

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA – INSA LYON
DEPARTEMENT INFORMATIQUE
VALPARAISO – CHILE
LYON – FRANCE



“L’UTILISATION DES TECHNOLOGIES DE LA BLOCKCHAIN POUR LA TRACABILITÉ DES MÉDICAMENTS”

JOACHIM DOREL

**MEMOIRE POUR CANDIDATER AU TITRE D’INGÉNIEUR CIVIL EN
INFORMATIQUE**

Professeur Guide : Florent De Dinechin (florent.de-dinechin@insa-lyon.fr)
Professeur Co-Référent : Omar Hasan (omar.hasan@insa-lyon.fr)

Novembre 2019

Remerciements

Merci à mes parents pour leur soutien durant mes longues années d'études,

Merci à l'INSA de Lyon à la Federico Santa Maria pour l'opportunité que ces écoles m'ont donnée afin de réaliser ce double diplôme.

Merci à Xavier Bonnaire, Erika Rosas, Florent de Dinechin et à Omar Hasan pour avoir encadré ce mémoire.

Résumé

Résumé — Ce mémoire explore l'utilisation des technologies associées à la Blockchain pour améliorer le processus de traçabilité des médicaments. Cette exploration a deux buts principaux : réaliser une analyse théorique de l'usage de la Blockchain, et réaliser l'implémentation d'une version de démonstration. L'implémentation de la solution permet de démontrer que la traçabilité des médicaments à travers une blockchain est bien plus efficace pour assurer le suivi des médicaments et la non-falsification de ceux-ci. Ce mémoire présente en plus une analyse de la chaîne d'approvisionnement de l'industrie pharmaceutique, et une modélisation de celle-ci afin de l'adapter aux besoins de la traçabilité.

Mots clés — Blockchain, Traçabilité, Sécurité, Supply Chain, Industrie Pharmaceutique

Abstract

Abstract—This thesis will explore the use of technologies associated with the Blockchain in order to improve the current process of drugs traceability. This exploration will have two main goals: analyze the theoretical use of the Blockchain for our problem and developed an implementation of a solution. The implementation of the solution will allow to prove that drugs traceability is possible through a blockchain, and that this traceability is more efficient in order to follow the drugs and to keep them safe from corruption. This memoir also presents an analysis of the pharmaceutical industry's supply chain, and a modelization of that supply chain in order to adapt the traceability to the supply chain.

Keywords— Blockchain, Traceability, Security, Supply Chain, Pharmaceutical Industry

Index du Contenu

Index des Figures	7
Introduction.....	8
Chapitre 1 : Définition du Problème	10
1.1. Marché des médicaments et contrefaçons	10
1.1.1. Un marché mondial	10
1.1.2. Conséquences économiques de la contrefaçon	10
1.1.3. L'attractif marché de la contrefaçon	11
1.1.4. Les mesures mises en place pour combattre la contrefaçon	12
1.2. Objectifs de ce mémoire	12
Chapitre 2 : Cadre Conceptuel	14
2.1. La Chaîne d'Approvisionnement de l'Industrie Pharmaceutique.....	14
2.1.1. Qu'est-ce qu'un médicament	14
2.1.2. La création d'un médicament	15
2.1.2.1. La découverte d'un nouveau médicament	15
2.1.2.2. Le développement préclinique	16
2.1.2.3. Le développement clinique	16
2.1.3. La chaîne d'approvisionnement.....	17
2.1.3.1. La chaîne d'approvisionnement de Novartis.....	18
2.1.3.1.1. Les opérations chimiques	18
2.1.3.1.2. Les opérations pharmaceutiques	18
2.1.3.1.3. Les bureaux pharmaceutiques nationaux	19
2.1.3.2. Un modèle de chaîne d'approvisionnement théorique	20
2.2. L'État Actuel de la Traçabilité dans l'Industrie Pharmaceutique.....	22
2.2.1. Analyse des Datamatrix	22
2.2.2. Analyse de la RFID.....	24
2.3. Les blockchains	26
2.3.1. Chaines, blocks et données.....	26
2.3.1.1. Les données	27
2.3.1.2. Les blocks	27
2.3.1.3. Les chaines	29
2.3.2. Le système distribué	29
2.3.2.1. Les propriétés d'un système distribué	29
2.3.2.2. Le problème des généraux byzantins.....	31
2.3.2.3. Les mécanismes de consensus	33
2.3.2.3.1. Paxos	33
2.3.2.3.2. Raft	34
2.3.2.3.3. Practical Byzantine Fault Tolerance (PBFT)	34
2.3.2.3.4. Consensus de Nakamoto	35
2.3.2.4. Le droit de vote	35
2.3.2.4.1. Preuve de travail (Proof-of-Work)	35
2.3.2.4.2. Preuve d'enjeu (Proof-of-Stake).....	36
2.3.2.4.3. Preuve d'activité (Proof-of-Activity)	36
2.3.2.4.4. Preuve de brûlage (Proof-of-Burn)	36
2.3.2.4.5. Preuve d'espace (Proof-of-Space)	36
2.3.2.4.6. Preuve de capacité (Proof-of-Capacity).....	37
2.3.2.4.7. Preuve de temps écoulé (Proof-of-Elapsed-Time)	37
2.3.2.4.8. Preuve d'autorité (Proof-of-Authority)	37
Chapitre 3 : Proposition de Solution	38

3.1. L'adaptation de la traçabilité	38
3.1.1. Datamatrix contre tags RFID	38
3.1.2. L'utilisation des datamatrix.....	39
3.2. La conservation des données	41
3.2.1. Les données des transactions	41
3.2.1.1. Les acteurs non identifiés	42
3.2.1.2. Les acteurs identifiés.....	42
3.2.1.3. Les fabricants de médicaments.....	43
3.2.2. Les données des blocks.....	43
3.2.3. Les données des médicaments	44
3.3. La blockchain et son fonctionnement	45
3.4. Récits d'utilisateurs de la solution	47
Chapitre 4 : Validation de la Solution	49
4.1. La gestion des données.....	49
4.1.1. La gestion de la base de données	49
4.1.2. La gestion de la blockchain	50
4.2. Interaction avec la base de données	51
4.3. Validation des récits d'utilisateurs	52
4.3.1. Récits d'utilisateurs des acteurs non identifiés	52
4.3.2. Récits d'utilisateurs des acteurs identifiés.....	54
4.3.3. Récits des fabricants de médicaments.....	58
4.4. Exemples de tentatives de corruption de la blockchain.....	58
4.4.1. Ajout de médicaments extérieurs par un transporteur	59
4.4.2. Modification de la quantité d'un lot	59
Chapitre 5 : Conclusion.....	60
5.1. Conclusions générales	60
5.2. Réalisation des objectifs	60
5.3. Travaux futurs	61
Bibliographie	62
Annexes.....	65
1. Exemple de blockchain	65
2. Code d'un block.....	66
3. Code de la blockchain	66

Index des Figures

FIGURE 1: LES PHASES DE LA CONCEPTION D'UN MEDICAMENT - SOURCE : GENOME RESEARCH LIMITED	17
FIGURE 2 : UN MODELE GENERIQUE DE SUPPLY CHAIN	21
FIGURE 3: EXEMPLE DE DATAMATRIX ET DES DONNEES ASSOCIEES – SOURCE : HTTPS://EC.EUROPA.EU/	24
FIGURE 4 : EXEMPLE D'UNE PUCE RFID - SOURCE : WIKIMEDIA.....	25
FIGURE 5: SCHEMA D'UNE TRANSACTION	27
FIGURE 6: EXEMPLE DE HACHAGE AVEC SHA-256	27
FIGURE 7: COMPOSITION DU HASH D'UN BLOCK SOUS FORME D'ARBRE DE MERKLE	28
FIGURE 8: COMPOSITION D'UN BLOCK	29
FIGURE 9 : SCHEMA D'UNE BLOCKCHAIN	29
FIGURE 10: REPRESENTATION DU THEOREME CAP - SOURCE : TOWARDSDATASCIENCE.COM	31
FIGURE 11: PROBLEME DES GENERAUX BYZANTINS - SOURCE : EDX.ORG	32
FIGURE 12 : SCHEMA DU FONCTIONNEMENT DU BPFT – SOURCE : EDX.ORG	35
FIGURE 13 : FLUX DES NUMEROS DE LOT	40
FIGURE 14: SCHEMA DE LA BASE DE DONNEES.....	45
FIGURE 15: ARCHITECTURE DE LA SOLUTION	47
FIGURE 16: PAGE D'INDEX	52
FIGURE 17: PAGE D'UN LOT DE MEDICAMENT, AVEC LES TRANSACTIONS DE CE LOT	53
FIGURE 18: INFORMATIONS SUR LES PROPRIETAIRES SUCCESSIFS D'UN MEDICAMENT	53
FIGURE 19: ACCEPTATION OU REFUS D'UN LOT	54
FIGURE 20: PAGE DE LOGIN.....	55
FIGURE 21: PAGE D'INSCRIPTION.....	55
FIGURE 22: BOUTON DE DECONNECTION	55
FIGURE 23: PROFIL D'UN UTILISATEUR.....	56
FIGURE 24: VISUALISATION DU STOCK D'UN UTILISATEUR	56
FIGURE 25: ENVOIE DU LOT 8 A L'ACTEUR AYANT LE NUMERO D'IDENTIFICATION 2	56
FIGURE 26: FILTRAGE DES MEDICAMENTS	57
FIGURE 27: BOUTON DE DEMANDE DE SYNCHRONISATION DE LA BLOCKCHAIN	57
FIGURE 28: DIVISION D'UN LOT EN DEUX, ET ENVOIE DE L'UN DES SOUS LOTS	57
FIGURE 29: VISUALISATION DU DATAMATRIX D'UN LOT	58
FIGURE 30: AJOUT D'UN NOUVEAU MEDICAMENT DANS LA BASE DE DONNEES.....	58
FIGURE 31: AJOUT D'UN NOUVEAU LOT DE MEDICAMENT	58

Introduction

Les médicaments sont utilisés tous les jours par des milliers de personnes. Leur utilisation présente plusieurs contextes, mais le plus important est de soigner. Pour soigner, un médicament a besoin d'être adapté à la maladie qu'un patient a. A l'origine, les médicaments étaient pour la plupart des produits naturels (des plantes, racines et autres). Mais l'arrivée de la chimie au XXème siècle a vu la création des médicaments de synthèse augmenter fortement, et l'utilisation des médicaments par l'homme augmenter en parallèle.

L'augmentation de la taille du marché des médicaments a produit le développement d'un marché de la contrefaçon parallèle : les médicaments rencontrés dans ce marché sont moins chers, mais la qualité et l'efficacité de ceux-ci sont aléatoires, voire dangereux.

Identification du Problème

La contrefaçon des médicaments présente un risque pour les consommateurs, risque potentiellement mortel. Consommer un médicament non adapté ou inefficace ne permet pas de soigner un patient, et il faudrait qu'un patient puisse, peu importe où il se procure un médicament, vérifier l'origine du médicament. En confirmant l'origine d'un médicament, le patient peut alors être assuré de ne pas mettre sa santé en danger.

Pour confirmer l'origine d'un médicament, un patient doit pouvoir identifier ce médicament et connaître les différents manipulateurs du médicament et leur localisation. L'ensemble des manipulateurs du médicament, qui font partie de la chaîne d'approvisionnement des médicaments, sont alors les clés permettant d'assurer que le médicament consommé n'a pas été, à un moment, remplacé par un médicament alternatif.

La contrefaçon des médicaments est aujourd'hui l'une des problématiques majeures de l'industrie pharmaceutique, et ce mémoire a pour but de présenter une solution à ce problème.

Objectifs

Objectif Général

Créer et développer une solution permettant de tracer des médicaments grâce à une blockchain.

Objectifs Spécifiques

- Comprendre et connaître ce qu'est une blockchain, avec le fonctionnement de celle-ci et l'utilité future de la technologie
- Analyser la chaîne d'approvisionnement de l'industrie pharmaceutique
- Développer un programme permettant d'améliorer le suivi des médicaments grâce à une blockchain

Plan du mémoire

Ce mémoire présente dans une première partie la problématique du suivi des médicaments par l'industrie pharmaceutique, et les problèmes actuels que rencontre l'industrie dans la lutte contre la contrefaçon des médicaments. Une seconde partie présente une analyse des différents thèmes centraux du mémoire : les médicaments, les blockchains et la chaîne d'approvisionnement de l'industrie pharmaceutique. La définition des thèmes centraux va permettre de connaître et de maîtriser les principales options possibles afin de résoudre la problématique du mémoire. Cette partie de définitions est ensuite suivie d'une proposition de solution basée sur ce qui a été étudié précédemment. Cette dernière partie explore les possibilités offertes actuellement par l'industrie

pharmaceutique pour le suivi des médicaments, et l'adaptation de ce suivi afin d'utiliser une blockchain. Dans une quatrième partie sera étudié la validation de cette solution, si la solution répond bien aux problématiques du mémoire et si la solution permet effectivement d'éviter la corruption de la chaîne d'approvisionnement des médicaments. Enfin, une conclusion permettra de clore le mémoire et de présenter les travaux futurs pour la solution proposée.

Le mémoire présente la structure suivante :

Chapitre 1 – Définition du Problème : Une introduction concernant la problématique de la contrefaçon des médicaments.

Chapitre 2 - Cadre Conceptuel : Une présentation des différents outils et techniques du mémoire, comme l'industrie des médicaments, le fonctionnement actuel de la traçabilité et le fonctionnement d'une blockchain.

Chapitre 3 – Proposition de Solution : La construction d'une solution permettant de résoudre le problème de suivi des médicaments grâce à une blockchain.

Chapitre 4 – Validation de la Solution : La vérification que la solution présente une solution au problème initial, et que la solution permet d'éviter la corruption de la chaîne d'approvisionnement des médicaments.

Chapitre 5 – Conclusion : Les conclusions générales du mémoire ainsi que les perspectives créées grâce à la réalisation du mémoire.

Chapitre 1 : Définition du Problème

1.1. Marché des médicaments et contrefaçons

1.1.1. Un marché mondial

La falsification et contrefaçon des médicaments est l'un des marchés illégaux les plus importants et prospères au monde : près de deux cents milliards de dollars en 2017 [3] selon l'OMS, l'Organisation Mondiale de la Santé. Les médicaments provenant de ce marché se classent en trois catégories :

- *Les médicaments de qualité inférieure*, ce sont des médicaments autorisés qui ne remplissent pas les standards de qualités ou les spécifications, ou les deux.
- *Les médicaments non-enregistrés ou sans licence* correspondent à des produits médicaux n'ayant pas été évalués ou approuvés par l'autorité nationale ou régionale d'un marché dans lequel ceux-ci sont distribués.
- *Les médicaments falsifiés* correspondent à des produits médicaux qui sont délibérément présentés sous de fausses informations pouvant concerner leur identité, leur composition ou leur source.

Les chiffres suivants permettent d'approfondir et de mieux connaître ce problème [34] :

- 10% des ventes du marché mondial des médicaments concernent des médicaments falsifiés, selon le découpage suivant :
 - 1% dans les pays développés
 - De 5 à 30% dans les pays émergents
 - Près de 70% dans certains pays d'Asie et d'Afrique

En plus de ces chiffres, on se doit aussi de souligner que 50% [7] des médicaments achetés en ligne sont falsifiés. Ces médicaments falsifiés ont des conséquences directes pour les consommateurs. Annuellement c'est près de 1 000 000 de personnes qui décèdent chaque année à cause des médicaments falsifiés. De plus la prise d'un médicament non adapté pour les patients entraîne surdosage ou sous-dosage d'un médicament, utilisation de molécule ou principe actif différent, excipients dangereux, présence dans le médicament d'autres molécules, des risques d'interactions du médicament falsifié avec d'autres médicaments ou molécules, ou un médicament n'ayant aucun effet pour améliorer la santé du patient, cela ayant des conséquences graves pour le patient, en empirant potentiellement l'état de celui-ci.

1.1.2. Conséquences économiques de la contrefaçon

La falsification de médicaments a aussi des conséquences économiques importantes [18]. Les laboratoires pharmaceutiques investissent des sommes énormes dans l'objectif de développer des nouveaux médicaments, et la contrefaçon de ceux-ci réduit le retour sur investissement des laboratoires.

Si une entreprise doit investir des millions pour le développement d'un médicament, celle-ci va chercher, une fois le médicament développé et prêt à être commercialisé, à être rentable par rapport aux coûts de recherche, de production et de commercialisation. Les laboratoires et entreprises pharmaceutiques vont en conséquence concentrer la recherche de nouveaux médicaments sur les médicaments « grand public », ayant potentiellement de nombreux consommateurs, réduisant ainsi le risque de manque de rentabilité, et délaissant des maladies plus rares dont le traitement serait moins rentable.

1.1.3. L'attractif marché de la contrefaçon

Pour les entreprises et individus produisant ou commercialisant des médicaments contrefaits, il existe de multiples motivations. Le trafic de médicaments contrefaits est 10 à 25 fois plus rentable que le trafic de produits stupéfiants (celui de cannabis par exemple) par rapport au coût d'investissement initial [31]. De plus, l'augmentation des achats sur des boutiques en ligne (comme Amazon ou EBay) et la croissance du e-commerce depuis les années 90 font que beaucoup de personnes ont l'habitude d'acheter en ligne. Or, près de 50% des médicaments achetés en ligne sont contrefaits. Enfin, les inégalités concernant l'accès aux médicaments : la présence ou non de subventions, sous la forme d'assurances ou de sécurités sociales, va directement influencer sur la proportion d'achats de médicaments sur des marchés parallèles.

Pour les acheteurs et consommateurs de médicaments, il existe de nombreuses raisons motivant l'achat de médicaments potentiellement douteux et difficilement traçables. Dans les pays développés, les principales raisons sont les suivantes :

- Le médicament est considéré comme tabou : par exemple, les médicaments pour perdre du poids ou contre l'impuissance sexuelle
- Le médicament est cher, et passer par des circuits alternatifs pour acheter un médicament qui semble être le même permet d'acquérir, ou de penser acquérir, celui-ci à un prix plus faible
- Le médicament est seulement disponible avec une ordonnance, comme par exemple les médicaments permettant de lutter contre l'insomnie
- Le médicament permet d'améliorer ses performances, mais sa vente légale n'a pas cet objectif, et il est principalement prescrit pour d'autres troubles : on retrouve dans cette catégorie les anabolisants, les hormones et les médicaments permettant d'augmenter sa concentration
- Le médicament n'est pas légal dans certains pays, mais l'est dans d'autres. Par exemple les médicaments permettant d'avorter (le misoprostol et la mifépristone) sont légaux dans de nombreux pays, mais tout à fait illégaux dans d'autres
- Le médicament n'a aucune valeur scientifique, comme certaines pastilles pour la gorge présentes sur les marchés au Chili.

En plus de l'ensemble de ces raisons globales, il existe d'autres justifications dans les pays en voie de développement expliquant le phénomène :

- Les médicaments de base sont falsifiés, comme par exemple les antibiotiques, les médicaments anti-malaria ou les antiparasites.
- Les organismes de contrôle sont inefficaces, et donc effectuent trop peu de contrôles sur les médicaments pour permettre de s'assurer que les médicaments vendus sur un territoire sont bien les bons
- Les systèmes de santé sont inefficaces, et donc le seul moyen d'acquérir certains médicaments est de passer par des marchés parallèles
- Les pénuries de certains médicaments, dont parfois des médicaments de bases sont régulières [34]
- La pauvreté de certaines personnes les pousse à chercher des médicaments toujours moins chers
- La corruption d'une partie des élites empêche de mettre en place un circuit de distribution de qualité, et pousse donc les consommateurs à passer par un circuit de distribution parallèle

La taille et l'importance du marché des médicaments falsifiés sont dues à la fois à des raisons économiques, mais aussi à des raisons d'approvisionnements, de gestions ou la stabilité de certains pays.

