs de surveillance sur les flux entrant et sortant de la sidechain.

Si les flux entrant et sortant sont contrôlés, alors les échanges internes à la sidechain peuvent y être plus confidentiels.

Des échanges de valeurs publiques mais plus confidentiels et contenus entre les acteurs de soins permettent de garantir le secret médical.

Pour cette solution nous utiliserons en initial les outils et services proposés par Blockstream dans le cadre de la création du Liquid network [13] ce qui permet un volume d'échanges anonymes suffisants en termes de nombre de transactions par seconde.

Nous noterons que des solution comme Taproot [14] pourraient changer la vision de la sécurité du secret médical sur les protocoles publiques mais pouvant poser une problématique au niveau de la LAB-FT. S'il existe d'autres structures d'horodatage capables d'accueillir l'écosystème, le choix technologique initial, que nous proposons, repose sur la résilience aux attaques du protocle de Nakamoto [12] et une confidentialité par défaut via la plateforme Elements [15]. Enfin, la possibilité de déployer des contrats-intelligents dont les résultats sont de confiance via simplicity [16] est un atout sécurisant.

Les briques technologiques pour répondre aux besoins de stockage et de sécurisation étant identifiés, il convient d'établir les règles initiales du consensus social.

8 Le Réseau

8.1 Les Noeuds

Les nœuds participent au stockage décentralisé et valident les transactions. Les frais associés aux transactions viennent rémunérer le travail des noeuds.

Les nœuds peuvent rejoindre et quitter le réseau à tout moment. Pour devenir nœuds de réseau il est nécessaire de réaliser un séquestre d'une valeur en bitcoin dont le montant sera précisé ultérieurement. Le séquestre est réalisé via une adresse multi-signature gérée par la gouvernance.

Quitter le réseau revient à demander la libération du séquestre. La demande de libération se fait auprès de la gouvernance du réseau. La libération du séquestre s'opère après transfert sur un autre nœud du réseau des données stockées sur le nœud sortant.

8.2 La Gouvernance

Si tout le monde est libre de participer ou non au réseau, la participation à la gouvernance exige une preuve d'intérêt.Les nœuds de gouvernance sont des nœuds de réseau ayant fait preuve d'intérêt à gouverner. Ces preuves d'intérêts sont souvent matérialisées par un jeton de gouvernance. Il nous est apparu que les fonctionnalités des blockchains résolvent le besoin de création d'un nouveau jeton sans compromettre l'intérêt secondaire de revente de ses droits.

Ensuite, le niveau de décentralisation est un élément important de la robustesse d'un réseau. Il est donc nécessaire de mettre en place des solutions qui limitent la création de nœuds par personne tout en s'assurant que le possesseur du nœud est bien humain. Et si l'intérêt est de maximiser le niveau de décentralisation, alors une incitation à gouverner doit être mise en place.

Enfin, la gouvernance doit pouvoir s'opérer par le vote de motions libres de dépôt. La gouvernance doit pouvoir répondre à un besoin de vote de motion qui pourrait être élevées et ou urgentes. Si l'on admet, de fait, qu'il existe chez les votants des groupes minoritaires et majoritaires, le vote 1 pour 1 devient inopérant pour un choix de bien commun. Il est alors nécessaire de permettre la pondération du vote en fonction de l'importance qu'il revêt pour chacun.

Nous proposons la mise en place d'une preuve de sens pour les mises en route de nœuds et lors des votes. La preuve de sens se pose comme un test requis pour différencier les utilisateurs humains d'éventuels robots malveillants réduisant les risques de centralisation et de la profitabilité d'une attaque sybile. La preuve de sens assure qu'un humain vote les motions et permet d'assurer également un niveau de décentralisation [17].

Nous proposons qu'un second séquestre soit nécessaire pour participer à la gouvernance du réseau. Cette sollicitation engendre des frais et ces frais viennent financer le développement du réseau. En plus du droit de vote, les nœuds de gouvernance bénéficient d'une prime supplémentaire qui s'ajoute aux récompenses pour le travail de stockage et de validation des transactions. Cette prime supplémentaire vient couvrir, à terme, les frais de participation à la gouvernance. Cette prime est définie comme un pourcentage pris sur toutes les valeurs venant en paiement des indemnités d'accès aux données des patients. Cette prime est

donc à la charge de tout tiers sollicitant le réseau de données de santé.

Nous proposons la mise en place du vote quadratique [18], qui permet de défendre ses convictions face à une majorité, dans le cadre d'une démocratie liquide [19] ou la délégation de vote est possible.

A date de maturité, c'est-à-dire au moment où les créateurs du réseau se retirent de la gouvernance ou dans un maximum de 5 ans, la gouvernance pourra modifier ou non les modalités de preuve d'intérêt à sa convenance.

Nous avons proposé une gouvernance, mais l'aspect décentralisé d'un environnement de santé n'assure pas le financement de l'accès aux soins.

9 Financement de l'accès aux soins

Ici il n'est question que des capacités financières des patients eux-mêmes et non des institutions de soins. Ces dernières sont invitées à manifester leur intérêt à participer à la gouvernance.

Nous savons que les données de santé ont une valeur marchande et sont, après traitement, une source de revenus importante pour la recherche médicale, le marché des dispositifs médicaux ou encore l'intelligence artificielle (IA) grande consommatrice de données.

Nous savons aussi que la publicité ciblée est un outil performant pour les entreprises car elle permet une meilleure expérience d'achat, des messages plus pertinents, plus adaptés aux intérêts de leurs cibles, des conversions en ventes plus grandes et donc un produit publicitaire de plus grande valeur.

Le besoin consiste donc à redistribuer équitablement et sans intermédiaire, les indemnités d'accès aux données de santé et de générer des revenus supplémentaires permis par un don d'attention des patients.

Nous proposons que chaque patient puisse librement (après consentement) permettre l'accès aux traitements de ses données de santé et que dans la mesure du possible les données de santé ne soient pas communiquées à un tiers. Tout besoin d'accès aux données de santé, hormis celui du patient, nécessite le paiement d'une indemnité aux patients.

Nous proposons que les publicitaires opèrent des modalités similaires à la recherche médicale. Les publicitaires pré-publient leurs produits publicitaires sur un espace dédié, règlent les frais de publication à la gouvernance. Les frais de publication comprennent la rémunération de l'attention des patients ainsi que les frais de réseau et de gouvernance. Cette dernière valide alors la publication. Un patient identifie ses besoins et préférences sur une application fonctionnant sur le réseau. Ses préférences sont stockées au même titre que des données de santé. L'application interroge les nouvelles entrées publicitaires. Si une entrée correspond aux indications de besoins ou de préférences, le patient est notifié et peut consulter la publicité. Le patient est alors gratifié par l'annonceur en sus de toute promotion incluse dans la publicité.

Les moyens de financements étant établis, il est nécessaire de poser les principes économiques généraux.

10 Principes Economiques généraux

Une économie structurée latéralement à une monnaie suppose d'avoir des principes économiques venant en soutien de cette monnaie.

Les acteurs de soins et les nœuds de réseau ne présentent pas les mêmes attentes et l'acceptation ou non de la volatilité d'une cryptomonnaie peut être un point de friction. Certaines prédictions donnent une stabilisation du cours du bitcoin après émission de la dernière prime de résultat, aux alentours de l'année 2140. A l'échelle d'une vie humaine, il ne semblerait pas déontologique d'attendre une stabilisation pour favoriser l'accès aux soins, qu'elle soit proche ou lointaine.

Ensuite la croissance du nombre d'actifs stables montre, par leurs volumes d'échanges, et en tout état de cause, un aspect cognitivement écologique et rassurant. Dès lors, établir une stabilité relative à partir d'un actif volatile (par rapport à un actif fiat dit stable) demande de réaliser une collatéralisation et d'exclure tout principe de réserve fractionnaire. Cependant l'émission d'un actif stable ne résout pas la problématique de thésaurisation (principe d'accumulation de valeur en dehors du circuit économique) qui lui diminue la vélocité d'une monnaie (principe de circulation par unité de temps). Cette vélocité est un élément d'appréciation du dynamisme économique. En termes de santé, la vélocité pourrait devenir un indicateur particulièrement important. Plus la vélocité serait importante, plus elle indiquerait que l'accès aux soins est performant. Si l'on s'intéresse aux expérimentations d'accélération de la vélocité d'une monnaie, Gesell avec son principe de monnaie fondante [20] à montré qu'il tendait à rendre le phénomène de thésaurisation inefficace, sans distinction de richesse et tout en augmentant la vélocité des actifs.