1.1.4. Les mesures mises en place pour combattre la contrefaçon

Pour combattre les problèmes de falsifications de médicaments, il existe des technologies et des méthodes pour compenser certains de ces problèmes :

- La mise en place d'une traçabilité du médicament, afin de faire connaître l'ensemble du processus de production et de distribution au consommateur final. En Europe, l'usage de datamatrix est obligatoire depuis le 9 février 2019 [36]. Ceux-ci ont permis de renforcer la traçabilité des médicaments, mais ils sont encore perfectibles. Plus loin dans ce mémoire il y aura une analyse de ceux-ci.
- Le contrôle en laboratoire de certains lots afin de s'assurer que le médicament vendu correspond bien au médicament dans la boîte. Cette méthode, bien qu'extrêmement efficace, est impossible à mettre en place à grande échelle, de par son coût et sa vitesse.

Plus globalement, la lutte contre la falsification des médicaments implique que les pays établissent une plus importante surveillance de ce qui rentre ou sort du pays, et cela avec l'action des douanes principalement. Il existe aussi *International Medical Products Anti-Counterfeiting Taskforce (IMPACT)*, une équipe internationale formée par l'OMS afin de lutter contre la falsification de médicaments, et qui collabore avec les douanes de nombreux pays et d'autres associations internationales afin d'étendre l'impact de sa lutte. Les membres d'IMPACT travaillent notamment à aider les pays à renforcer leurs systèmes de détection et de répression, et aident l'industrie pharmaceutique afin de mettre au point des mesures internationales de lutte contre la contrefaçon de médicaments [15]. Preuve de l'importance du sujet, depuis 2013 l'université Panthéon-Assas à Paris propose un « diplôme d'université criminalité pharmaceutique », permettant de connaître les lois et les procédures pour lutter contre la criminalité pharmaceutique¹.

Dans le secteur médical il existe aujourd'hui de plus en plus de produits à suivre, que ce soit les médicaments génériques vendus en pharmacie ou la prothèse de hanche utilisée en salle de chirurgie d'un hôpital. L'ensemble des chaînes d'approvisionnements de l'industrie doit donc être sécurisé en utilisant un maximum d'outils. Les technologies actuelles devraient permettre d'améliorer grandement la traçabilité de ces produits. Ce mémoire s'appuie sur une technologie récente (la blockchain), et propose une solution aux problèmes de traçabilité des médicaments.

1.2. Objectifs de ce mémoire

L'industrie pharmaceutique nécessite donc, d'une part pour sa stabilité économique à long terme, et d'autre part pour garantir une confiance des consommateurs envers l'ensemble de l'industrie, de mettre à jour ses normes et ses pratiques afin de lutter contre la falsification de médicaments dans l'ensemble du globe. Lutter contre la falsification peut aussi permettre aux entreprises du secteur de se dédommager en cas de problèmes ou d'introduction de médicaments frauduleux dans leurs chaînes d'approvisionnement. Ce mémoire s'adresse principalement aux médicaments, mais l'ensemble des outils du secteur médical devrait être tracés d'une meilleure façon globalement, du médicament à la prothèse cardiaque, cette traçabilité permettant au consommateur d'avoir un meilleur aperçu, et donc une meilleure connaissance, de ce qu'il va mettre dans son corps. Offrir la possibilité aux consommateurs de connaître l'origine des médicaments qu'ils achètent et

¹ <https://www.u-paris2.fr/fr/formations/offre-de-formation/diplome-duniversite-du/diplome-duniversite-criminalite-pharmaceutique>

consomment pourraient offrir aux pharmacies en ligne une réelle légitimité, grâce à la garantie auprès des consommateurs sur ce qu'ils achètent.

Ce mémoire possède deux objectifs principaux tournant tous les deux autour d'une blockchain, et de l'implémentation de celle-ci. Le premier objectif, qui est un objectif intermédiaire, est d'explorer les possibilités qu'offre les blockchains afin d'améliorer la traçabilité des médicaments, et plus largement les possibilités des blockchains dans le cadre des chaîne d'approvisionnement. Un second objectif est de développer une *proof of concept* permettant de démontrer une solution, avec l'intérêt potentiel de cette solution pour l'industrie pharmaceutique, et les limites de la solution. Ces deux objectifs globaux sont ensuite découpés en plusieurs parties afin de mieux comprendre les choix techniques proposés dans ce mémoire.

Chapitre 2 : Cadre Conceptuel

Dans le cadre du développement d'une nouvelle solution pour assurer une meilleure traçabilité des médicaments, il convient d'en savoir un peu plus sur la traçabilité actuelle des médicaments, la chaîne d'approvisionnement de l'industrie pharmaceutique, et sur les blockchains. L'exploration de comment ces différentes parties se rencontrent permettra de proposer une solution conceptuelle dans la prochaine partie.

Ces trois thèmes distincts que sont la traçabilité des médicaments, la chaîne d'approvisionnement de l'industrie pharmaceutique et les blockchains forment les trois branches principales de cette partie. La traçabilité des médicaments l'est car il nous faut en apprendre plus sur le système actuellement en place afin de découvrir ses différentes faiblesses, et donc de mettre en avant certains points d'améliorations. L'étude des chaînes d'approvisionnement doit permettre de comprendre les différents flux pour produire des médicaments et les distribuer, et d'en savoir plus sur ce qu'est un médicament. Enfin, l'étude des blockchains et des différentes possibilités associées à celles-ci vont permettre de clarifier leurs usages potentiels et d'ouvrir sur une proposition conceptuelle de l'utilisation de celles-ci.

2.1. La Chaîne d'Approvisionnement de l'Industrie Pharmaceutique

L'ensemble des flux de médicaments de l'industrie pharmaceutique passe par une chaîne d'approvisionnement. Dans le cadre de la recherche de l'amélioration de celle-ci, analyser et comprendre cette chaîne d'approvisionnement est primordial, celle-ci ayant un lien direct avec la traçabilité des médicaments. C'est l'analyse de la chaîne d'approvisionnement de Novartis qui va permettre d'identifier les acteurs et les flux clés. L'identification de ses acteurs et flux permettra ensuite de construire et de développer un modèle de chaîne d'approvisionnement générique. Un second objectif de cette analyse est de permettre d'identifier les moments clés lors desquels la traçabilité des médicaments est mise en place, et donc lors desquels la solution présentée aura à intervenir dans la chaîne d'approvisionnement. Ces moments clés vont permettre de comprendre quand les nouveaux processus de sécurisation dépendant d'une blockchain pourront être mis en place.

2.1.1. Qu'est-ce qu'un médicament

Pour mieux comprendre le cœur de ce mémoire, il est important de définir les fondamentaux de ce qu'est un médicament, et de comprendre comment sont fabriqués et de quoi sont composés ceux-ci. En dehors de la pastille, sirop ou crème acheté en magasin, les consommateurs en connaissent très peu sur les médicaments. Simplement, et en une simple équation, un médicament est [9]:

$$\text{Médicament} = \text{Principe Actif} + \text{Excipients}$$

Le principe actif correspond à la molécule permettant de supporter l'activité pharmacologique (la "molécule active"), et les excipients correspondent aux différents produits permettant de donner sa forme au médicament (un sirop, un gel, une pastille...), de doser le principe actif, d'aider la digestion du principe actif, de faciliter la production du médicament, de protéger le principe actif de l'environnement extérieur (une capsule par exemple, contenant une poudre à l'intérieur), ou d'aider les patients à "accepter" plus facilement le médicament (ajout d'un goût, d'une couleur, d'une texture). Il faut aussi noter que le principe actif tout comme les excipients sont composés d'un ensemble de matière première. Ces matières premières peuvent être organiques ou chimiques.

Les matières premières organiques, bien que souvent modelées de façon chimique, tracent leurs origines des plantes médicinales. Et quand la fragilité de l'écosystème d'une plante médicinale ne peut garantir le besoin et le volume de production d'un médicament, les chimistes doivent alors

développer des alternatives : c'est par exemple le cas de l'if de l'Ouest, ou if du Pacifique (*Taxus brevifolia*), un conifère utilisé en médecine parce qu'il contient du paclitaxel, une substance permettant de traiter les cancers du poumon, de l'ovaire et du sein. Lors de la découverte de cette substance dans les années 1960, la surexploitation des ifs a causé un déclin de leur population, et des protestations du public. La méthode utilisée à l'époque pour obtenir du paclitaxel laissait les arbres morts, et les chimistes ont dû développer une alternative. Aujourd'hui, le paclitaxel est développé en laboratoire à l'aide de résine présente dans les branches et les aiguilles d'ifs communs européens, et la résine est ensuite modifiée et cultivée grâce à la fermentation cellulaire. Ce processus de fabrication est durable et permet de ne pas laisser d'arbres morts [39].

D'un point de vue plus législatif, les médicaments sont aussi encadrés par un ensemble de lois et de règles. En France, c'est l'article L5111-1 qui se charge de définir ce qu'est un médicament [23]:

On entend par médicament toute substance ou composition présentée comme possédant des propriétés curatives ou préventives à l'égard des maladies humaines ou animales, ainsi que toute substance ou composition pouvant être utilisée chez l'homme ou chez l'animal ou pouvant leur être administrée, en vue d'établir un diagnostic médical ou de restaurer, corriger ou modifier leurs fonctions physiologiques en exerçant une action pharmacologique, immunologique ou métabolique.

Cette définition de ce qu'est un médicament permet en plus de mettre en avant le fait que les médicaments et leurs usages, sont et restent encadrés. Leur commercialisation, distribution, consommation sont donc des éléments clefs des systèmes de santé actuels.

2.1.2. La création d'un médicament

Certains médicaments sont découverts par accident, comme par exemple la pénicilline par Alexander Fleming en 1928 (cette découverte lui a valu de partager le prix Nobel de médecine en 1945 avec Howard Walter Florey et Ernst Boris Chain) [28]. Mais plus généralement, et encore plus aujourd'hui avec les géants pharmaceutiques dominant très largement l'industrie, il faut des millions, voir dans certains cas des milliards de dollars afin de développer un médicament ayant une autorisation de mise sur le marché et des propriétés médicinales spécifiques.

2.1.2.1. La découverte d'un nouveau médicament

La première étape de la création d'un médicament [1] passe par la recherche de celui-ci. La durée de cette période est aléatoire, un laboratoire pouvant rencontrer très rapidement un ensemble de molécules efficaces, ou bien passer des années à réaliser des simulations afin d'obtenir un résultat performant avec une molécule cible. Cette recherche est souvent inhibée par des études de marchés. Ces études de marchés ont comme objectif d'identifier les différentes maladies qui ont besoin de médicaments, de vérifier la faisabilité de la commercialisation, et le rendement. Il existe deux procédés distincts permettant de découvrir un nouveau médicament :

- Le criblage à haut débit consiste à tester un grand nombre de molécules différentes avec un substrat donné, permettant d'identifier assez rapidement les molécules les plus efficaces, et au fur et à mesure des tests (tests sur animaux ou des cellules cultivées), isoler certaines molécules offrant des réactions aux tests.
- L'approche rationnelle consiste à développer des molécules spécifiques pour un substrat en modélisant les tests grâce à un ordinateur, et à ensuite effectuer des tests pour corroborer les modèles créés.

Ces deux procédés, bien qu'ayant des approches distinctes, permettant l'identification d'environ 250 différentes molécules potentielles qui doivent ensuite être filtrées et testées de nouveau lors du développement préclinique.

2.1.2.2. Le développement préclinique

Cette phase de développement, d'une durée entre 2 et 4 ans pour arriver à sa conclusion, a pour but de déterminer le meilleur moyen d'assurer la conception du médicament pour son usage final. Elle permet d'analyser comment le médicament est reçu par le corps, la réaction de celui-ci, comment le corps élimine le médicament, et réduire à quelques molécules candidates sur lesquelles sera basé le futur médicament commercial. Ces développements correspondent à des batteries de tests du médicament, la plupart du temps pour un meilleur ciblage d'une pathologie spécifique.

Cette phase permet également de déterminer la forme commerciale du médicament : sous forme de crème, de pilule, d'injection ou de spray. La forme du médicament n'est pas négligeable, car celle-ci a un impact direct sur l'efficacité de celui-ci, mais aussi sur la potentielle acceptation du médicament par les consommateurs (les suppositoires par exemple sont plus largement acceptés dans les pays latins).

La finalisation du développement préclinique correspond à l'approbation (ou non) du médicament par les agences sanitaires des différents pays dans lesquels l'entreprise souhaite tester son produit. Si les agences sanitaires valident l'utilité du médicament, celui entame sa phase suivante, celle du développement clinique.

2.1.2.3. Le développement clinique

Cette étape correspond aux essais cliniques sur des volontaires afin d'en apprendre plus sur le médicament, notamment son efficacité et sa sûreté. Le développement clinique d'un médicament est constitué de 5 phases : 0 (effet sur le corps), I (sûreté pour l'homme), II (efficacité à traiter la maladie visée), III (sûreté et efficacité du médicament à grande échelle) et IV (suivi continu des effets du médicaments sur les patients). L'ensemble des 4 premières phases (de 0 à III) prend entre trois et six ans avant d'arriver à sa fin.

Environ cinq molécules arrivent jusqu'au développement clinique, et de ces cinq molécules une ou deux vont jusqu'à l'autorisation de mise sur le marché. Une fois un médicament autorisé à entrer sur le marché, l'entreprise qui a développé celui-ci détient une exclusivité sur le médicament, qui lui permet de récupérer les coûts de développement. C'est après une certaine durée de commercialisation qu'un concurrent peut développer un générique du médicament, les génériques ayant la particularité globale d'avoir un prix plus faible. Cette durée est différente en fonction des pays et zones économiques : entre 5 et 12 ans aux États-Unis d'Amérique en fonction du type de médicament, 6 ans au Japon, 8 ans (avec 2 années supplémentaires d'exclusivité de mise sur le marché, et une année supplémentaire si le médicament est innovateur) en Europe [40], et 20 ans au Chili². Même après validation par les agences sanitaires, l'entreprise doit continuer de tester et de surveiller les retours des utilisateurs afin de s'assurer de la sûreté et de l'efficacité du médicament.

² <http://www.cifchile.cl/propiedad-intelectual/>

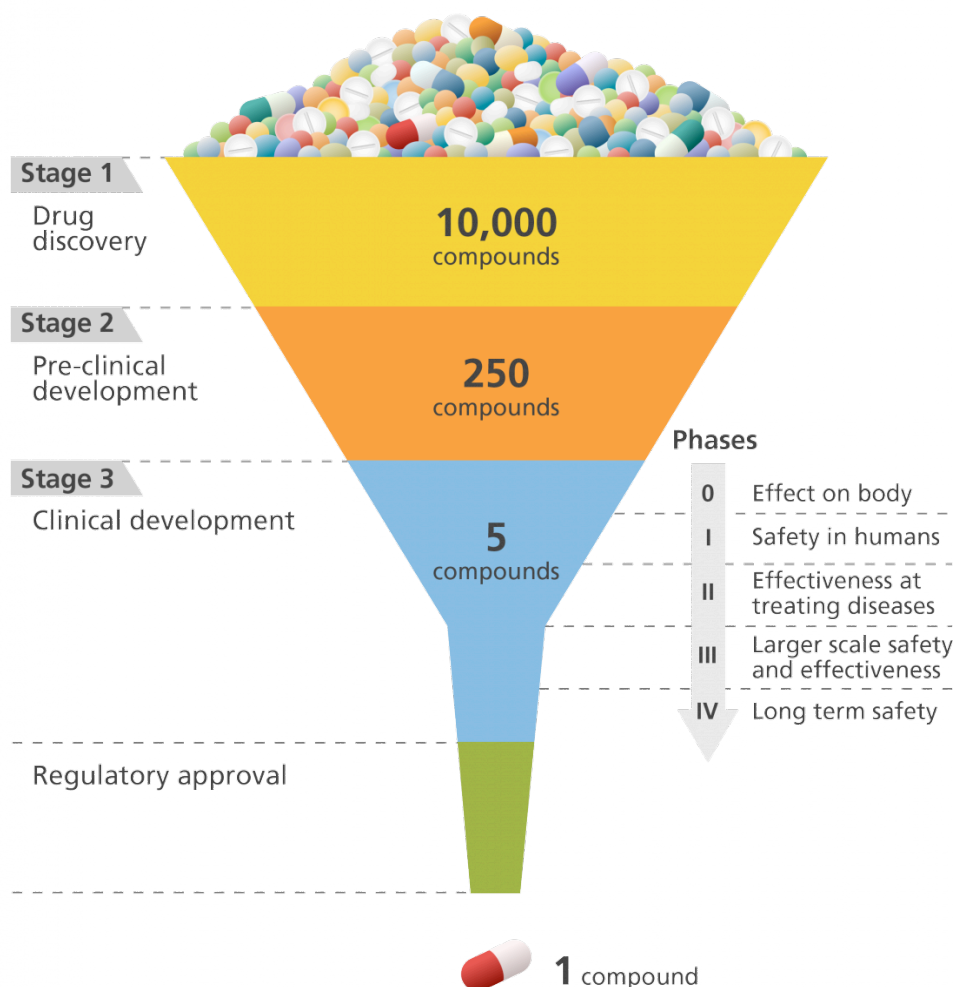


Figure 1: Les phases de la conception d'un médicament - Source : Genome Research Limited

L'autorisation de mise sur le marché d'un médicament dépend d'agences sanitaires nationales. En France, c'est l'*agence nationale de sécurité du médicament et des produits de santé* qui s'occupe d'autoriser la mise sur le marché de médicaments, tandis qu'au Chili c'est le ministère de la santé [11]. Une fois l'autorisation obtenue, le médicament peut être vendu dans l'ensemble des points de ventes autorisés.

2.1.3. La chaîne d'approvisionnement

La chaîne d'approvisionnement des médicaments est constituée de quatre étapes successives. Ces étapes se passent dans des centres à des milliers de kilomètres les uns des autres, le bon fonctionnement de la chaîne est donc primordial : un retard de livraison d'un des centres peut entraîner un retard sur l'ensemble de la chaîne de production. L'analyse de la chaîne d'approvisionnement a pour objectif de nous permettre d'identifier les étapes clés qui pourraient impacter les consommateurs, et donc celles pour lesquelles une meilleure traçabilité présente de l'importance.

Dû à l'importance dans les résultats finaux du bon fonctionnement des chaînes d'approvisionnement, la majorité des entreprises du secteur pharmaceutique essaye de garder celle-ci secrète, afin de conserver les spécificités et avantages propres à chacune d'entre elles. En revanche, il est possible de théoriser et de créer un modèle proche de l'ensemble des modèles existants, en s'inspirant de données publiques. Pour développer ce modèle, la chaîne d'approvisionnement de

Novartis va être utilisée [35]. Novartis est un groupe pharmaceutique Suisse, 4^{ème} plus gros groupe pharmaceutique en termes de revenu en 2018³ [24].

2.1.3.1. La chaîne d'approvisionnement de Novartis

Pour gérer son processus de fabrication et sa chaîne d'approvisionnement, Novartis divise ses activités en 3 subdivisions : les opérations chimiques, les opérations pharmaceutiques et les bureaux pharmaceutiques nationaux. Ces trois divisions ont chacune des objectifs indépendants dans le cadre de la production de médicaments, avec comme liens physiques entre elles des livreurs, membres de Novartis ou non. Chacune de ces subdivisions est présente dans un ensemble de pays, en plus de la Suisse où se trouve le siège de Novartis.