Le besoin consiste donc à obtenir, uniquement pour les acteurs de soins, une stabilité de la valeur détenue, anticipant la stabilisation du sous-jacent, ainsi qu'un principe orientant la valeur plus rapidement vers les soins.

Nous proposons que les demandes de données ou d'actes promotionnels soient réglées à la gouvernance exclusivement en bitcoin. Ce règlement comprend :

- Les frais de transaction au bénéfice du nœud validateur.
- L'alimentation d'un collatéral.
- Les primes des nœuds de gouvernance.
- Le financement des droits d'accès aux données ou l'attention des patients.

Nous proposons que pour toute valeur entrante en collatérale, un équivalent en valeur stable soit transmis aux patients et exécuté par les nœuds. La valeur stable transmise à un patient est dépendante de la zone géographique optimale (dollars, euro, etc. . .) définie par le patient. Cette valeur stable suit alors l'indice de rebasage de sa zone [10.1]. Cette indice de rebasage est supprimé dès lors qu'il est égal à la plus petite unité de monnaie de cette zone.

Nous proposons la mise en place d'une fonte monétaire [10.2] (perte de valeur dans le temps) des adresses de portefeuille (des acteurs de soins) qui réceptionne les valeurs provenant d'une indemnité d'accès aux données ou provenant du don d'attention. La fonte vient alimenter la collatéralisation et les primes de gouvernance. La fonte est calculée par les validateurs si et seulement si aucune action en faveur des soins n'est réalisée dans un temps imparti.

Les expérimentations montrent aussi que l'intérêt d'une monnaie fondante n'existe que si l'actif est liquide. Et nous savons que, actuellement, l'acceptation des cryptomonnaies par les entreprises proposant des produits et services croît moins rapidement que leurs intérêts spéculatifs ou d'actif de réserve. Le besoin consiste alors à favoriser la liquidité de l'actif.

Nous proposons que l'écosystème se dote de produits ou services de soins acceptant cette monnaie dès son lancement. Les produits ou services mis en place au lancement proposeront, au même titre que l'écosystème, une gouvernance communautaire, et viendront soutenir l'économie de l'écosystème tout en interagissant avec le monde extérieur à l'écosystème.

10.1 Rebasage

Le rebasage [21] est le principe d'établir une valeur stable de telle sorte que la valeur détenue à T0 soit équivalente à la valeur détenue à T1. Pour se faire le système propose un indice de rebasage correspondant au taux de change moyen obtenu auprès d'un d'oracle décentralisé.

Se posent les problématiques de l'indexation, la valeur cible de l'unité monétaire (dollars, euros, yen, etc...) ainsi que la méthode de rebasage définie.

Nous définissons l'indice de rebasage comme moyenne des prix de vente de bitcoin sur les marchés des zones géographiques optimales. L'indice est mis à jour à chaque nouveau bloc par les validateurs via les informations provenant des oracles.

Nous définissons que chaque valeur unitaire cible comme égale à la valeur unitaire en monnaie fiat de la zone monétaire optimale concernée. Pour la zone dollars la valeur unitaire sera le dollars US. Pour la zone euro la valeur unitaire sera l'euro, etc.

Nous définissons la méthode de détermination de l'indice de rebasage comme le rapport entre la capitalisation à Tn+1 et Tn bloc de la chaine latérale. Si la capitalisation à augmenter de 8% entre T0 et T1 l'indice de rebasage est de 1.08. Si entre T1 et T2 une diminution de 3.85% s'est produite, l'indice de rebasage devient de 1.03842, etc.

La valeur stable présente l'expression suivante :

$$AS = SAT/IR \tag{1}$$

AS = Actifs Stable,
SAT = 1 Satoshi,
IR = Indice de Rebasage.

Le rebasage offre la stabilité rassurante recherchée mais il convient d'inviter aux échanges.

10.2 Fonte monétaire

Les adresses portefeuilles des acteurs de soins présentent une stabilité en valeur de zone géographique optimale dès lors qu'une action en faveur des soins est réalisée. Si un portefeuille est sans activité sur une période équivalente à un trimestre, une fonte de la valeur de 0.5% par semaine est calculée par le nœud validateur.