2.1.3.1.1. Les opérations chimiques

Les opérations chimiques, appelées *ChemOps* en interne (pour *Chemical Operations* en anglais), se chargent de transformer des matériaux initiaux purs en substances médicamenteuses. Novartis possède 4 centres dans le monde :

- Ringaskiddy, en Irlande
- Grimsby, en Grande-Bretagne
- Bâle, en Suisse
- Resende, au Brésil

Chaque centre *ChemOps* est responsable de son propre réseau d'approvisionnement de matières premières permettant de créer les substances médicamenteuses. Une fois les substances médicamenteuses produites, celles-ci sont ensuite stockées dans des entrepôts. De ces entrepôts les substances sont ensuite dispatchées dans les centres d'opérations pharmaceutiques aux quatre coins du monde. La majorité du transport de fret entre les différents centres Novartis s'effectue par transport aérien, pour deux raisons principales ; la distance entre la plupart des centres est importante, et le transport aérien permet de s'assurer de la préservation des substances médicamenteuses dans un état excellent (la chaîne du froid est conservée, les substances médicamenteuses ne connaissent pas de changement de températures importants ni de chocs...).

2.1.3.1.2. Les opérations pharmaceutiques

Les opérations pharmaceutiques, appelées *PharmOps* en interne (pour *Pharmaceutical Operations* en anglais) s'occupent de récupérer les substances médicamenteuses produites par les quatre centres de production pour les transformer en médicaments finaux (sous forme de gélules, sirops, liquides à injecter...), puis de gérer l'emballage des médicaments sous forme de produit fini afin ensuite de distribuer les médicaments prêts à être commercialisés dans les différents bureaux pharmaceutiques nationaux. De par le monde, Novartis possède 15 centres *PharmOps* :

- Stein, en Suisse
- Wehr, en Allemagne
- Huningue, en France
- Horsham, en Grande-Bretagne
- Barberà del Vallés, en Espagne
- Torre Annunziata, en Italie
- Kurtköy, en Turquie

³ <https://www.novartis.com/sites/www.novartis.com/files/q4-2018-media-release-en.pdf>

- Tabao de Serra, au Brésil
- Tlaplan, au Mexique
- Suffern, au États-Unis
- Sasayama, au Japon
- Beijing, en Chine
- Rabat, au Maroc
- Jakarta, en Indonésie
- Le Caire, en Égypte

En parallèle de 15 centres PharmOps interne à Novartis, l'entreprise travaille aussi avec des fournisseurs tiers. Le travail de ces fournisseurs tiers est de fabriquer des médicaments Novartis, soit sous des marques différentes, soit des médicaments génériques. Ces entreprises sont entièrement indépendantes, mais passent cependant par les bureaux pharmaceutiques nationaux pour commercialiser leurs produits. Ces fournisseurs tiers sont les huit entreprises suivantes :

- Noven Pharmaceuticals, basé à Miami aux États-Unis
- Patheon, basé à Durham aux États-Unis
- Famar, basé à Paris en France
- Jamshoro, basé à Jamshoro City aux Pakistan
- Mipharm, basé à Milan en Italie
- Orion, basé à Espoo en Finlande
- Akorn, basé à Hettlingen en Suisse
- Zarate, basé à Zarate en Argentine

L'ensemble de ces centres et entreprises sont regroupés par Novartis au sein de « *pools* » (soit des groupements) géographiques afin de gérer les coordinations avec les bureaux pharmaceutiques nationaux. Ces groupements sont les suivants :

- Le groupement Europe (composé des centres PharmOps de Grande-Bretagne, d'Allemagne, de France, d'Espagne, d'Italie, de Turquie et de Suisse, et des fournisseurs tiers Famar à Paris en France, Mipharm à Milan en Italie, Orion à Espoo en Finlande et Akorn à Hettlingen en Suisse)
- Le groupement Nord-Américain (composé du centre PharmOps des États-Unis et des fournisseurs tiers Noven Pharmaceuticals à Miami et Patheon à Durham, tous les deux aux États-Unis)
- Le groupement d'Amérique Latine (composé des centres PharmOps du Brésil et du Mexique, et du fournisseur tiers Zarate, à Zarate en Argentine)
- Le groupement des autres pays, qui fonctionnent nationalement (composé des centres PharmOps du Maroc, de l'Égypte, de l'Indonésie, de la Chine et du Japon, et du fournisseur tiers Jamshoro basé au Pakistan). Chacun de ces centres est indépendant, et est responsable d'un pays ou d'une zone géographique.

2.1.3.1.3. Les bureaux pharmaceutiques nationaux

Les bureaux pharmaceutiques nationaux, appelés *Country Pharmaceutical Office* en interne, ou *CPO*, sont responsables de la vente et de la distribution des produits Novartis dans une région géographique spécifique (un pays ou un ensemble de pays). Ceux-ci sont soit gérés par Novartis, soit

gérés par des tiers. Dans l'ensemble, Novartis préfère gérer ses centres et tout son processus de production, dans le but d'augmenter sa valeur auprès de ses actionnaires, mais dans certains pays des lois ou réglementations locales les obligent à faire appel à des *CPO* tiers. Les bureaux pharmaceutiques nationaux sont répartis selon les régions suivantes :

- La région Asie / Pacifique, qui obtient ses médicaments auprès du groupement Europe
- La région Europe, qui obtient ses médicaments auprès du groupement Europe
- La région Amérique du Nord, qui obtient ses médicaments auprès du groupement Nord-Américain
- La région Amérique Latine, qui obtient ses médicaments auprès du groupement d'Amérique Latine
- Et finalement les bureaux nationaux par pays, qui obtiennent leurs médicaments auprès du groupement des autres pays (par exemple le Japon, qui obtient ses produits auprès du centre *PharmOps* de Sasayama)

Une fois les médicaments répartis dans leurs *CPO* respectifs, Novartis vend directement les médicaments à ses clients, sans passer par des tiers. Les clients peuvent être des hôpitaux, des chaînes de pharmacies, des grossistes, des agents nationaux, et dans certains cas spécifiques (dans le cas d'une maladie rare ayant un nombre limité de patients de par le monde), directement aux patients.

En plus de cet ensemble de centres répartis partout dans le monde, il faut aussi souligner que Novartis gère en plus des laboratoires de recherche & développement, et des bureaux plus classiques (se chargeant du marketing, de la relation clients, et de l'ensemble des opérations ne touchant pas à la confection et à la chaîne d'approvisionnement des médicaments). Bien que ces centres ne rentrent pas dans le processus de la chaîne d'approvisionnement, les citer permet de se faire une idée plus globale de l'ensemble de l'entreprise.

2.1.3.2. Un modèle de chaîne d'approvisionnement théorique

A partir du modèle de la chaîne d'approvisionnement de Novartis, il est possible de généraliser le fonctionnement de l'industrie pharmaceutique, et de créer un modèle de chaîne d'approvisionnement théorique. L'objectif, en modélisant, est d'analyser le rôle des uns et des autres et les liens existants entre les différents acteurs. Cette analyse sera utile pour la proposition de solution.

Ce modèle de chaîne d'approvisionnement va grandement s'inspirer de celle de Novartis, tout en ayant comme objectif de généraliser plusieurs éléments et plusieurs acteurs. Il sera imparfait, et aura plus un aspect théorique (fonctionnement global, liens entre les différentes parties) que pratique (en correspondance claire avec la chaîne d'approvisionnement d'une certaine entreprise). L'idée ici est de généraliser la logique des chaînes d'approvisionnement de plusieurs entreprises pharmaceutiques (Novartis, Pfizer, Sanofi, Johnson & Johnson...), et non d'analyser la supply chain de chaque entreprise connue. Cette analyse à l'avantage, lors de la phase d'implémentation de la solution de traçabilité, d'être assez générique pour pouvoir ressembler au modèle de l'entreprise A, B ou C, avec chaque entreprise ayant une chaîne d'approvisionnement différente. Par exemple, là où Novartis a quinze *PharmOps*, un modèle aura entre zéro et n *PharmOps*, avec un n pouvant aller jusqu'à l'infini. Ce modèle suppose aussi que toutes les supply chain du secteur pharmaceutique possèdent des équivalents aux *PharmOps* et aux *CPOs*.

Les *ChemOps* ne sont pas utilisés dans ce modèle, et cela parce que la traçabilité d'un médicament est importante dans le cas du médicament final, et car les entreprises pharmaceutiques ont comme objectif de proposer des produits finis, et non des principes actifs, aux consommateurs.

En généralisant les acteurs de la chaîne d'approvisionnement de Novartis, les acteurs suivants sont identifiés :

- Les fabricants de substances médicamenteuses (*FSM*), qui sont présents au sein de la supply chain dans les différentes usines de fabrications de médicaments. Ceux-ci transforment les différents produits et molécules de base en substances médicamenteuses. Les FSM correspondent aux *PharmOps* de Novartis.
- Les bureaux pharmaceutiques nationaux (*BPN*) qui se chargent de récupérer des médicaments pour une zone géographique donnée, et de les vendre à des clients sur une zone géographique attirée. A la différence du modèle de Novartis, ce modèle ne fera pas de groupement géographique de fabricants de substances médicamenteuses (*FSM*). Chaque BPN peut acheter à n'importe quel fabricant (et donc un BPN peut recevoir un médicament de différents FSM). Il est pris en compte ici que l'utilisateur futur du modèle fera preuve de discernement, et ira s'approvisionner dans un centre localisé dans sa zone géographique (l'approvisionnement dans un centre localisé dans sa zone géographique a comme objectif de réduire les coûts globaux de transports, et l'approvisionnement dans un centre localisé en dehors de sa zone géographique ne fera qu'augmenter les coûts).
 - Les clients finaux (*CF*), qui peuvent être des pharmacies, des hôpitaux, des grossistes, des patients. Dans le cadre de ce modèle, les clients finaux peuvent acheter à d'autres clients finaux selon une logique. Par exemple, un grossiste achetant des médicaments n'a pas vocation à consommer ceux-ci mais plutôt à les vendre, tandis qu'un patient final ne devrait pas revendre les médicaments qu'il possède. Le modèle est assez extensible pour accepter qu'un client final revende des médicaments, et donc que celui-ci se transforme en intermédiaire.

Il existe donc trois acteurs principaux au sein d'une chaîne d'approvisionnement pharmaceutique. L'objectif d'une traçabilité est de permettre au patient de savoir si le médicament qu'il va consommer est bien celui qu'il a acheté, et non un médicament potentiellement falsifié.

En plus des trois acteurs principaux, il existe les différents transporteurs. Les interactions entre les acteurs se font à travers de ceux-ci (le chimiste qui conçoit des médicaments perdrait son temps et son énergie à transporter lui-même une substance médicamenteuse jusqu'à un bureau pharmaceutique national). Ces transporteurs sont importants dans la chaîne d'approvisionnement, car ils peuvent aussi constituer une faille (un transporteur peut par exemple « gonfler » un lot avec des médicaments similaires, mais qui ne possède pas le même principe actif). La lutte contre la contrefaçon doit permettre d'identifier le ou les acteurs faisant entrer des produits contrefaits au sein d'une chaîne d'approvisionnement considérée sûre, et de prendre des mesures envers ces acteurs en cas de doutes.

La figure suivante présente les différents acteurs du modèle de chaîne d'approvisionnement, avec les différentes interactions entre ces acteurs :



Figure 2 : Un modèle générique de Supply Chain

Dans ce schéma, FSM correspond au fabricant de substances médicamenteuses, les deux T aux transporteurs (qui peuvent être ou non deux transporteurs différents), BPN à un bureau pharmaceutique national, et CF à un client final. Ce schéma présente la chaîne d'approvisionnement la plus simple et la plus directe possible. Il existe de nombreuses variations possibles de cette chaîne,

avec par exemple une suite de CF vendant des médicaments à d'autres clients finaux (dans le cadre des grossistes).

2.2. L'État Actuel de la Traçabilité dans l'Industrie Pharmaceutique

Vu l'importance de la traçabilité des médicaments pour la santé publique et économique de nombreux pays, il existe aujourd'hui de nombreux outils mis en place afin d'assurer celle-ci. C'est l'un des rares outils permettant au client de s'assurer que le médicament qu'il achète correspond au médicament qu'il souhaite acquérir. Cependant cet outil n'est pas sans failles, au contraire des tests en laboratoire d'un médicament d'un lot. Tout le monde ne pouvant pas tester chacun de ses lots de médicaments chez lui, la traçabilité à l'aide de données sur l'emballage est aujourd'hui l'outil mis en place à grande échelle pour suivre les médicaments. Lors de la production de médicaments, ceux-ci sont produits par lot (ou *batch* en anglais). C'est ce numéro de lot qui est ensuite tracé, permettant aux producteurs de médicaments de savoir, dans le cas où un médicament est défectueux, de rappeler l'ensemble d'un lot du médicament en question, et donc de prévenir les dangers potentiels pouvant porter atteinte à la santé du consommateur (ainsi que de conserver la confiance des consommateurs vis-à-vis des médicaments de ce producteur). Ce numéro de lot se trouve obligatoirement au sein d'un datamatrix, ainsi que sur l'emballage du médicament.

2.2.1. Analyse des Datamatrix

Les datamatrix sont aujourd'hui les outils les plus modernes qu'utilise l'industrie pharmaceutique. Ceux-ci ressemblent fortement aux QR codes (QR signifie *Quick Response*), très populaire aujourd'hui, mais il existe plusieurs différences entre QR codes et datamatrix. En parallèle de ces deux systèmes de codification, on rencontre aussi couramment les codes-barres traditionnels, aussi appelés codes à barres linéaires, dans la plupart des commerces. Ces trois systèmes représentent les systèmes les plus couramment rencontrés, mais il existe des dizaines d'autres types de codes : code aztec, high capacity color barcode, ShotCode, et de nombreux autres [5]. Entre les QR codes, les datamatrix et les codes-barres, ils existent des différences, représentées dans la table ci-dessus [29]:

QR Codes	Datamatrix	Code à Barres Linéaires
		
• Code en 2D • Développé en 1994 • 4296 caractères • Entre 7% et 30% de correction d'erreurs possibles à la lecture	• Code en 2D • Développé en 1989 • 2335 caractères • 30% de correction d'erreurs possible	• Code en 1D • Développé en 1951 • 80 caractères⁴ • 0% d'erreur, mais un nombre clé de contrôle permettant d'identifier des erreurs à la lecture

⁴ Il existe différents types de code à barres linéaire, ici le choix a été fait de comparer avec le Code 128, utilisé principalement pour les expéditions (et donc la Supply Chain d'éléments).

A l'usage, les codes en une dimension permettent d'encoder beaucoup moins d'informations que sur un code en plusieurs dimensions. De plus, ils ne peuvent être lus qu'en alignant correctement le lecteur avec le code. A l'inverse, les codes en deux dimensions sont beaucoup plus pratiques à manipuler, car ils peuvent être lus dans n'importe quel sens. Cela est dû à l'âge des codes-barres : ceux-ci ont été développés dans les années 50 (et réellement utilisés à partir des années 70, avec la première utilisation sur un paquet de chewing-gum de la Wrigley Company en Juin 1974 [13]), et les lecteurs à cette époque n'étaient pas autant accessibles qu'aujourd'hui. Les QR codes et les datamatrix, plus récents, peuvent être lus avec n'importe quel téléphone aujourd'hui.

Les QR Codes présentent cependant une faiblesse importante, pouvant être utilisés à des fins malicieuses. Ceux-ci redirigent automatiquement vers des pages internet si c'est ce qui est scanné, et ces pages peuvent télécharger des virus à leur ouverture, contenir du contenu illégal, et plus généralement contenir du contenu dangereux. De plus, les QR codes se trouvant dans de nombreux endroits, un sticker contenant un autre QR code peut être posé au-dessus d'un QR code présent sur une affiche officielle (par exemple d'une banque), le QR code « pirate » renvoyant vers un site qui ressemble grandement au site de la banque, et dans lequel il peut être demandé de rentrer des données personnelles (numéro de carte bleue, nom et adresse de la personne...). Ainsi, les QR codes peuvent permettre de réaliser le *phishing* d'utilisateurs ne connaissant pas les risques présentés par ceux-ci.

L'industrie pharmaceutique s'est donc tournée vers les datamatrix, plus sécurisés et permettant d'être inscrits sur un plus petit espace que les QR codes. Cette problématique de l'espace utilisé est importante pour les médicaments, car l'espace disponible sur les boîtes et les emballages des médicaments est très faible. Certains pays et gouvernements, comme les pays de l'Union Européenne, ont l'obligation d'utiliser des datamatrix depuis le 9 Février 2019 sur les emballages de médicaments. Mais plus globalement, c'est l'organisme GS1 (Global Standards 1) qui régule et développe la normalisation des méthodes de codages utilisées dans les chaînes logistiques. La France et le Chili font partie de cet organisme. Bien que cet organisme offre une latitude concernant les normes de traçabilités des médicaments (l'utilisation de datamatrix n'est pas obligatoire dans tous les territoires), les datamatrix se sont globalement imposés partout dans le monde (Chili, Argentine, États-Unis d'Amérique, les membres de l'UE entre autres) [12].

En Europe, l'usage des datamatrix permet d'avoir de nombreuses informations sur un médicament donné. Ces informations sont standardisées selon la norme ISO/IEC 16022:2006 [17], qui définit les exigences d'utilisation des datamatrix. Les données encodées par les datamatrix sur les emballages de médicaments sont les suivantes :

ASCII23201034009300001201715081010234X22ASCII299123587

Le découpage de ces données se fait selon le modèle suivant :

- En rouge c'est une balise informatique (usuellement non retranscrite par le lecteur) qui permet de connaître le format d'encodage. Dans l'exemple présent, c'est le format ASCII 232, un format de codage des caractères
- En vert ce sont des marqueurs afin d'aider le lecteur à reconnaître ce qu'il lit.
- En bleu c'est le code numéro GTIN (*Global Trade Item Number*) imposé par le GS1. Ce numéro contient 14 caractères, et le premier caractère permet de savoir si c'est un médicament destiné à la vente directe (s'il commence par un 0), un autre type de vente (1-8), ou un médicament spécifique (9). Le numéro GTIN permet de s'adapter à une codification nationale (en France par exemple). Cette codification nationale correspond au numéro NTIN (*National Trade Item Number*). Ces 14 caractères permettent d'identifier le médicament et sa marque

(par exemple, deux médicaments génériques vendus par la même marque auront le même numéro GTIN).

- En violet c'est la date de péremption du médicament, avec le format JJMMAA (JJ correspond au jour, MM au mois et AA à l'année).
- En orange c'est le numéro de lot du médicament.
- En marron ce sont des numéros libres permettant à l'entreprise productrice du médicament d'ajouter les informations qu'elle souhaite.

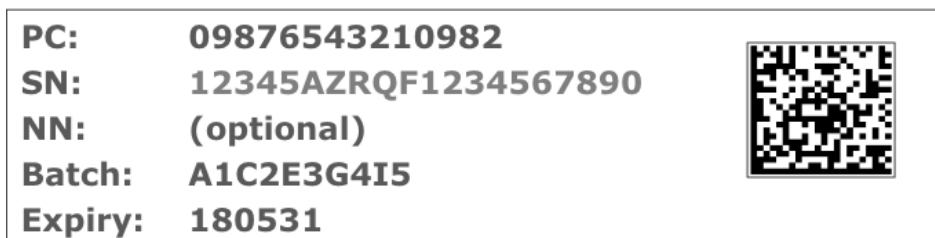


Figure 3: Exemple de Datamatrix et des données associées – Source : <https://ec.europa.eu/> [36]

Dans cet exemple, les données correspondent à celles encodées par le datamatrix, mais en plus lisible : PC (*Product Code*, code du produit), SN (*Serial Number*, numéro de série), NN (*National Number*, numéro national permettant d'identifier le produit dans un pays donné et permettant le remboursement de celui-ci), Batch (le numéro de lot), et Expiry (la date d'expiration).

L'ensemble de ces informations permette clairement d'identifier un lot défectueux pour l'entreprise vendant le médicament, mais donne très peu d'informations au consommateur sur d'où vient son médicament, et les étapes de production qu'il a suivies. De plus, l'ensemble des informations encodées se retrouve aussi sur l'emballage du médicament, et sont tout simplement codées de nouveau au sein du datamatrix. Mais il n'y a aucun ajout d'information dans ce datamatrix, et comme vu précédemment beaucoup plus d'informations (2335 caractères) peuvent être encodées au sein d'un datamatrix. Ces nouvelles informations peuvent être encodées au sein des numéros libres, à l'aide de nouvelles balises.

De plus, n'importe qui peut générer seul ce code datamatrix, et fabriquer un boîte « pirate » afin de faire passer des médicaments contrefaits pour des médicaments légitimes. Bien que les différentes personnes formées à identifier et lire un datamatrix pourraient se rendre compte de la contrefaçon, pour la majorité des personnes ces informations sembleraient légitimes. Le manque de protection des datamatrix, et la facilité de falsification, fait que c'est une évolution importante dans la traçabilité des médicaments, mais qui reste imparfaite.

2.2.2. Analyse de la RFID

Une autre technologie existante actuellement est la puce de radio-identification, plus couramment nommée d'après le sigle RFID (sigle en anglais signifiant **R**adio **F**requency **I**Dentification). L'utilisation du sigle RFID, bien que d'origine anglophone, est acceptée en français. La technologie RFID se base sur la radiofréquence, qui correspond à la fréquence d'une onde magnétique entre 30 hertz et 3000 gigahertz. L'identification d'un élément par radiofréquence est une technique qui permet d'identifier des objets à l'aide d'un dispositif électronique capable de transmettre des informations à un lecteur spécialisé. Aujourd'hui, l'utilisation du RFID est quotidienne pour la plupart des personnes, sans qu'elles ne s'en rendent compte. On retrouve par exemple cette technologie dans les cartes sans-contacts, dans les bibliothèques pour suivre les livres, dans les magasins pour lutter contre le vol...

La technologie RFID utilise le rayonnement électromagnétique pour identifier ou suivre des objets ou des personnes porteurs d'une étiquette lors du passage à proximité d'un lecteur. Au contraire des codes-barres linéaires, le lecteur ne nécessite pas d'alignement sur l'étiquette. La lecture

d'une étiquette est automatique et peut se faire sur des distances entre 10 mètres et près de 200 mètres. Une étiquette RFID peut stocker jusqu'à 64000 caractères [14], beaucoup plus donc que les 4296 caractères offerts par les QR codes (et les 2335 caractères des datamatrix). De plus, la RFID ne nécessitant pas de scans, elle permet de lire séquentiellement mais très rapidement, et cela sans intervention humaine, une multitude d'étiquettes. Cette lecture séquentielle est adaptée à l'industrie, pour scanner d'un coup un ensemble de produits arrivant d'un même fournisseur.

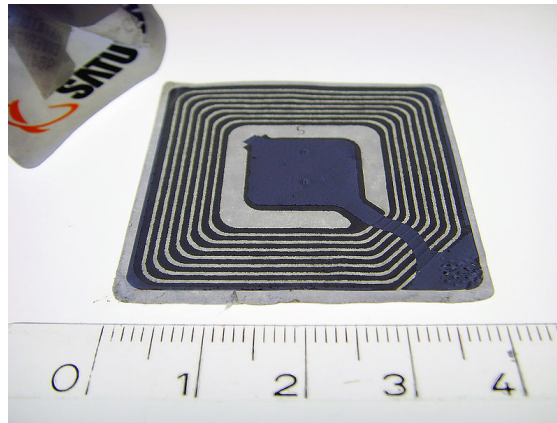


Figure 4 : Exemple d'une puce RFID - Source : Wikimedia

Une étiquette (qui peut aussi s'appeler *tag* ou radio-étiquette) se compose au moins d'une puce électronique. C'est dans cette puce électronique que se trouvent les informations. Il existe trois types d'étiquettes distinctes. Cette distinction se fait indépendamment du support, de la forme et de la taille de l'étiquette, ces paramètres pouvant être variés et combinés à l'infini. Les trois types d'étiquettes sont les suivants :

- Passive ; ce type de tag est le plus répandu, et il est présent aujourd'hui dans l'achat de nombreux produits (vêtements, jeux vidéo, livres...). Ce tag, comme son nom l'indique, est purement passif. Le tag contient des données figées lues par l'interrogateur RFID lorsqu'il est à proximité.
- Semi-passive ; ce type de tag est utilisé pour des applications spécifiques (relevé de températures, flux de personnes...). Il embarque une alimentation permettant de mettre à jour les données contenues dans celui-ci à l'aide de capteurs, mais cette alimentation ne permet pas d'émettre des données : sa lecture est passive, il utilise l'onde issue de l'interrogateur RFID afin d'alimenter la puce électronique embarquée, et ainsi transmettre les informations contenues dans sa mémoire [14].
- Actif ; ce type de tag embarque une batterie et un émetteur radiofréquence. La batterie, à l'inverse d'un tag semi-passif, alimente l'émetteur, et permet donc d'interagir de manière autonome avec l'environnement, par exemple en quadrillant une zone et en communiquant avec d'autres tags actifs sur les changements dans la zone. Ce tag relève les données sur une zone grâce à un ensemble de capteurs.

Dans le cadre des suivis des médicaments, le tag utilisé est un tag passif : il contient des informations sur le médicament (les mêmes qui se trouvent sur les datamatrix). Ces informations permettent à un scanner de lire l'ensemble des boîtes de médicaments arrivant dans un entrepôt ou une pharmacie [16].

Mais un système RFID, en plus des tags qui peuvent être uniques ou en nombre très élevé, se compose d'une base de données contenant des informations sur les données présentes sur les tags, d'une interface permettant de mettre en lien cette base de données avec le lecteur RFID, et d'un ou plusieurs lecteurs RFID. Ces lecteurs sont responsables de la lecture et de la transmission des informations contenues dans un tag [30]. Sur le marché, il existe une quantité énorme d'antennes et

de lecteurs selon la fréquence et l'usage souhaité. Plusieurs fréquences RFID peuvent être utilisées dans un même lieu sans que les ondes se concurrencent (si celles-ci sont sur différentes bandes).

Cependant, comme tout système électronique, les tags RFID possèdent plusieurs failles de sécurités. Ces failles, permettant de lire l'information contenue dans le tag (lecture par un système externe, analyse de puissance), de changer celle-ci (rétro-ingénierie, clonage du tag), ou bien plus largement d'éteindre l'ensemble du système (virus, dénis de service sur la base de données), font que l'utilisation du RFID présente certaines limites. Ces failles peuvent être compensées par un meilleur chiffrement de l'information sur la puce, des méthodes de filtrage des lecteurs, et des méthodes d'identification [33]. L'utilisation du standard du GS1 le plus récent, le G2V2 (pour génération 2 version 2) permet d'améliorer la sécurité des tags RFID passifs, avec l'ajout de nouvelles fonctionnalités : mesures anti-contrefaçon, amélioration de la sécurité, droits d'accès, amélioration de la traçabilité et possibilité de taguer un article (par exemple avec « vendu », « en rayon » ou « volé » [4]).

Dans le cadre du secteur pharmaceutique, la FDA (*Food and Drug Administration*), l'organisme américain chargé de réguler les médicaments, a commencé à travailler avec la technologie RFID au début des années 2000 face à l'émergence des médicaments contrefaits sur le territoire américain [8]. C'est la miniaturisation des étiquettes RFID des années récentes qui permet de penser à une plus grande adoption de la technologie au sein du secteur médical. En 2008 fut fondée l'organisation RFID in Healthcare Consortium (RHCC) [2], qui a pour objectif de promouvoir l'utilisation de la technologie RFID au sein du secteur médical, et l'optimisation de son intégration en prenant en compte plusieurs enjeux (la confidentialité, le risque d'interférence ou la sécurité par exemple). Cela permet de savoir que l'utilisation de la RFID dans le secteur médical est récente, mais a un fort potentiel à l'avenir.

L'utilisation de la RFID pourrait, en plus d'aider à la traçabilité des médicaments, aider à savoir quand un patient prend et suit son traitement [16], ce qui constitue un des autres challenges de l'industrie pharmaceutique aujourd'hui. Cependant, le coût d'un tag RFID est d'environ 10 centimes de dollars pour un tag passif (un tag actif, coûtant près de 40 dollars, n'a que peu d'intérêt dans le cadre de l'industrie pharmaceutique pour des médicaments consommés et distribués à grande échelle), tandis qu'imprimer un datamatrix sur une boîte de médicament à un coût substantiellement moins élevé (dans les millièmes de centime de dollars). Pour des médicaments qui valent entre 1 et 2 euros, cela constitue une augmentation du prix de 5 à 10%, difficilement justifiable pour le consommateur. Aujourd'hui, le coût des systèmes RFID est l'une des limites principales à son adoption globale par l'industrie pharmaceutique. Mais à long terme, cette technologie devrait très largement remplacer les datamatrix sur les boîtes de médicaments. Il faut cependant souligner que l'information, qu'elle soit contenue au sein d'un datamatrix ou d'un tag RFID, reste la même.

2.3. Les blockchains

En une phrase, une blockchain est un registre de transactions numérisé, transparent et décentralisé. Les blockchains enregistrent une liste sans cesse croissante d'enregistrements, appelés blocks, qui sont liés et sécurisés entre eux par cryptographie. Les blockchains permettent de résoudre un problème fondamental : plusieurs ordinateurs, qui ne se connaissent pas et qui n'ont pas confiance entre eux, tentent de se mettre d'accord sur quelque chose. L'objectif pour une application qui utilise une blockchain est de déployer un réseau, dans lequel des utilisateurs dans différents endroits du monde peuvent interagir entre eux en toute confiance. Pour atteindre cet objectif, il faut utiliser un système distribué capable de se mettre d'accord sur une vérité unique par consensus, sans faire confiance à aucun des utilisateurs. Un consensus permet de créer un système fiable à partir d'entités potentiellement non fiables.

2.3.1. Chaines, blocks et données

Une blockchain, avant d'être distribuée entre plusieurs machines, est une structure de données. L'absence de distribution enlève le principe même de la blockchain, qui est d'avoir une vérité unique distribuée entre plusieurs utilisateurs, mais enlever la distribution permet de comprendre la structure de données et les composants interne d'une blockchain.

2.3.1.1. Les données

Une blockchain est, d'un point de vue externe, une base de données. Elle permet de suivre un ensemble de transactions entre différents acteurs. Cet ensemble de transactions, représenté sous forme de journal, permet de connaître quelles données appartiennent à quels acteurs. Par exemple, dans le cadre d'une crypto monnaie, la donnée suivie est le montant de monnaie possédé par chaque acteur, tandis que les transactions suivies sont les transferts de cette monnaie entre les acteurs. Une blockchain est donc une base de transactions.



Figure 5: Schéma d'une transaction

2.3.1.2. Les blocks

Sous la forme d'un journal de transactions, la quantité de transactions contenues dans la blockchain augmente rapidement. Il ne faut pas oublier que les blockchains sont des systèmes distribués, et il existe en conséquence la possibilité d'avoir plusieurs transactions qui se passent en même temps entre plusieurs acteurs. Afin d'éviter la synchronisation entre les différents acteurs de la blockchain pour chaque transaction, les transactions sont regroupées en blocks.

La formation de blocks passe par plusieurs étapes. Dans une première étape, les acteurs vont créer des transactions entre eux, qui sont ajoutées au sein d'une réserve de transactions. Cette réserve se compose de transactions, mais la particularité de celles-ci est qu'elles ne sont pas encore validées par l'ensemble des acteurs. En effet, un acteur pourrait déclarer être propriétaire de données au reste du réseau, alors qu'il ne l'est pas. C'est dans cet objectif que la réserve de transactions existe. Dans la plupart des implémentations de blockchains, cette réserve n'est pas unique, mais est constituée d'un assemblage de plus petites réserves.

Des acteurs spécifiques, nommés mineurs, vont ensuite aller chercher dans ces réserves les transactions, et les vérifier. Si elles sont correctes (les bons propriétaires envoient les bonnes données, il n'y a pas de doublons), ceux-ci peuvent ajouter les transactions à un block. Plusieurs mineurs peuvent sélectionner les mêmes transactions à ajouter à leurs blocks, la seule condition de l'ajout d'une transaction à un block est sa validité.

En plus de transactions, un block doit contenir un ensemble de données supplémentaires [38]. Ces données supplémentaires servent à valider ou non l'ajout d'un block à la blockchain. L'une des données les plus importantes qu'un block doit avoir est un hash (empreinte numérique en français). Cet hash numérique est calculé à l'aide d'une fonction de hachage, qui prend en entrée un texte et l'associe à une empreinte numérique, et permet d'identifier les blocks les uns des autres. Il faut peu de ressources pour générer un hash.



Figure 6: Exemple de hachage avec SHA-256

Chaque chaîne de caractères possède son propre hash, et une légère modification d'une chaîne change complètement le hash associé à la chaîne, car les fonctions de hachages sont des fonctions déterministes. Un autre avantage des hashes est qu'il est impossible de déterminer le texte encodé à partir de celui-ci. Dans une blockchain, pour calculer un hash, la fonction de hachage du block va prendre en compte le hash du block précédent de la blockchain ainsi que le hash associé au block actuel. Par exemple, le hash du block numéro 32 sera généré à partir du hash du block 31 et du hash des textes du block 32. Chaque block contenant une multitude de transactions, le hash du block est composé de l'assemblage des hashes des transactions du block, à l'aide d'un arbre de Merkle, aussi connu sous le nom d'arbre de hachage.

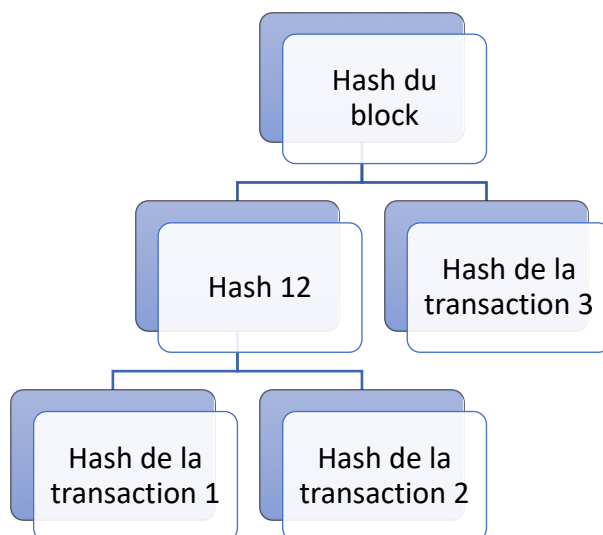


Figure 7: Composition du hash d'un block sous forme d'arbre de Merkle

Le premier hash, celui du block dit « *genesis* », est généré sans prendre en compte le hash du block précédent. Cet hash est uniquement généré à l'aide des transactions contenues dans ce premier block.

Une autre donnée incluse dans un block est le nonce. C'est un nombre arbitraire qui a vocation à être utilisé une seule fois et qui permet de créer une difficulté pour le mineur. Ce nonce est généré à l'aide du hash du block. Par exemple, si le nonce est déterminé pour qu'il soit « 00 », chaque hash doit commencer par ce nonce pour être valide. Cela permet de créer, pour le mineur du block actuel, une difficulté supplémentaire lors du calcul du hash, tandis que les mineurs qui vont vérifier la validité du block peuvent calculer rapidement si un block est valide (si le hash est correct et s'il commence bien par « 00 »). L'objectif de ce nonce, de cette difficulté, est d'éviter l'ajout permanent de block à la blockchain par des mineurs cherchant à corrompre celle-ci.

Enfin, chaque block est horodaté à l'aide d'un timestamp. Ce timestamp est une valeur générée en prenant en compte la date et l'heure actuelle. Ce timestamp est une couche supplémentaire de protection de la blockchain, permettant d'éviter sa corruption, car l'ensemble des transactions doit avoir des timestamps croissants (les transactions les plus récentes de la blockchain sont les transactions ayant les timestamps les plus récents).

Pour résumer, un block se compose donc de transactions, d'un hash, d'un nonce, et d'un timestamp :

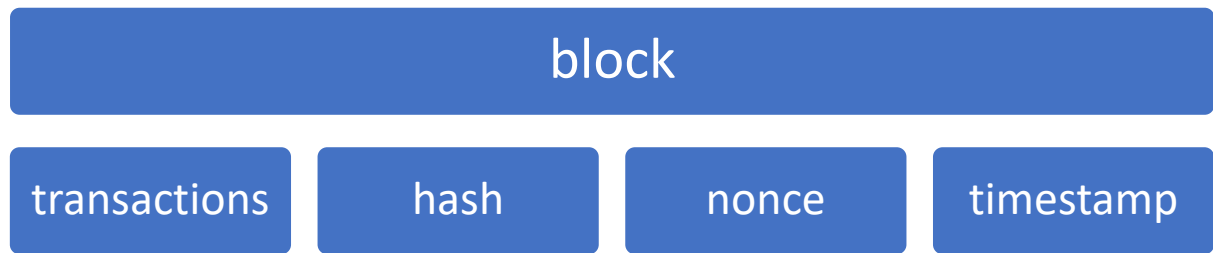


Figure 8: Composition d'un block

2.3.1.3. Les chaines

Comme précisé antérieurement, les blocks contiennent des hashes. Ces hashes sont générés à l'aide des hashes des fonctions précédentes. Ces hashes permettent de lier les transactions entre elles, et ainsi de créer la chaine. Toute transaction est donc dépendante de l'ensemble des transactions précédentes pour générer son hash. C'est cette dépendance qui crée l'immuabilité d'une blockchain: chaque transaction étant dépendante des précédentes, la modification d'une des transactions précédentes change complètement les transactions suivantes, et donc modifie (ou corrompt) la blockchain.