Nous définissons une action en faveur des soins le fait de réaliser un échange de valeurs entre patient et professionnel de santé ou la réalisation d'une transaction en faveur de l'acquisition d'un produit ou service de soins immédiat ou futur.

Si nous émettons l'hypothèse que la valeur perçue par les patients est conséquente dès la mise en route de l'écosystème, l'incitation produite par la fonte monétaire pourrait produire l'effet indésirable de surconsommation de soins et notamment une surconsommation de consultations médicales dans une démographie médicale en baisse.

Si la fonte monétaire invite à la circulation de la monnaie, il est nécessaire d'inviter à ce que les dépenses soient aussi à destination de soins futurs. Il est donc impératif de proposer un investissement de soins à long terme.

10.3 Investissement de santé

La prévention en santé se définit par l'action de se préserver d'une situation pouvant occasionner un risque de santé.

Si les systèmes financiers bancaires suivent le principe de réserve fractionnaire pour se financer, les assurances santé, elles, établissent des réserves qui suivent les performances de leurs investissements boursiers ayant pour effet leur exposition au risque de crise systémique.

Dès lors le besoin se traduit pour un patient d'avoir l'assurance de soins futurs en dehors des marchés financiers.

Par ailleurs, les assurances santé actuelles sont limitées, elles restent des investissements à perte pour le patient tant que le besoin de soins n'est pas présent, elles ne génèrent aucun intérêt sur les sommes déposées, elles sont très peu modulaires et le capital investi est très peu reportable d'une année sur l'autre et surtout immobilisé.

Il convient donc de permettre que cet investissement devienne générateur d'intérêt tant qu'il n'est pas dépensé, qu'il soit mobilisable à tout moment, qu'il soit modulaire à souhait en fonction de ses besoins de soins (dentaires, optiques, etc.).

Nous proposons que le capital investi par les patients pour leurs soins futurs soient générateurs d'intérêts. Ses intérêts proviennent :

- Soit de la mise à disposition de ses fonds pour des prêts et des assurances envers d'autres acteurs de soins. Le risque est contenu par le transfert des droits de contrôle d'accès aux données du demandeur

vers le prêteur ainsi que l'orientation des valeurs perçues pour le don d'attention vers le prêteur. Procédé qui court jusqu'à remboursement du financement octroyé. A échéance, le tiers demandeur récupère l'ensemble de ses droits.

• Soit par mise à disposition des fonds en collatérales pour des prêts flash sur les marchés financiers.

Les taux d'intérêts sont votés par la communauté trimestriellement. Le capital investi est transmissible à des ayants droits définis par le patient tant qu'une créance n'est pas en cours. A l'échéance d'une créance, les ayant droits définis récupèrent leurs capacités d'ayant droit.

Cette gestion assurantielle est permise par des smart-contrat et a pour bénéfice de stopper la fonte monétaire. Par ailleurs, elle assure une visibilité sur la demande de produits et services de soins. Ce qui permet une meilleure anticipation de production pour ces fournisseurs.

Nous avons assuré les valeurs d'échanges, invité aux échanges à destination de soins dans un fonctionnement d'assurance santé, mais il convient de rendre l'actif liquide, c'est-à-dire qu'il soit accepté en échange de produits et services de soins en dehors des professionnels de santé.

10.4 Produits et services de soins à gouvernance communautaire

Les fournisseurs de services et de produits de soins sont des acteurs incontournables.

Et si l'on admet que l'accessibilité aux soins est du ressort de tous, alors il convient que les produits et services de soins de l'écosystème soient des propositions des acteurs de l'écosystème, pour les acteurs de l'écosystème par les acteurs de l'écosystème.

Nous proposons la mise en place de services et produits de soins à gouvernance communautaire favorisant l'accès aux soins sans limitation d'évolution hors écosystème.

Si l'on traduit l'accessibilité aux soins, en premier lieu, en termes de services, naturellement un service de prise de rendez-vous en ligne doit être proposé et gratuit pour tous (patients et professionnels de santé).

Nous proposons le service, en cours de création, du nom de **Heallers** . **Heallers** permettra la prise de rendez-vous en ligne, l'ensemble des services de e-santé comme la téléconsultation ainsi qu'un point d'information à destination des patients utilisable par les institutions.