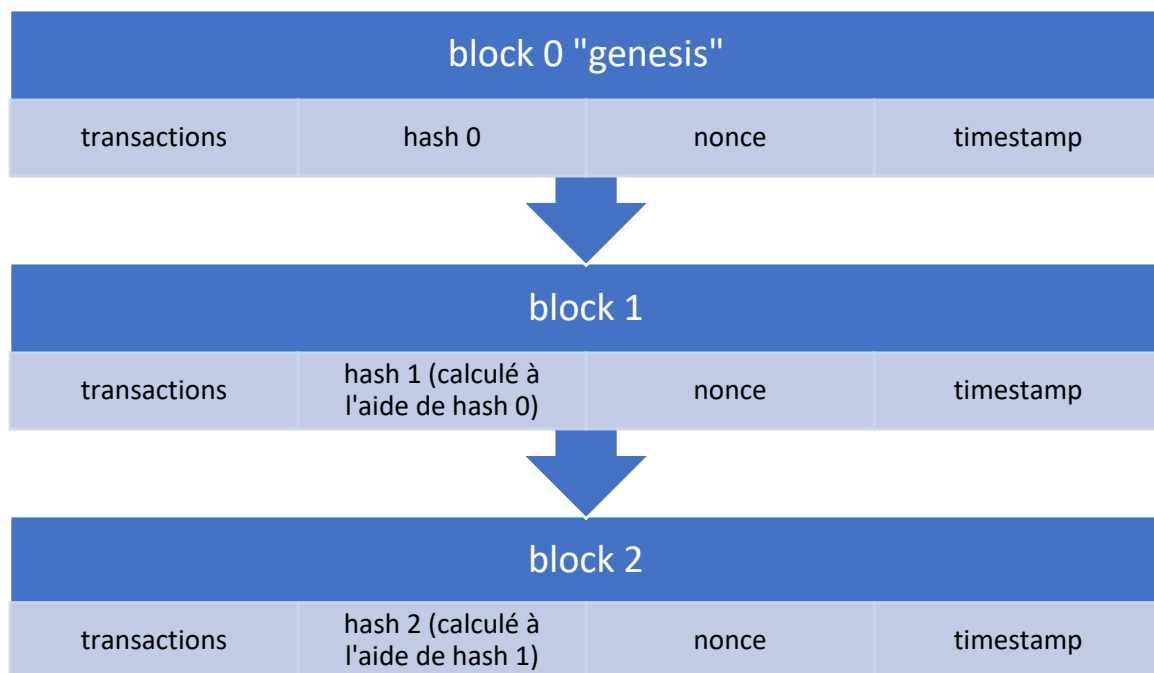


Figure 9 : Schéma d'une blockchain

2.3.2. Le système distribué

2.3.2.1. Les propriétés d'un système distribué

Une blockchain est distribuée entre plusieurs mineurs, ou nœuds. Un système distribué se compose de nœuds indépendants représentant différents processus et de canaux de messages permettant aux nœuds d'échanger entre eux. L'objectif de l'ensemble des nœuds, et donc du système distribué est d'accomplir une tâche globale. Dans le cadre d'une blockchain la tâche est de garantir la validité de la blockchain. Les nœuds peuvent effectuer quatre actions : envoyer, recevoir, enregistrer et faire des calculs sur les données qu'ils ont. Un système distribué présente plusieurs avantages en

comparaison avec un système centralisé : tandis qu'un système centralisé peut arrêter de fonctionner, commettre des erreurs, perdre des données ou être corrompus, un système distribué doit permettre de s'assurer de la persistance des données entre les différents nœuds, et d'éviter des erreurs de la part du système. C'est pour cela que les systèmes distribués sont adaptés dans le cadre du stockage d'informations sensibles (telles des données bancaires). Un système distribué présente plusieurs propriétés :

- Les nœuds sont concurrents entre eux pour gérer l'information.
- Il n'y a pas d'horloge globale entre les nœuds, chaque nœud est responsable de son propre temps, mais l'ensemble des nœuds essaye de rester synchronisé entre eux.
- Il existe la possibilité qu'un ou plusieurs des nœuds connaissent des défaillances (perte d'un message de synchronisation, un processus de s'exécute pas correctement...). Dans le cas de défaillances, les protocoles d'échanges (par exemple l'algorithme de Chandy-Lamport [10]) entre les nœuds doivent gérer celle-ci, afin que l'ensemble du système réalise correctement son travail.

Pour s'assurer de l'exactitude d'un système distribué, c'est à dire qu'il remplit correctement son objectif, celui-ci utilise des algorithmes de consensus. Un algorithme de consensus correct doit remplir 3 propriétés.

- La validité de la solution finale (*validity*), c'est à dire que la valeur sur laquelle l'algorithme se mettra d'accord doit être proposé par un des processus.
- Un accord sur la valeur finale entre les différents processus (*agreement*), c'est à dire que tous les processus qui n'ont pas connus de défaillance soient d'accord sur la même valeur finale.
- Une conclusion (*termination*), soit l'algorithme doit forcément renvoyer une valeur finale : il ne peut pas chercher indéfiniment une valeur.

Ces 3 propriétés entrent dans deux catégories : les propriétés de sécurité (*safety*), qui s'assurent que le résultat final est correct, soit la validité et l'accord, et la propriété de vie (*liveness*), qui s'assure qu'une valeur sera renvoyée, et qui est la conclusion (*termination*). La définition de ces propriétés et catégories est l'œuvre de Leslie Lamport.

Mais les systèmes distribués présentent aussi des limites. Le théorème de Brewer (ou théorème CAP) définit ces limites. Selon ce théorème, il est impossible pour un système informatique de calcul distribué de garantir en même temps :

- Cohérence (*consistency*) : tous les nœuds du système voient exactement les mêmes données au même moment
- Disponibilité (*availability*) : toute les requêtes sont garanties de recevoir une réponse
- Tolérance au partitionnement (*partition tolerance*) : aucune panne moins importante qu'une coupure totale du réseau ne doit empêcher le système de répondre correctement (et donc une panne de nœuds ne doit pas empêcher le système de répondre correctement)

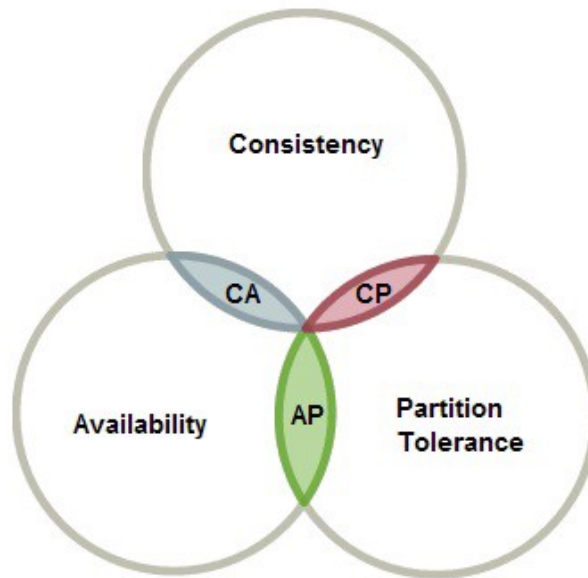


Figure 10: Représentation du théorème CAP - Source : towardsdatascience.com [26]

Selon ce théorème, un système distribué ne peut garantir à un instant T que deux de ces trois contraintes, mais pas les trois. Le système doit donc faire un compromis entre la cohérence, la disponibilité et la tolérance au partitionnement.

Dans un système distribué, celui-ci est partitionné entre différentes machines. Donc la tolérance au partitionnement est toujours à prendre en compte. Le choix revient donc à choisir entre la cohérence du système, et donc retourner une valeur potentiellement fausse, et la disponibilité, et donc ne rien retourner. Mais le théorème n'est pas binaire, il répond plus à un spectre de possibilité. Par exemple, la disponibilité peut ne pas être immédiate (une latence est acceptable) afin de satisfaire à l'exigence de disponibilité. Le théorème du CAP permet de comprendre les limites des systèmes distribués. Les systèmes distribués peuvent donc échouer à générer un résultat. Un exemple d'échec de système distribué est celui des généraux byzantins, lui-même une généralisation du problème des deux généraux.

2.3.2.2. Le problème des généraux byzantins

Ce problème est l'un des problèmes classiques des systèmes distribués. Son énoncé est le suivant :

« Des généraux byzantins encerclent une ville qu'ils souhaitent prendre. Pour communiquer entre eux, ils ne peuvent qu'utiliser des messagers, et ils n'ont pas décidé sur ce qu'ils allaient faire : attaquer la ville ou abandonner l'attaque et rentrer chez eux. Pour conquérir la ville, l'ensemble des généraux doit attaquer en même temps. Mais le problème est que certains généraux ont été corrompus en échange d'une somme d'argent, et vont donc envoyer un message incorrect afin de faire échouer l'assaut, et donc empêcher un consensus entre les généraux. En plus des traîtres, certains messagers peuvent se perdre ou eux-mêmes corrompre leur message. L'objectif est d'établir un consensus entre les généraux afin d'attaquer la ville, tout en s'assurant que les communications entre eux ne soit pas corrompues (perdues ou modifiées). Permis les généraux, il y a un commandant et des lieutenants. Tous peuvent être corrompus. Les généraux corrompus sont des nœuds byzantins. »

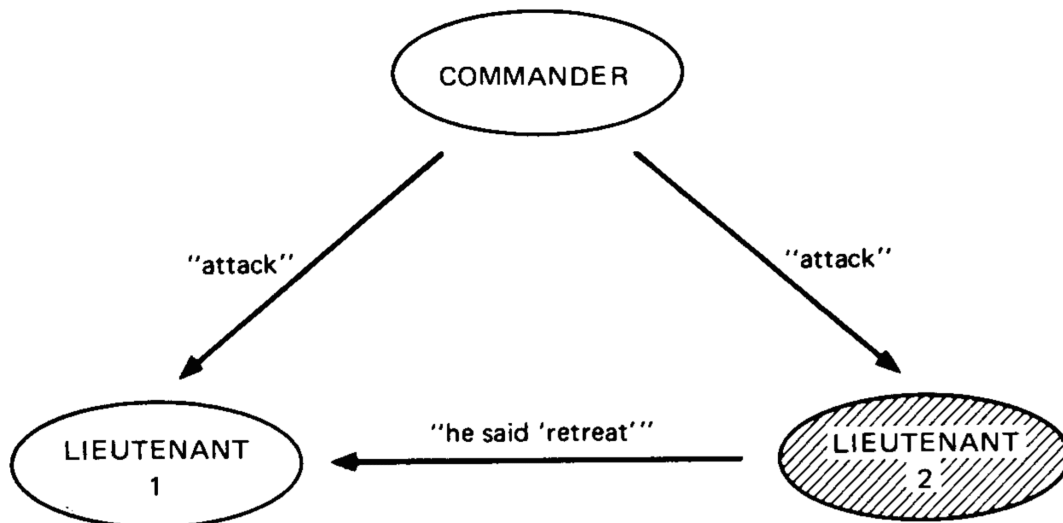


Figure 11: Problème des généraux byzantins - Source : edx.org

Dans l'exemple ci-dessus, le commandant envoie l'ordre d'attaquer, mais le lieutenant 2 est corrompu, et modifie le message qu'il fait parvenir au lieutenant 1. Le lieutenant 1 reçoit deux messages contraires : l'un d'attaquer, l'autre de se retirer. Mais le lieutenant 1 ne peut pas savoir qui est le traître. Le commandant peut aussi avoir envoyé les messages "attaquer" au lieutenant 1, et "se retirer" au lieutenant 2. Le lieutenant ne sait donc que faire, et ne sait pas non plus qui est le traître entre le commandant et le lieutenant 2. Ce problème n'a pas de solution si plus d'un tiers des nœuds sont des traîtres.

Ce problème permet d'identifier les deux types d'erreurs qui peuvent subvenir dans un système distribué, les erreurs de type *fail-stop* et les erreurs de type byzantin. Une erreur *fail-stop* est le crash d'un nœud ou l'absence de valeur retournée. Ce premier problème est le plus simple à identifier pour les autres nœuds du système, car ceux-ci se rendent compte de l'absence d'une réponse d'un nœud. Une erreur byzantine est celle inspirée par le problème des généraux byzantins : les nœuds peuvent ne pas fonctionner, ne pas retourner de valeur, mais peuvent aussi répondre une information ou corrompue, ou fausse. Les erreurs de types byzantines sont une généralisation des erreurs *fail-stop*. Une blockchain publique doit éviter à tout prix une erreur byzantine, car les participants d'une blockchain sont anonymes et imprédictibles. La présence d'une erreur byzantine dans une blockchain corrompt celle-ci.

Le problème des généraux byzantins peut être comparé à une blockchain. C'est le même concept avec deux noms différents :

Distance géographique	Réseau distribué
Généraux	Nœuds
Généraux traîtres	Nœuds défectueux ou malveillants
Messagers non fiable	Messages entre les nœuds perdus ou corrompus
Attaquer ou se retirer	Consensus sur les transactions

Le problème des généraux byzantins est typique dans le cas des blockchains. Pour résoudre celui-ci, il faut donc utiliser des algorithmes de consensus, permettant aux différents nœuds de se mettre d'accord sur une valeur à renvoyer.

2.3.2.3. Les mécanismes de consensus

Les mécanismes de consensus sont la colonne vertébrale des systèmes distribués. Ces mécanismes fonctionnent principalement sur un principe de votes lors des mises à jour du système distribué. Ce système de votes se base sur une logique mathématique.

2.3.2.3.1. Paxos

Paxos est une île au large de la Grèce. C'est aussi une famille d'algorithme de consensus pour les systèmes distribués, créé par Leslie Lamport [20], le même Lamport de l'algorithme de Chandy-Lamport. Le nom Paxos vient du système politique en place sur l'île de Paxos lors de la Grèce ancienne. Pour passer des décrets, le parlement de Paxos, surnommé « le parlement à temps partiel », avait un fonctionnement propre. Les parlementaires avaient l'habitude de quitter sporadiquement celui-ci afin de se rendre à des banquets et d'autres activités. Tous les parlementaires n'étant jamais dans le parlement en même temps, ils possédaient chacun un journal contenant l'ensemble de ce qui se passait. Tous les journaux devaient être les mêmes. Les parlementaires se divisaient en trois groupes : les proposant, les accepteurs et les apprenants. Les proposant défendaient les requêtes et idées de lois des citoyens, les accepteurs votaient les requêtes et lois, et les apprenants se souvenaient de celles-ci et les transmettaient aux citoyens.

Les requêtes et lois étaient décidées par consensus. Afin d'arriver à un consensus, une majorité d'accepteurs devait être dans le parlement : cette majorité d'accepteurs correspondait à un quorum. Pour arriver à un quorum (et donc qu'une majorité d'accepteurs se mettent d'accord sur une loi), il fallait de nombreux tours jusqu'à arriver à un consensus entre les accepteurs. Chaque tour se faisait en deux parties : préparer et accepter.

Premièrement, des citoyens de l'île pouvaient parler et discuter avec des proposant. Une fois un proposant prêt à défendre une cause, celui-ci la propose sous forme de décret au parlement. Chaque décret possède alors un numéro et une valeur (par exemple : « 45. Il est interdit d'écrire sur les temples »). Les numéros liés aux décrets doivent forcément augmenter. Ensuite, une fois le décret proposé au parlement, les accepteurs en discutent et votent. Si à un moment donné il y a un quorum d'accepteurs qui votent en majorité pour le décret, celui-ci est passé et il est écrit dans les journaux de chaque parlementaire. Une fois un consensus conclu, les apprenants apprennent le résultat et le transmettent à la population de l'île.

Le parlement de Paxos fonctionnait exactement comme un consensus distribué. Les membres du parlement correspondent aux nœuds d'un système distribué, les citoyens correspondent aux clients, et la loi actuelle à l'état sur lequel les nœuds doivent se mettre d'accord. Le parlement de Paxos fait cependant quelques suppositions : les apprenants délivrent toujours le bon message aux citoyens, et ne cherchent pas à le corrompre. En d'autres mots, le parlement ne fonctionne que pour une erreur de type *fail-stop*, soit l'absence de nœuds (et donc l'absence de quorum), ce qui correspond alors à un parlement vide. Il ne répond pas au problème de généraux byzantins. L'absence d'un des membres du parlement ne fait pas que celui-ci est fermé, et le fonctionnement de Paxos permet de garantir la rapidité des lois, et permet de produire un ensemble important de données (ici les lois et décrets), et de reproduire ces données [21]. Seulement Paxos a toujours été difficile à comprendre, et Lamport a essayé de le clarifier en publiant un nouvel article, « Paxos made simple » [22]. En 2014, une alternative plus compréhensible à Paxos fut proposé, Raft.

2.3.2.3.2. Raft

L'algorithme alternatif, surnommé Raft, fut proposé dans un article nommé "*In Search of an Understandable Consensus Algorithm*" de 2014, écrit par Diego Ongaro and John Ousterhout [27]. Dans cet article, l'objectif est d'échapper à l'aide d'un bateau (« *raft* » en anglais) l'île de Paxos. Cet algorithme est formulé afin d'avoir un leader, qui est élu à chaque tour, et des *followers*, qui sont tous les autres nœuds. Le leader est le seul à communiquer avec le client, et il est responsable d'orchestrer et d'organiser l'envoi de messages du client aux différents nœuds, tout en maintenant un journal de l'ensemble de ce qui est transmis. Lorsque le leader reçoit une requête d'un client, il vérifie que tous les autres nœuds ont bien reçu la requête, et qu'ils ont bien tous écrit dans leur propre journal la requête. Le leader dirige le consensus, jusqu'à ce que lui-même s'arrête ou fasse des erreurs (*fail-stop*). Et dans le cas d'un *fail-stop*, un nouveau leader est élu.

Le leader est chargé d'envoyer régulièrement des requêtes aux autres nœuds, afin de leur annoncer qu'il est toujours présent et en vie. Si les autres nœuds ne reçoivent plus de requêtes, ceux-ci assument que le leader est "mort", et ils élisent un nouveau leader. Chaque nœud possède une horloge interne, qui se met en marche dès qu'il ne reçoit plus de requête du leader. Au bout d'un certain temps déterminé par cette horloge interne, chaque nœud peut alors candidater pour être le nouveau leader. Le nouveau leader est celui dont l'horloge interne est la valeur la plus grande (chaque nœud communique à un autre nœud sa valeur, et le nœud ayant la plus petite valeur devient alors supporter de l'autre, ceci jusqu'à qu'il n'y ait plus qu'un nœud, le leader élu). Il faut cependant noter que l'algorithme Raft ne peut pas compenser les erreurs byzantines.

2.3.2.3.3. Practical Byzantine Fault Tolerance (PBFT)

Publié par Miguel Castro et Barbara Liskov en 1999 [6], cet algorithme de consensus répond au problème des généraux byzantins. Tandis que Paxos et Raft sont des algorithmes *fail-stop*, le PBFT peut supporter des erreurs byzantines (et donc résoudre un problème du type des généraux byzantins). L'algorithme PBFT peut traiter f erreurs byzantines lorsque le nombre de nœuds est égal à $3f+1$ (il peut en conséquence résoudre l'algorithme pour moins de $1/3$ de nœuds "traîtres"). C'est un algorithme qui se compose de 3 parties : pré-préparation, préparation et réalisation.

PBFT commence lorsque le client envoie une requête à l'un des nœuds, nœud qui devient responsable de transmettre la requête (dans Paxos, les proposants remplissent ce rôle).

Vient ensuite la phase de pré-préparation, lors de laquelle le nœud responsable du message fait parvenir celui-ci à l'ensemble du réseau. Chaque nœud accepte le message seulement s'il est valide (les messages doivent contenir un numéro séquentiel, comme dans le cas de Paxos, et d'autres données permettant de déterminer la validité de ceux-ci). Si un nœud accepte un message pré-préparé, il envoie à chacun des autres nœuds du réseau un message de préparation (qui est seulement accepté par les autres nœuds s'il est valide). Un nœud est alors considéré préparé s'il a reçu le message original, et s'il a reçu $2f$ messages de préparation (et ce faisant le nœud sait qu'il y a $2f+1$ nœud de préparé).

Après que les nœuds soient préparés, ils doivent envoyer un message de réalisation. Si un nœud reçoit $f+1$ messages de préparation, il exécute la requête du client et la fait parvenir à celui-ci. Le client considère qu'il a reçu une réponse acceptable s'il reçoit $f+1$ réponses identiques. La figure suivante explique la chaîne des messages, en prenant en compte que le nœud 3 est en échec.

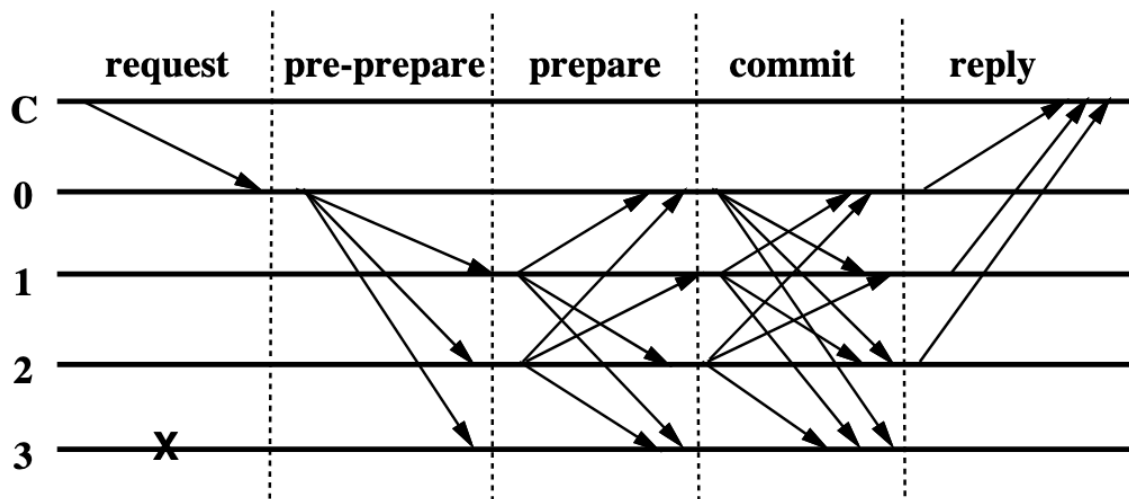


Figure 12 : Schéma du fonctionnement du BPFT – Source : edx.org

2.3.2.3.4. Consensus de Nakamoto

En 2008, Satoshi Nakamoto (nom supposé d'emprunt) a introduit dans un article nommé *Bitcoin whitepaper A peer-to-peer electronic cash system* [25]. Ce papier a révolutionné à la fois les transactions financières, mais a aussi introduit une nouvelle classe de consensus : les mécanismes de consensus de Nakamoto. Ceux-ci sont différents des consensus basés sur votes sur la façon dont les mises à jour des données distribuées sont faites. Les consensus basés sur votes nécessitent les votes explicites de chacun des nœuds du réseau, tandis que les mécanismes de consensus Nakamoto font voter les utilisateurs implicitement. Ces votes implicites sont basés sur un système de loterie aléatoire, où les utilisateurs sont en concurrence entre eux pour mettre à jour le système. C'est le gagnant de cette loterie qui obtient le droit de mettre à jour le système.

Les consensus de Nakamoto ont plusieurs propriétés particulières, qui les distinguent des consensus traditionnels, les consensus basés sur votes. Premièrement, cette famille consensus peut permettre à des utilisateurs ni connus, ni fiables de faire des mises à jour du système. Dans le Bitcoin, une monnaie électronique, et l'implémentation de celui-ci, n'importe qui peut se joindre au réseau, et n'importe qui peut donc envoyer des messages erronés ou corrompus aux autres nœuds du réseau. De plus, n'importe quel utilisateur peut utiliser autant d'identités virtuelles (une clé publique et une clé privée) qu'il le souhaite. Pour éviter la corruption du réseau (par exemple par un utilisateur possédant plusieurs identités), le droit de vote doit être rare, et doit donc être lié à une ressource rare.

2.3.2.4. Le droit de vote

Dans les blockchains, le droit de vote permet de déterminer qui a le droit d'ajouter un block ou non à la chaîne, et si l'ajout de ce block est cohérent. Il existe différents mécanismes permettant de déterminer qui possède ce droit de vote.

2.3.2.4.1. Preuve de travail (*Proof-of-Work*)

Pour le bitcoin, la solution fut de lier le droit de vote à la puissance de calcul des participants (c'est le système de validation par preuve de travail, ou *proof-of-work*). C'est l'une des possibles solutions pour arriver à un consensus de Nakamoto. La preuve de travail est apparue dans le même article que celui sur le bitcoin, en 2008 [25]. A cause de cette manière implicite de voter, les leaders sont élus grâce à une loterie aléatoire, où les chances de gagner cette loterie sont liés aux puissances

de calcul des participants. Le gagnant de la loterie a ensuite le droit de faire la prochaine mise à jour des données.

Mais il est possible que le leader élu souhaite corrompre les données. Dans ce cas, les autres participants au réseau votent en choisissant ou non de mettre à jour leurs versions locales du réseau. Pour le bitcoin, chaque nœud peut choisir les blocs qu'il rajoute dans sa blockchain, et cet ajout est valide uniquement si le reste du réseau est d'accord sur la présence de ce bloc dans la blockchain. Il faut donc que les consensus de Nakamoto définissent une série de règles, permettant de choisir et de trancher sur l'état du réseau. Une de ces règles peut être de conserver la chaîne la plus longue du réseau (dans le cas du Bitcoin). Les consensus de Nakamoto sont donc des consensus basés sur une chaîne.

Dans le cas du Bitcoin, le premier mineur (un mineur, dans ce cas précis, et un participant au réseau) qui résout un block envoie celui-ci à l'ensemble du réseau. Le réseau vote ensuite implicitement sur ce block, avec chaque nœud du réseau qui ajoute ou non la copie du block à sa chaîne. Dans les validations par preuve de travail, la ressource utilisée est la puissance de calcul de chacun des nœuds du système. Plus vite un mineur calcule, plus de chances il aura de résoudre le prochain block et de l'envoyer au reste du réseau, et donc mettre à jour celui-ci (et au passage remporter une récompense pour son travail).

2.3.2.4.2. Preuve d'enjeu (Proof-of-Stake)

Un autre exemple de consensus de Nakamoto est la preuve d'enjeu (*proof-of-stake*), introduit par Sunny King (nom d'emprunt) en 2012 [19]. Comme les mineurs dans la preuve de travail, les valideurs dans la preuve d'enjeu doivent mettre à jour et aider le réseau. Au lieu d'utiliser la puissance de calcul pour déterminer qui peut mettre à jour le réseau, cet algorithme utilise un système de jetons. Plus un valideur possède de jetons du réseau en question (par exemple l'éther pour l'Ethereum, une autre crypto monnaie introduite par Vitalik Buterin), plus il aura de chances d'être élu pour proposer une nouvelle mise à jour du réseau.

2.3.2.4.3. Preuve d'activité (Proof-of-Activity)

Un autre consensus de Nakamoto est la preuve d'activité (*proof-of-activity*). Ce consensus est un hybride entre la preuve d'enjeu et la preuve de travail. Dans un premier temps, sur le modèle de la preuve de travail, les mineurs résolvent et soumettent des blocs au réseau. Dans un second temps, et cette fois-ci sur le modèle de la preuve d'enjeu, le block possède dans ses métadonnées une liste de valideurs pouvant confirmer celui-ci. Cette liste de valideurs est générée aléatoirement, mais plus un valideur possède de jetons de la monnaie, plus il a de chances d'être dans ces métadonnées (et donc de valider ou non le bloc). Une fois le bloc validé par des valideurs, les autres membres du réseau peuvent l'ajouter à leurs copies locales.

2.3.2.4.4. Preuve de brûlage (Proof-of-Burn)

Le consensus par preuve de brûlage est une alternative à la preuve d'enjeu. Dans ce consensus, le plus de jetons un valideur accepte d'envoyer à une adresse de brûlage (cette adresse n'est pas accessible, et en conséquence les jetons envoyés à cette adresse sont perdus), le plus il a de chance d'être élu pour proposer le prochain bloc.

2.3.2.4.5. Preuve d'espace (Proof-of-Space)

Cet autre type de consensus de Nakamoto, la preuve d'espace (*proof-of-space*) utilise de l'espace de stockage comme la ressource permettant d'avoir le droit de voter. Ce type de consensus est vu comme plus écologique et moins coûteux, car l'espace de stockage coûte moins cher que la

capacité de calcul d'un ordinateur, et il consomme donc moins d'énergie. Ce type de consensus est plus utilisé pour le stockage de données que comme une méthode de vote en soi (par exemple avec le filecoin).

2.3.2.4.6. Preuve de capacité (Proof-of-Capacity)

Une alternative à la preuve d'espace, la preuve de capacité (*proof-of-capacity*) se base sur la preuve de l'utilisation d'une certaine quantité de stockage pour la résolution de celle-ci, permettant alors de proposer le prochain bloc ou la prochaine mise à jour du système.

2.3.2.4.7. Preuve de temps écoulé (Proof-of-Elapsed-Time)

Autre type de consensus, la preuve de temps écoulé (*proof-of-elapsed-time*) est un algorithme qui se base sur le temps de calcul de chaque nœud. Chaque nœud sélectionne un temps d'attente aléatoire, et attend pendant cette durée. Le nœud ayant le plus long temps d'attente est le prochain à soumettre un bloc. Pour éviter que ce type d'algorithme soit manipulé par les autres participants du réseau, il faut la présence d'environnements d'exécution approuvés (*trusted execution environment*, par exemple ceux permettant de débloquent les téléphones à l'aide d'une empreinte spécifique). Ces environnements, qui sont littéralement une partie de certains processeurs, ne répondent qu'à certaines conditions d'exécution s'assurant que le temps écoulé est bien le temps qu'il devait attendre, et permettent donc d'éviter la corruption du système.

2.3.2.4.8. Preuve d'autorité (Proof-of-Authority)

La preuve d'autorité (*proof-of-authority*) n'est pas un type de consensus de Nakamoto en soit, mais une alternative à ceux-ci. Ce type de preuve s'appuie sur un ensemble de nœuds de confiance qui ont le droit de mettre à jour le réseau. La ressource à utiliser dans ce type de preuve est l'identité : un nœud a le droit de mettre à jour le réseau en fonction de son identité.

Chapitre 3 : Proposition de Solution

L'objectif de ce mémoire est de renforcer la sécurité de la traçabilité des médicaments dans le respect des normes actuelles mises en place par le GS1. Pour atteindre cet objectif, l'utilisation des normes actuelles est prioritaire, afin d'éviter un changement trop profond de l'organisation de la chaîne d'approvisionnement de l'industrie pharmaceutique. Pour la plupart des grandes entreprises du secteur, la mise en place de leur chaîne d'approvisionnement et le bon fonctionnement de celle-ci furent des étapes clés afin de réduire les coûts des médicaments (et/ou d'augmenter les bénéfices).

3.1. L'adaptation de la traçabilité

La solution présentée dans ce mémoire doit donc être rétro compatible avec les normes actuelles que l'on retrouve pour la traçabilité des médicaments. Il faut donc adapter l'ancien modèle de traçabilité au nouveau.

3.1.1. Datamatrix contre tags RFID

Le modèle actuel de traçabilité mis en place est d'utiliser des datamatrix afin d'assurer la traçabilité. Une alternative aux datamatrix présentée précédemment est l'utilisation des tags RFID. L'avantage clair des tags RFID est qu'un ensemble de médicaments peut être scanné en une seule fois (grâce à des lecteurs lisant les lots), facilitant ainsi le suivi et réduisant les coûts de manutention. En revanche, le prix des tags RFID est prohibitif : il constitue dans certains cas pour des médicaments courants (par exemple le paracétamol) près de 10% du prix de vente. Ce sont pourtant ces médicaments qui ont le plus gros volume de vente, et augmenter le prix de ceux-ci de 10% ne fera que pousser les consommateurs vers des médicaments ou des circuits de distribution « alternatifs » (donc potentiellement dangereux). L'objectif de fond du mémoire étant d'éviter aux consommateurs de devoir passer par des circuits de distributions non officiels afin d'acheter des médicaments à prix compétitif mais falsifiées, la solution de l'utilisation de tags RFID, malgré son potentiel, n'est aujourd'hui pas adaptée pour la traçabilité.

A l'inverse, le prix des datamatrix est faible (dans les millièmes de centime de dollars). En prenant en compte que le modèle actuel de la traçabilité se base sur des datamatrix, le coût est quasi nul : il suffit d'adapter les datamatrix à une traçabilité plus performante. En revanche, l'obligation de scanner chaque boîte de médicament afin de connaître son contenu grâce au datamatrix représente un coût important. Mais il faut remettre les datamatrix dans leur contexte actuel : aujourd'hui deux médicaments (de la même marque, possédant la même molécule active, et partageant le même lot) possèdent le même datamatrix. Ce datamatrix permet aux producteurs du médicament, dans le cas où un des médicaments du lot présente des problèmes, d'identifier et de rappeler rapidement le lot mis en cause, mais du point de vue du consommateur, le numéro de lot ne donne que très peu d'informations.

Rendre ce numéro de lot plus informatif pour le consommateur permettrait à ce dernier de connaître plusieurs informations sur les médicaments qu'il consomme : d'où vient-il, qui l'a produit, par où est-il passé, est-il un médicament officiel... Ces questions, centrales pour le consommateur, sont aujourd'hui délaissées sur le principe que tout le monde achète ses médicaments en pharmacie, ce qui n'est pas forcément vrai. L'explosion des achats en ligne indique que les consommateurs ont tendance à préférer acheter en ligne. La sécurisation de ce secteur, tout en minimisant les coûts de cette sécurisation est donc une clé pour le secteur pharmaceutique. Les datamatrix remplissent tout à fait ce rôle de sécurisation, tout en respectant les contraintes économiques du secteur pharmaceutique, par rapport aux alternatives (notamment les tags RFID).

3.1.2. L'utilisation des datamatrix

Comme vu précédemment, la traçabilité à l'aide de datamatrix se fait grâce à une série de chiffres. Ces chiffres permettent de tracer plusieurs informations concernant le médicament. Ces informations sont les suivantes :

- Un code numéro GTIN (*Global Trade Item Number*) imposé par le GS1). Ces 14 caractères permettent d'identifier le médicament et sa marque (pour rappel, deux médicaments génériques vendus par le même laboratoire, potentiellement sous des marques différentes, auront le même numéro GTIN).
- La date de péremption du médicament, avec le format JJMMAA (JJ correspond au jour, MM au mois et AA à l'année).
- Le numéro de lot du médicament.
- Et des numéros libres permettant à l'agence nationale ou au producteur du médicament d'ajouter des informations sur le médicament en question.

Comme indiqué précédemment, ces informations sont plus utiles au producteur du médicament qu'au consommateur de celui-ci. En revanche rien n'empêche d'utiliser les informations de ce médicament pour permettre au consommateur final d'avoir des informations sur celui-ci. Les numéros libres présent au sein du datamatrix peuvent permettre d'ajouter des informations. Une autre solution serait de modifier le numéro de lot à chaque fois que ce lot est découpé. Cette seconde solution propose plusieurs avantages, avec comme avantage principal l'utilisation d'un système déjà en place.

Mettre à jour le numéro de lot à chaque transfert de médicament, tout en conservant l'historique des numéros de lot de ce médicament permet à la fois de modifier très peu le système actuel, et permet de limiter les investissements des entreprises du secteur pharmaceutique. En effet les technologies actuelles pour imprimer sur les boîtes de médicaments et créer les datamatrix liées aux médicaments sont déjà en place dans les usines des producteurs. Les coûts de mises à jour du système de traçabilité serait donc minimes pour les producteurs actuels.

Mais mettre à jour un système présente toujours des coûts supplémentaires pour certains acteurs de la chaîne d'approvisionnement. Ces acteurs doivent s'équiper de machines afin d'imprimer les datamatrix. Dans le cadre de la solution proposée, imprimer de nouveaux datamatrix se ferait seulement dans le cas où un lot de médicaments se retrouve divisé. Par exemple si un grossiste, qui cherche donc à revendre des médicaments après les avoir achetés souhaite diviser un lot en deux, il doit générer deux nouveaux datamatrix (l'un pour le premier lot, le second pour le second lot) permettant de lier ces deux nouveaux lots au lot initial. Ce lien se fera travers une nouvelle traçabilité basée sur des logiciels, expliquée un peu plus tard dans ce mémoire.

L'idée fondamentale ici c'est que les normes actuelles restent en vigueur. Conserver les normes actuelles permet de laisser aux producteurs de médicaments la liberté de mettre à jour ou non leurs systèmes de traçabilité, et de conserver une rétro compatibilité entre les systèmes. Cette liberté est indispensable, car elle permet aux producteurs de continuer à respecter les législations actuelles tout en adaptant leur système à des normes plus modernes. Aujourd'hui le numéro de lot sur les médicaments a pour but d'aider les producteurs à identifier les médicaments défectueux. Grâce à la génération de nouveaux numéros de lots lors de chaque division d'un lot, numéros de lots liés au lot initial, les producteurs pourront toujours identifier les lots défectueux. Pour le consommateur ces nouveaux numéros de lot présentent l'avantage de connaître le circuit suivi par le médicament, et donc assure la traçabilité de celui-ci.

Pour mieux comprendre cette solution rien de mieux qu'un exemple. Le circuit complet d'un médicament est constitué d'une suite de transfert entre différents propriétaires. Ces propriétaires, qu'il soit le propriétaire initial (donc le producteur), un propriétaire intermédiaire, ou le propriétaire final, doivent chacun déclarer la propriété du médicament à un temps donné. Pour passer la propriété de ce médicament à un autre propriétaire, il faut deux choses :

- La première est que le propriétaire envoie le médicament au prochain propriétaire.
- La seconde que le nouveau propriétaire accepte de recevoir le médicament.

La plupart du temps les médicaments ne sont pas envoyés individuellement, mais sont envoyés par lot. Ces lots, d'une taille variable, circulent entre les propriétaires. L'unique moment lors duquel un médicament est individualisé d'un lot est lors de l'achat de celui-ci par le consommateur final. La traçabilité d'un médicament s'arrête à ce moment-là, car la prochaine étape est la consommation de ce médicament.

Dans le cas où le futur propriétaire refuse le lot de médicaments, il le retourne au propriétaire précédent. Dans le cas où il accepte le lot, il devient propriétaire du lot de médicaments. Il peut à ce moment-là envoyer de nouveau le lot, soit complet soit partitionné. S'il envoie le lot complet, il suffit juste de changer le propriétaire du lot, sans mettre à jour le numéro de celui-ci. A l'inverse s'il décide de partitionner son lot, il se retrouve donc avec deux lots (ou plus si d'autres partitions surviennent). Aucun de ces nouveaux lots n'a la même quantité de médicaments que le lot initial. Il faut donc générer de nouveaux numéros de lot pour chaque lot créé à partir de ce lot initial. Le propriétaire doit à ce moment-là mettre à jour les emballages des médicaments afin que les datamatrix présents sur les emballages soit corrects.