Si l'on traduit l'accessibilité aux soins en termes de dispositifs médicaux quotidiennement utilisés et non soumis à certaines contraintes de classification, il nous est apparu que 7 personnes sur 10 portent un équipement optique.

Nous proposons la solution **EyeEarth** , en cours de création. **EyeEarth** fabrique des équipements optiques de vue et solaire respectueux de l'environnement par revalorisation des déchets (marc de café, algues vertes, etc.)

Nous proposons donc, dès la mise en route du réseau, des produits et servcices de soins.

11 Conclusion

Nous avons proposé un écosystème de santé décentralisé résolvant la problématique de l'accès aux soins.

Nous avons tout d'abord proposé un système de stockage décentralisé et sécurisé de données de santé. Cette structure reste incomplète pour garantir le secret médical. Nous avons alors proposé un serveur d'horodatage latéral qui offre une sécurisation du secret médical. Les deux systèmes ainsi définis n'assurent pas un niveau de décentralisation nécessaire et suffisant. Nous avons donc proposé une gouvernance communautaire résolvant la problématique du niveau de décentralisation. Le système ainsi décentralisé n'assure pas le financement de l'accès aux soins. Nous avons proposé une méthode sécurisante de valorisation des données anonymisées et de l'attention. Les moyens de financements initiaux établis, nous avons proposé les principes économiques généraux définissant l'économie de l'écosystème. Enfin nous avons proposé une solution pour rendre liquide et à destination des soins les échanges de valeurs résolvant la problématique de l'accès aux soins.

References

[1] WHO World Health Organization. *The Global Health Observatory.* World Health Data Platform, 2020.

[2] OECD Organization for Economic Co-operation and Development. *Healthcare costs unsustainable in advanced economies without reform.* Organization for Economic Co-operation and Development, 2015.

[3] DREES Direction de la Recherche des Études de l'Évaluation et des Statistiques. *Comparaisons internationales des médecins.* Direction de la Recherche, des Études, de l'Évaluation et des Statistiques, 2017.

[4] United Nation. *Universal Declaration of Human Rights.* United Nations General Assembly resolution 217 A, 1948.

[5] Dacher Keltner. *The Power Paradox: How We Gain and Lose Influence.* Penguin Press, 2016.

[6] Yehuda Lindell. *Secure Multiparty Computation for Privacy Preserving Data Mining.* Journal of Privacy and Confidentiality, 2009.

[7] Gordon Moore. *Moore's law.* Electronics Magazine Vol. 38, No. 8, 1965.

[8] Foldingathome.org. *Foldingathome.* Foldingathome.org, 2000.

[9] Luc Rocher Julien M. Hendrickx et Yves-Alexandre de Montjoye. *Estimating the success of re-identifications in incomplete datasets using generative models.* Nat Commun 10, 3069, 2019.

[10] Juan Benet. *IPFS - Content Addressed, Versioned, P2P File System.* Protocol labs, 2014.

[11] Sutula Hagopian Gozalishvili Hill And Pick, Farmer. *A protocol event-sourced database for decentralized user-siloed data.* Textile.io, 2019.

[12] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* San Val, 2009.

[13] Blockstream Corporation. *Liquid Network.* Blockcstream Corporation, 2018.

[14] Gregory Maxwell. *Taproot: Privacy preserving switchable scripting.* Bitcoin-dev Linux Foundation, 2018.

[15] Elements community. *Elements Project blockchain platform.* Elements community, 2015.

[16] Russell O'Connor. *Simplicity: A New Language for Blockchains.* Proceedings of the 2017 Workshop on Programming Languages and Analysis for Security. ACM, New York, NY, USA, 2017.

[17] Idena Network. *flip challenge.* Idena.io, 2020.

[18] Vitalik Buterin and Glen Weyl. *Liberation Through Radical Decentralization.* medium, 2018.

[19] Alois Paulin. *Ten years of liquid democracy research an overview.* Central and Eastern European EDem and EGov Days 338 (July):455-66, 2020.

[20] Jérôme Blanc. *Silvio Gesell's theory and accelerated money experiments.* ffhalshs-00119192, 1998.

[21] Ferdinando M. Ametrano. *Hayek Money: The Cryptocurrency Price Stability Solution.* SSRN, 2014.