Ci-dessous un schéma permettant de visualiser le fonctionnement de ce système :

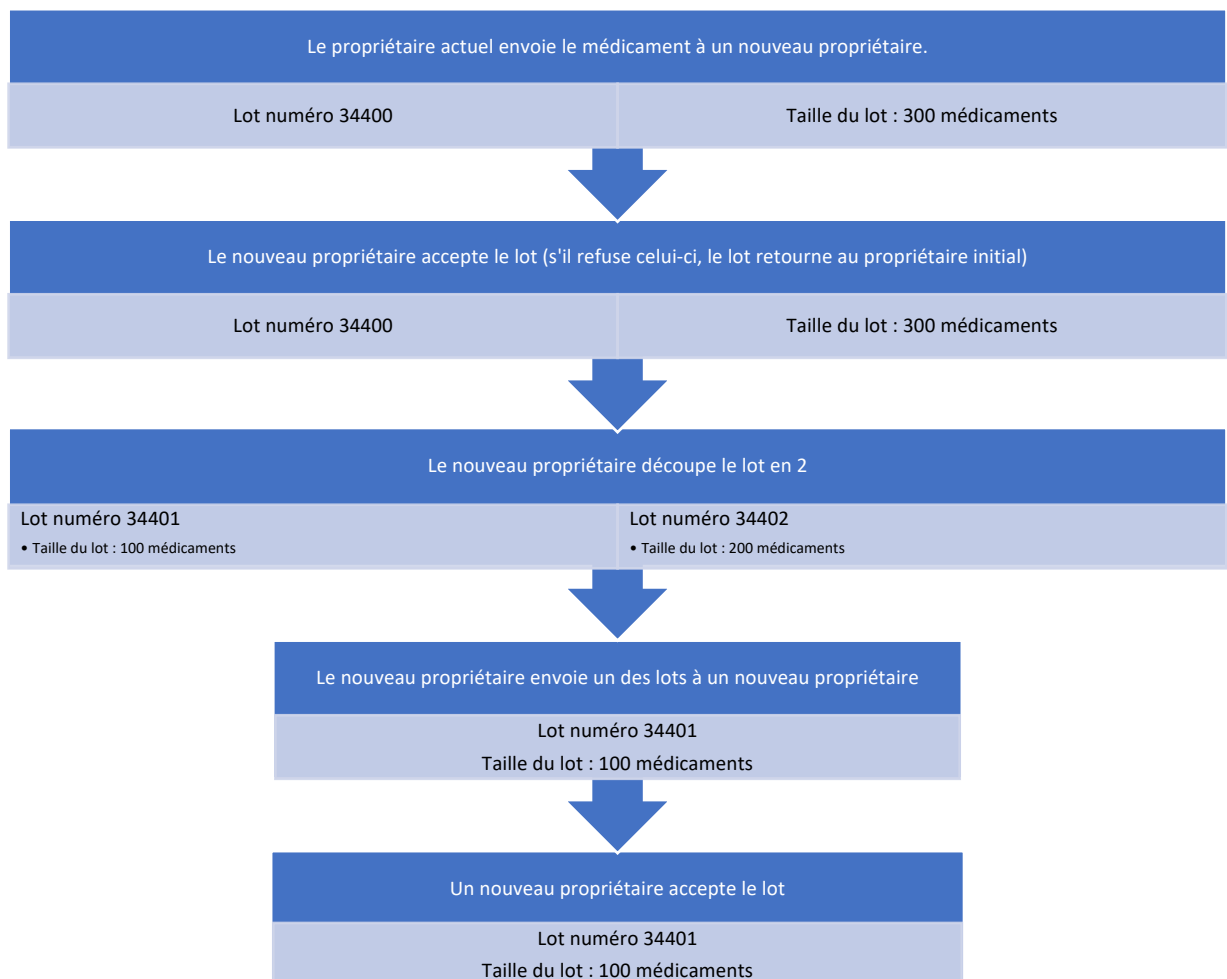


Figure 13 : Flux des numéros de lot

En remontant grâce à ce système les différents propriétaires d'un lot, on peut reconstituer l'origine du lot et son numéro d'origine, ainsi que la liste complète des propriétaires. Le premier

propriétaire du lot dans ce système est le producteur du lot, soit une entreprise pharmaceutique. Grâce à cette nouvelle traçabilité, les modifications apportées au système existant sont minimales : l'unique nouveauté est l'actualisation régulière du datamatrix de chaque emballage de médicaments pour chaque lot. Cette opération peut sembler lourde, mais une automatisation des chaînes de réception et d'envoi est une solution directe à l'actualisation des datamatrix de chaque médicament. Dans un monde qui tend de plus en plus à aller vers l'automatisation, ce système apporte en plus une rapidité d'exécution. On trouve en revanche dans l'automatisation une barrière économique comparable à l'utilisation de tags RFID. Cependant à l'inverse des RFID, la mise en place d'une automatisation se fait une seule fois, tandis qu'un passage par des RFID demanderait à l'ensemble de la chaîne à la fois de passer par l'automatisation des lectures pour chaque lien de la chaîne, et en plus à installer des tags RFID dans chaque boîte de médicaments. Mais l'avantage clair des tags RFID et la rapidité des mises à jour des numéros de lots (il suffit de passer un sous lot devant un lecteur, et de réécrire le numéro de lot pour chaque tag). À plus long terme l'utilisation de tags RFID semble, dans le cas où le prix des tags diminue, une solution idéale. Une solution utilisant des tags RFID serait rétro-compatible avec la solution présentée ici : ce pourrait donc être une étape future pour l'amélioration de la traçabilité des médicaments.

3.2. La conservation des données

En mettant en place une traçabilité avec les datamatrix, il faut stocker les données des médicaments afin que n'importe quel participant puisse interagir avec les données de ceux-ci. Cette interaction se produit en deux parties. Ces deux parties se croisent entre elles, mais sont dissociables sur plusieurs points. La différence la plus importante entre ces parties est comment les données sont stockées : sous forme d'une base de données SQL ou sous la forme d'une blockchain. Comme expliqué précédemment, une blockchain permet de stocker des données de façon permanente et intangible. Chaque donnée enregistrée dans une blockchain ne peut plus être supprimée ensuite : et c'est là le cœur même de la blockchain, qui est de créer un registre de données immutables. Une autre particularité d'une blockchain est qu'elle est distribuée : il existe plusieurs machines ayant le contrôle de celle-ci, et ces machines travaillent entre elles afin de produire un résultat. Ces deux formats de stockages des données sont présents au sein de la solution présentée car ils se complètent : là où la blockchain permet une traçabilité, la base de données de support va permettre d'enrichir les données de la blockchain.

3.2.1. Les données des transactions

Une blockchain permet de stocker des données. Ces données sont permanentes. Cette permanence est un outil concret permettant de garantir l'inviolabilité d'une blockchain et des données qui sont écrites sur celle-ci. Une fois qu'une donnée est écrite dans une blockchain, et qu'elle est validée par les participants de cette blockchain, elle se retrouve permanente. Les chaînes d'approvisionnement ont donc là un outil proposant d'enregistrer l'ensemble des échanges et des transactions. Les données sont écrites sous forme de transactions, et les transactions sont ensuite rangées dans des blocks. Il faut donc déterminer quelles données sont contenues dans les blocks et quelles données sont contenues dans les transactions.

L'objectif de la blockchain de la chaîne d'approvisionnement étant de suivre des transactions entre deux acteurs, il est possible d'en déduire deux des données contenues dans les transactions : deux identifiants permettant d'identifier l'expéditeur du médicament et le récepteur de celui-ci. Ces identifiants, présents sous forme d'identifiant numérique unique, sont liés à la base de données. Dans la base de données, ces identifiants correspondent aux données des acteurs.

Ces données d'identification permettent deux choses :

- La première, identifier un acteur lorsqu'il souhaite faire une transaction sur la blockchain. En effet, tous les acteurs n'ont pas les mêmes droits.

- Deuxièmement, ces données enrichissent les informations concernant les acteurs : leur adresse, leur mail... L'enrichissement de ces données permet d'éviter d'avoir des transactions contenant des dizaines et des dizaines de données. La taille des données dans la blockchain de traçabilité doit être réduite au minimum, tout en conservant un maximum d'informations, afin de garantir une vitesse d'exécution de la blockchain.

3.2.1.1. Les acteurs non identifiés

Les acteurs non identifiés, qui n'ont donc pas de numéro d'identification, peuvent uniquement consulter la blockchain. Ils ne peuvent ni interagir avec celle-ci à travers l'ajout d'une transaction, ni se connecter avec des identifiants. Transposé dans un cas d'utilisation, ces acteurs non identifiés correspondent aux consommateurs finaux des médicaments. Une fois un médicament acheté, et si le nouveau propriétaire souhaite obtenir des informations sur son médicament, il peut scanner le datamatrix présent sur l'emballage du médicament et à l'aide d'une plateforme reliée à la blockchain, obtenir des informations sur le médicament qu'il vient d'acheter (qui ont été les propriétaires successifs, son lieu de fabrication...).

3.2.1.2. Les acteurs identifiés

Un second type d'acteur doit interagir avec la blockchain. Ces acteurs possèdent l'ensemble des droits des acteurs non identifiés, plus d'autres droits. Ils peuvent recevoir des transactions et en accepter. Pour cela, ces acteurs doivent s'enregistrer auprès de la plateforme pour obtenir un numéro d'identification. Ces acteurs correspondent à l'ensemble des acteurs de la chaîne d'approvisionnement de l'industrie pharmaceutique : transporteurs, grossistes, pharmacies, bureaux nationaux... Ce numéro d'identification leur permettra ensuite d'interagir avec la blockchain en liant des transactions à leur numéro d'identification. Le lien entre transaction et acteur se fait si l'acteur est récepteur ou expéditeur d'un médicament. Ces acteurs sont gérés par les autorités locales se chargeant d'autoriser la mise sur le marché de médicaments.

Cela permet d'identifier une autre donnée contenue dans les transactions. Lorsqu'un acteur reçoit un lot de médicament, il peut l'accepter, mais il peut aussi le refuser (par exemple si le lot n'est pas complet, si le récepteur rencontre des problèmes dans le lot...). Il faut donc définir un état pour toutes les transactions. Cet état peut prendre 3 valeurs :

- *accepted* : si le récepteur accepte le lot qui lui a été envoyé. Dans ce cas le récepteur du lot devient le propriétaire
- *refused* : si le récepteur refuse le lot qui lui a été envoyé. Dans ce cas le propriétaire du lot est l'expéditeur. Le lot revient à son propriétaire d'origine.
- *waiting* : si le lot a été envoyé par l'expéditeur, mais que le récepteur n'a pour le moment ni pris la décision de l'accepter ou de le refuser. Le récepteur doit prendre une décision pour changer l'état du lot à « *accepted* » ou « *refused* ».

Un lot peut aussi se voir diviser en 2 lots plus petits : par exemple si un grossiste possède 100 unités d'un médicament X, et qu'il a une commande de 20 unités de ce médicament, il va donc diviser le lot en un lot de 20 et un autre de 80. En plus de générer deux lots avec leur numéro d'identification respectif, il faut aussi signaler dans la blockchain l'actualisation du lot d'origine comme divisé. Il faut donc une valeur pour l'état en plus :

- *split* : le propriétaire d'un lot a pris la décision de partager ce lot en deux. Le lot d'origine est supprimé, et il se retrouve remplacé par deux nouveaux lots. Cependant, l'état *split* n'est pas enregistré dans la blockchain. Lorsqu'un lot est divisé en deux, deux nouveaux lots sont créés. Ce sont donc deux nouvelles transactions à ajouter dans la blockchain, et ces deux transactions sont des transactions de création.

La possibilité de diviser un lot en lots plus petits introduit une nouvelle donnée présente pour les transactions : chaque transaction va avoir des informations sur la taille du lot. Cette taille va permettre de pouvoir diviser un lot en deux lots plus petits.

L'utilisation d'états permet d'avoir rapidement accès au type d'opération que chaque lot peut réaliser : être transféré, être accepté, être refusé ou être divisé. Ce sont les quatre opérations que peut subir un lot.

3.2.1.3. Les fabricants de médicaments

Dans le processus de suivi d'un lot, il faut aussi créer le lot à un moment donné. Créer un lot est une action particulière, car elle implique un paramètre important : le créateur de lot ne peut être qu'un fabricant de médicament. Pour qu'un nouveau lot rentre sur le marché, les producteurs de médicaments doivent mettre en vente le lot en question. Tout ce qui se passe avant pour le lot n'existe pas, du point de vue de la blockchain, avant que le lot soit enregistré. L'enregistrement d'un lot est le moment où celui-ci est ajouté au stock du producteur du médicament, ce qui entraîne l'inscription du lot dans la blockchain. Cet enregistrement ajoute un nouveau type d'acteur, celui de fabricant de médicament. Ces acteurs ont l'ensemble des droits des acteurs non identifiés et des acteurs identifiés, avec en plus le droit d'ajouter des lots à la blockchain.

Lors de l'inscription dans la blockchain de l'ajout d'un lot, ce lot est horodaté. L'horodatage est une autre donnée incluse dans une transaction. Il permet de certifier le moment d'ajout d'un block à la blockchain. Il est un outil pour classer les transactions présentes dans la blockchain. L'ensemble des transactions est ensuite ajouté dans des blocks.

3.2.2. Les données des blocks

Comme indiqué dans la première partie, dans toute blockchain, les transactions sont regroupées au sein de block. Les blocks contiennent des données qui enrichissent les informations qu'ils contiennent. Ces données sont ensuite utilisées pour les différentes opérations que doivent subir les blocks, opérations qui seront détaillées dans une prochaine partie. Les transactions sont rangées dans une liste, avec l'ensemble des données détaillées ci-dessus pour chaque transaction (un numéro de lot, une quantité, l'identifiant du récepteur, l'identifiant de l'expéditeur, un état de la transaction et l'horodatage de celle-ci).

En plus des données des transactions, un block possède des données propres. La première donnée, qui permet de certifier le moment lors duquel le block a été validé et ajouté à la blockchain, c'est l'horodatage de celui-ci. Comme pour les transactions, l'horodatage des blocks va donner des informations sur le moment auquel le block a été ajouté à la blockchain (et donc le moment où celui-ci a été validé). Cependant, l'horodatage n'est pas utile pour classer les transactions.

Pour le classement des transactions les unes par rapport aux autres, chaque block possède un index. Cet index est strictement croissant (à partir de l'index zéro du block « genesis »).

En plus de l'index et de l'horodatage, chaque block possède des données cryptographiques utiles pour supporter la blockchain. Ces données cryptographiques sont un hash, un nonce, et le hash du block précédent. Le hash du block permet de certifier celui-ci, et est calculé à l'aide du hash du block précédent.

La présence du hash du block précédent n'est pas en soit importante pour le calcul du hash du block actuel. Son utilité vient lors de l'ajout d'un block dans la blockchain : si le hash du block précédent dans la blockchain ne correspond pas au hash du block précédent présent dans le block qui doit être ajouté, cela permet de comprendre que le block qui est en train d'être ajouté n'est pas à la bonne place, soit est corrompu. Le hash actuel quant à lui sert à identifier un block par rapport aux autres blocks de la blockchain.

Enfin, chaque block contient un nonce, pour permettre à l'ensemble du réseau de vérifier que le block ajouté a bien été calculé, et qu'il a fallu un travail de la part du mineur du block pour ajouter

celui-ci à la blockchain. Avec le hash du block et le hash du block précédent, ce sont trois outils permettant de vérifier la validité d'un block, et la validité globale de la blockchain.

3.2.3. Les données des médicaments

En plus de contenir les identifiants des acteurs du système de traçabilité, les transactions doivent contenir des informations sur les lots de médicament transférés entre les acteurs. L'identification des lots de médicaments, que ce soit dans la blockchain ou dans la base de données SQL, se fait à l'aide d'identifiants numériques uniques. Ces identifiants permettent de lier entre eux les lots de médicaments avec des données supplémentaires : le nom des médicaments, l'identifiant du fabricant ou bien encore la date d'expiration de ceux-ci. Pour permettre cela, chaque lot et les informations liées à celui-ci sont écrites dans la base de données et dans la blockchain. La différence entre les deux est la localisation des données dans le système d'information.

Pour identifier les lots, que ce soit dans la blockchain ou dans la base de données, chaque lot possède un identifiant unique. Dans la blockchain, cet identifiant du lot permet de suivre les transactions que celui-ci subit. Dans la base de données, l'identifiant de lot va permettre de relier un lot à l'ensemble des données liées à celui-ci. C'est aussi dans la base de données que se trouvent les informations concernant un lot :

- Un identifiant unique, permettant de lier un lot de la base de données à la blockchain.
- Une date d'expiration, indiquant jusqu'à quand un lot de médicament est consommable.
- Une quantité, qui correspond à la taille du lot.
- L'identifiant du médicament composant le lot. Cet identifiant est une clé externe, permettant de faire le lien entre les informations des lots et les informations des médicaments.
- Si un lot est divisé à partir d'un autre lot, on retrouve dans la base de données l'identifiant du lot « parent » dans les données du lot « enfant ». Cet identifiant permet de faire un lien entre tous les enfants d'un est parent.

Grâce à l'identifiant du médicament composant un lot, il est possible de récupérer les informations d'un médicament. Ces informations sont les suivantes :

- Un identifiant unique permettant d'identifier le médicament par rapport aux autres (par exemple si deux médicaments ont le même nom).
- Le nom du médicament, permettant de faire, pour le consommateur, un lien entre la boîte de médicament qu'il vient d'acheter et son ordonnance.
- Le numéro GTIN (*Global Trade Item Number*), qui permet ensuite d'identifier le médicament et sa marque.
- L'identifiant du fabricant du médicament. Cet identifiant, qui fonctionne comme une clé externe, permet d'accéder à des informations supplémentaires concernant le médicament. Ces informations sont celles du fabricant du médicament.

Les fabricants de médicament sont des acteurs. Comme précisé précédemment, il y a trois types d'acteurs qui devront interagir avec la blockchain :

- Les acteurs non identifiés.
- Les acteurs identifiés.
- Les fabricants de médicaments.

L'interaction entre les acteurs et la blockchain se réalise à travers une plateforme web. Les acteurs non identifiés n'ont pas besoin de conserver des informations dans la base de données. Pour les acteurs identifiés et les fabricants de médicaments, la base de données ne fait qu'une légère distinction entre les deux, distinction contenue dans la base de données. Les données des acteurs identifiés et des fabricants de médicaments sont les mêmes, et sont :

- Un identifiant unique afin de distinguer deux acteurs entre eux.

- Un nom, qui peut-être le nom commercial d'un acteur ou son nom auprès de la chambre de commerce locale. L'importance ici n'est pas le nom en soit, et deux acteurs peuvent avoir le même nom (par exemple si tous les centres Novartis souhaitent s'appeler « Novartis », c'est tout à fait possible).
- Un email, identifiant unique, permettant à un acteur de se connecter et de communiquer avec les clients si ceux-ci ont des questions sur un médicament.
- Un mot de passe, haché pour plus de sécurité, qui permet à un acteur de s'identifier sur la plateforme.
- Un numéro de téléphone, pour qu'un consommateur puisse contacter un acteur.
- Un binaire, permettant de distinguer les fabricants de médicaments des acteurs normaux. Ce binaire, vrai si l'acteur est fabricant, faux si l'acteur ne l'est pas. Seul le binaire « vrai » permet d'obtenir pour un acteur le droit d'ajouter des médicaments à la plateforme.

Enfin, les adresses des acteurs sont stockées dans la base de données. Ces adresses contiennent les données suivantes :

- Un identifiant unique pour chaque adresse, qui agit comme clé primaire.
- La rue, contenant le numéro ainsi que le nom de la rue.
- La ville.
- L'état ou région.
- Le code postal lié à l'adresse.
- Le pays.
- Une clé externe permettant de relier une adresse à un acteur.

L'ensemble de ces données sont dans la base de données de la plateforme. Ce sont des données supplémentaires qui permettent à la fois d'obtenir des informations sur les transactions et les acteurs de ces transactions, lui permettant d'interagir avec la blockchain.

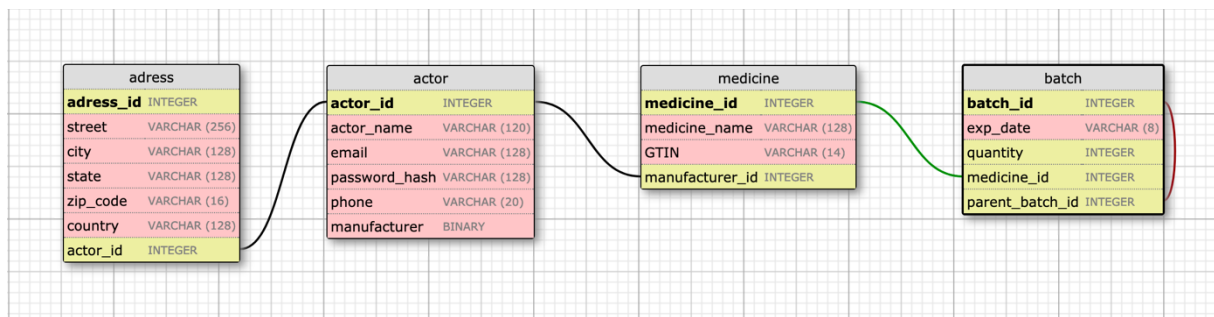


Figure 14: Schéma de la base de données

Ces données, qui servent de données de support, ne sont pas fondamentales pour le fonctionnement de la blockchain. Mais elles sont utiles pour automatiser celle-ci (par exemple l'ajout d'une transaction dans la blockchain est plus facile à réaliser à l'aide de boutons déclenchant une action qu'en rentrant manuellement chaque transaction).

3.3. La blockchain et son fonctionnement

L'ensemble des blocks et des transactions sont liés entre eux dans une blockchain. Cette blockchain possède des données et un ensemble d'interfaces permettant des interactions avec celle-ci. Les données contenues dans la blockchain sont l'ensemble des transactions, contenues dans les blocks minés par les participants. Une des données des nœuds de la blockchain est l'adresse de chaque autre nœud, permettant la décentralisation de celle-ci. Dans l'industrie pharmaceutique, ces nœuds correspondent aux agences nationales qui autorisent les mises sur le marché des médicaments. Pour

la solution proposée, le rôle et la gestion des nœuds de la blockchain seraient donc à la charge des organismes autorisant la mise sur le marché de médicaments. Cette blockchain serait donc semi-publique : sa lecture est possible par n'importe quel acteur (des trois types d'acteurs précédemment identifiés), mais son écriture est un droit réservé aux nœuds, et donc aux agences nationales.

Chaque organisme national gèrerait un nœud accédant la blockchain. Chaque entreprise pharmaceutique souhaitant vendre sur le territoire de l'organisme doit s'enregistrer dans la base de données. La base de données étant globale entre les acteurs, tous les acteurs possèdent un accès à toutes les données concernant les acteurs, les médicaments et les lots (ainsi que secondairement les adresses). Rendre la base de données globale permet d'éviter des collisions entre deux acteurs, deux lots ou deux médicaments ayant les mêmes numéros d'identification. Cela permet en plus pour les lots de médicaments de franchir les frontières : les numéros d'identification étant uniques, un lot peut facilement passer d'un client à un autre sans devoir prendre en compte de limite géographique ou de marché. Laisser la responsabilité des nœuds aux agences nationales permet à celles-ci de filtrer les acteurs (par exemple une entreprise perd son autorisation de mise sur le marché d'un médicament).

Mettre en place cette architecture crée plusieurs conséquences pour le déploiement. La première est que chaque acteur ne peut s'enregistrer qu'auprès d'une seule agence nationale. Cet enregistrement va faire que toutes les requêtes qu'un acteur a auprès de la blockchain vont passer par l'agence nationale avec laquelle cet acteur s'est enregistré. Une seconde conséquence concerne la base de données : celle-ci doit être accessible par l'ensemble des acteurs, sans aucun lien avec les nœuds gérés par les agences nationales. Enfin, les agences nationales doivent s'enregistrer entre elles afin de synchroniser la blockchain est de mettre en place un consensus, afin d'éviter d'avoir deux blockchains complètement différentes entre deux nœuds.

Pour le consensus, plusieurs algorithmes sont possibles. Les principaux algorithmes de consensus ont été évoqués précédemment, et certains peuvent être éliminées. Certains consensus peuvent être éliminés car ils ne répondent pas au cahier des charges : par exemple le consensus par preuve d'enjeu présente comme faille qu'il n'y a aucun jeton à transmettre entre les nœuds dans cette blockchain, et l'utilisation de jetons permettrait aux principaux producteurs de médicaments de contrôler celle-ci. Dans une industrie au sein de laquelle les plus gros acteurs sont régulièrement accusés d'entente, la blockchain serait sous le risque d'une attaque.

Précédemment, l'identification des nœuds de la blockchain comme les organismes nationaux chargés des autorisations de mise sur le marché de médicaments a permis de mettre en avant qu'un groupe restreint possède le monopole de l'actualisation de la blockchain et de l'accès à celle-ci. Ce fonctionnement d'accès à la blockchain par un groupe restreint permet de déduire que le type de consensus lié à cette blockchain est un consensus par preuve d'autorité. La preuve d'autorité permet de valider l'idée que seuls les organismes autorisant la mise sur le marché de médicaments doivent interagir avec la blockchain. C'est par preuve d'autorité que les nœuds de la blockchain vont ajouter des transactions à celle-ci.

En cas de conflit entre deux organismes, une solution simple serait de prendre la blockchain la plus longue depuis le block genesis entre les deux nœuds en conflits, et de faire parvenir cette modification à l'ensemble des acteurs. Le nœud ayant la blockchain la plus courte voit sa blockchain remplacée par celle plus longue. Cette solution, simple, permet de créer un niveau initial d'exigences. Tout système de résolution de conflits moins performant que cette solution doit donc être éliminé. Tous les nœuds ont les mêmes droits sur la blockchain, aucun ne peut prétendre être plus important que les autres, et donc en cas de conflit imposer sa blockchain pour les autres.

Résumer en un schéma permet de mieux comprendre l'architecture de la solution. Pour créer ce schéma simplifié, deux agences nationales et quatre acteurs (deux pour chaque agence) sont utilisés, et l'architecture de la solution ressemblerait à la figure suivante :

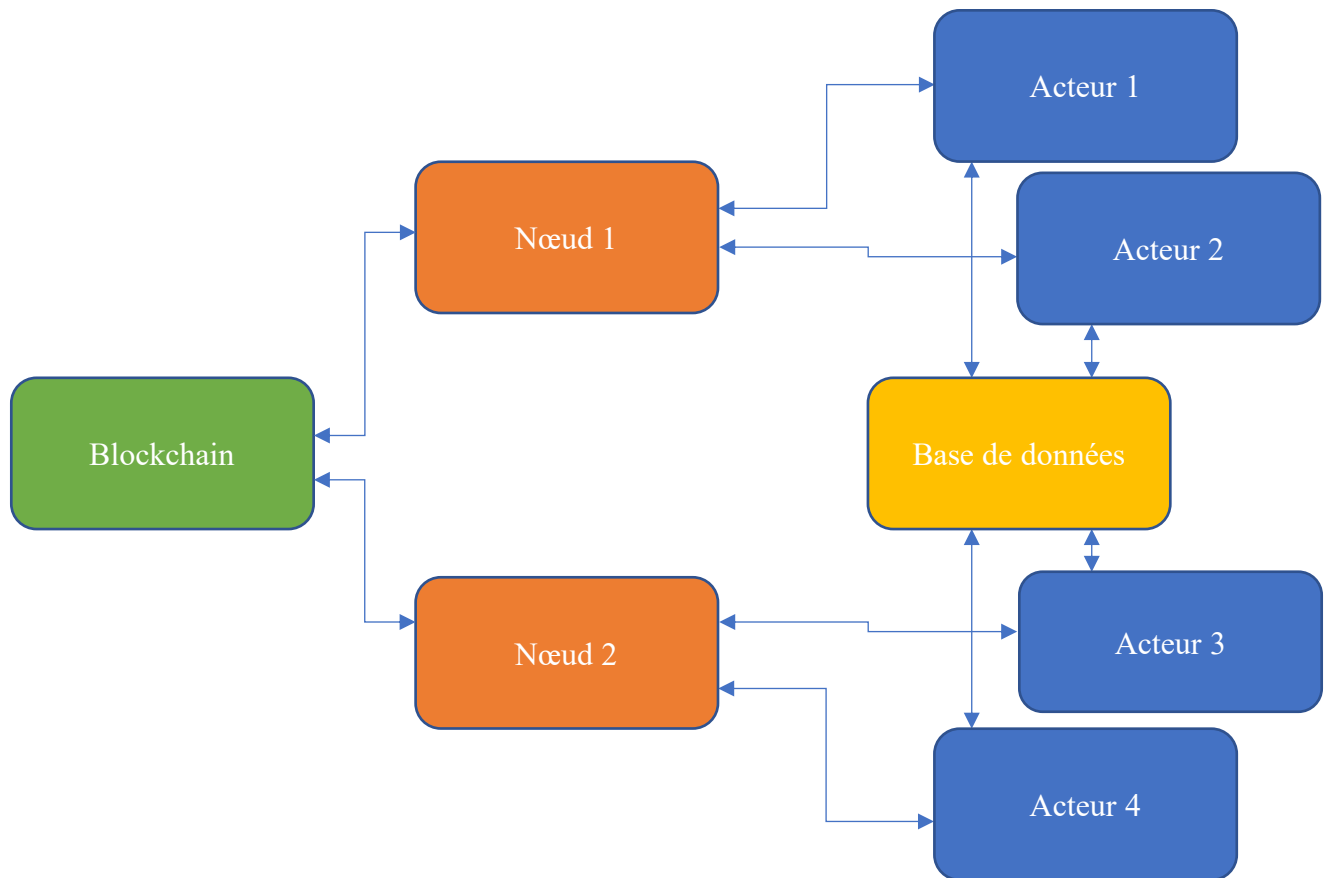


Figure 15: Architecture de la solution

3.4. Récits d'utilisateurs de la solution

L'architecture de la solution proposée, il faut maintenant définir les différentes actions des acteurs. Pour définir celles-ci, les récits d'utilisateurs sont un outil adapté. Grâce à ceux-ci, la détermination des actions des différents acteurs va permettre de poser les bases de la validation de la solution.

Lors de l'identification des acteurs, trois acteurs ayant accès à la plateforme ont été identifiés : les acteurs non identifiés, les acteurs identifiés et les fabricants de médicaments. En plus de ces trois acteurs, un quatrième existe : ce sont les organismes d'autorisation de mise sur le marché de médicaments. Ces organismes auront le contrôle des nœuds, et doivent répondre à un cahier des charges afin d'effectuer intelligemment les actions sur la blockchain.

Les acteurs non identifiés correspondent aux consommateurs souhaitant obtenir des informations sur les médicaments qu'ils achètent : pour cette catégorie d'acteurs, les récits d'utilisateurs sont les suivants :

- *En tant que consommateur, je veux lire un datamatrix afin d'obtenir des informations sur le médicament que je viens d'acheter (1).*
- *En tant que consommateur, je veux lister les différents propriétaires d'un médicament afin de m'assurer de la provenance et de l'origine du médicament (2).*
- *En tant que consommateur, je veux visualiser la blockchain afin d'avoir des informations sur les différents acteurs de la chaîne d'approvisionnement de l'industrie pharmaceutique (3).*

Les acteurs identifiés correspondent aux différents intermédiaires entre les producteurs de médicaments et les consommateurs. Ces intermédiaires peuvent être des grossistes, des transporteurs, des hôpitaux... Une partie des récits d'utilisateurs de ceux-ci sont les mêmes que pour les acteurs non identifiés, avec plusieurs ajouts :

- *En tant qu'intermédiaire, je veux pouvoir recevoir des lots de médicaments afin de les ajouter à mon stock (4).*
- *En tant qu'intermédiaire, je veux pouvoir accepter ou refuser des lots de médicaments afin de gérer mes réceptions de médicaments et détecter les lots défectueux (5).*
- *En tant qu'intermédiaire, je veux pouvoir m'enregistrer, me connecter et me déconnecter de mon compte afin d'être le seul à pouvoir gérer mes transactions (6).*
- *En tant qu'intermédiaire, je veux consulter mon profil afin de modifier des informations (7).*
- *En tant qu'intermédiaire, je veux pouvoir lister les lots de médicaments en ma possession afin d'obtenir un état des lieux de mon stock actuel (8).*
- *En tant qu'intermédiaire, je veux pouvoir envoyer un lot de médicament afin de vendre ceux-ci (9).*
- *En tant qu'intermédiaire, je veux filtrer les lots de médicaments afin de visualiser les médicaments pour lesquelles une action de ma part doit être effectuée (10).*
- *En tant qu'intermédiaire, je veux pouvoir demander aux nœuds auquel je suis connecté d'actualiser la blockchain afin de confirmer mes transactions et d'ajouter celles-ci à la blockchain (11).*
- *En tant qu'intermédiaire, je veux diviser un lot de médicament afin de répondre à la demande d'un client (12).*
- *En tant qu'intermédiaire, je veux générer des datamatrix afin d'actualiser les boîtes de médicaments qui transitent par moi (13).*

Le troisième type d'acteur, fabricant de médicaments, regroupe l'ensemble des récits d'utilisateurs des acteurs non identifiés et des acteurs identifiés, avec en plus d'autres récits d'utilisateurs :

- *En tant que fabricant de médicament, je veux pouvoir ajouter des médicaments avec leur numéro de GTIN lié afin de créer des lots de ceux-ci dans la blockchain (14).*
- *En tant que fabricant de médicament, je veux créer des lots de médicaments avec la date d'expiration et la quantité liée à ceux-ci afin de commencer la traçabilité de ceux-ci (15).*

Lors de la validation de la solution proposée, les récits d'utilisateurs vont permettre de valider la solution, et de lier celle-ci à des contraintes. A partir de l'ensemble du cahier des charges défini, avec le fonctionnement de la blockchain, l'architecture de la solution et les récits d'utilisateurs, il faut maintenant valider la solution après avoir développé celle-ci.

Chapitre 4 : Validation de la Solution

Pour valider la solution, il faut dans un premier temps l'implémenter. Par choix technique, l'implémentation de la solution est en python, avec l'utilisation du framework Flask⁵. C'est un framework orienté vers les applications web, avec un moteur de template (Jinja2) pour générer les pages web. Ce framework présente l'avantage d'être léger : il vient avec très peu de paquets initialement. Ce framework contient un serveur de développement ainsi qu'un débogueur et la gestion de cookies de session. A l'inverse d'autres framework (Django notamment), peu de paquets sont installés initialement et cela permet à Flask d'être assez vite adaptable à des besoins spécifiques. La communauté supportant le framework est importante, et développe régulièrement des extensions adaptées à celui-ci.

4.1. La gestion des données

Comme indiqué précédemment, les données sont stockées dans deux espaces différents : une base de données, et une blockchain.

4.1.1. La gestion de la base de données

Pour la gestion de la base de données, Flask possède une extension nommée Flask-SQLAlchemy⁶, une extension de SQLAlchemy. SQLAlchemy est un outil contenant un mapper objet-relationnel, permettant de convertir des requêtes écrites en python en SQL. L'objet central de ce mémoire étant la blockchain, la présentation de la base de données liée va être minimale. SQLite est adapté pour cela : en conservant la base de données dans un fichier local, il évite d'avoir à utiliser une configuration plus lourde avec un serveur (par exemple en utilisant PostgreSQL). Pour éviter des conflits, et simplifier le développement, il faut pouvoir migrer facilement la base de données entre deux versions : une autre extension de Flask permettant de faire cela est Flask-Migrate.

Au moment de programmer, le mapper de Flask-SQLAlchemy permet de faire le lien entre un modèle codé en python et la table de la base de données liée. Par exemple pour les acteurs, le code du modèle en python sera le suivant :

```
class Actor(UserMixin, db.Model):
    id = db.Column(db.Integer, primary_key=True)
    actor_name = db.Column(db.String(120), index=True, unique=True)
    email = db.Column(db.String(120), index=True, unique=True)
    password_hash = db.Column(db.String(128))
    phone = db.Column(db.String(20))
    manufacturer = db.Column(db.Boolean, unique=False)
```

Il faut souligner que le code écrit dans le mémoire (et non celui des annexes) est adapté pour être lisible. Certaines fonctions et propriétés n'apportant rien à la compréhension ne sont pas écrites. A partir de ce code, Flask-SQLAlchemy se charge de générer la table de données. Flask-SQLAlchemy, car c'est un mapper objet-relationnel, permet d'insérer des données dans la base sans passer par l'écriture de code. Par exemple pour ajouter un nouvel acteur à la base de données :

```
actor = Actor(actor_name=form.actor_name.data, email=form.email.data, phone=form.phone.data,
manufacturer=form.manufacturer.data)
```

⁵ <https://palletsprojects.com/p/flask/>

⁶ <https://flask-sqlalchemy.palletsprojects.com/en/2.x/>

L'ensemble des tables de la base de données sont construites sur le même modèle. L'abstraction de l'interaction avec la base de données obtenue grâce à Flask-SQLAlchemy permet une gestion rapide et facile de la base de données.

4.1.2. La gestion de la blockchain

La blockchain est stockée sous forme de structure de données par les différents nœuds. Lorsqu'il est indiqué que tous les nœuds ont accès à la même blockchain, tous les nœuds stockent leur propre blockchain, mais avec l'intention d'avoir les mêmes données. En cas de désynchronisation, les nœuds doivent alors chercher à trouver un consensus afin d'avoir les mêmes données. Les interactions avec la blockchain se font à travers une API Rest. Utiliser une API offre la possibilité à certaines entreprises du secteur pharmaceutique de développer leur propre couche logiciel pour l'interface. Cela permettrait aussi à ces mêmes entreprises d'intégrer le suivi de médicament dans la blockchain à leur propre programme existant de suivi de la chaîne d'approvisionnement. Pour cela, ces entreprises doivent uniquement s'enregistrer auprès d'un nœud de la blockchain, et avec la base de données.

La première étape est de connecter les nœuds entre eux. S'il y a deux nœuds qui fonctionnent sur les adresses `http://localhost:8000/` et `http://localhost:8001/`, il faut connecter les nœuds de la forme suivante :

- Depuis le nœud sur le port 8000, il faut réaliser une opération POST sur la route `http://localhost:8000/register_with` et avec l'objet JSON :

```
{
  "node_address": "http://localhost:8001"
}
```

Cet objet JSON contient l'adresse du nœud auprès duquel ce nœud souhaite se connecter.

- Depuis le nœud sur le port 8001, il faut réaliser une opération POST sur la route `http://localhost:8001/register_with` et avec l'objet JSON :

```
{
  "node_address": "http://localhost:8000"
}
```

Cet objet JSON contient l'adresse du nœud auprès duquel ce nœud souhaite se connecter.

Pour la gestion des nœuds, l'ensemble se fait grâce à des routes exécutant des fonctions internes au nœud. Ces nœuds sont les suivants :

- `/register_node` : enregistre de nouveaux nœuds passés en paramètres (sous forme d'un JSON) auprès du nœud actuel.
- `/register_with` : enregistre le nœud actuel auprès d'autres nœuds passés en paramètres (sous forme d'un JSON)
- `/add_block` : ajoute un nouveau block au nœud actuel. Pour ajouter un block, cette route nécessite de recevoir les informations du block. Ces informations sont l'index du block (*index*), les transactions contenues dans le block (*transactions*), l'horodatage de l'heure à laquelle le block fut ajouté (*timestamp*), le hash du block précédent à celui ajouté actuellement (*previous_hash*), et le nonce du block (*nonce*)

Une fois deux nœuds connectés entre eux, l'interaction avec les nœuds se fait à travers les routes suivantes :

- `/new_transaction` : permet d'enregistrer une nouvelle transaction dans la blockchain. Cette route a besoin de recevoir le numéro unique du lot qui va être transmis (*batch_id*), le numéro unique de l'expéditeur (*sender_id*), le numéro unique du destinataire (*recipient_id*), et la taille du lot à envoyer (*quantity*).
- `/response_transaction` : permet d'enregistrer la réponse d'une transaction (acceptation ou refus de celle-ci) lorsqu'un acteur souhaite transmettre un batch à un autre acteur. Cette route

a besoin de recevoir le numéro unique du lot qui va être transmis (*batch_id*), le numéro unique de l'expéditeur (*sender_id*), le numéro unique du récepteur (*recipient_id*), la taille du lot à envoyer (*quantity*) ainsi que le statut actuel de la transaction à effectuer.

- */register_batch* : permet pour un fabricant de médicaments d'ajouter un nouveau lot à partir d'un médicament. Cette route a besoin de recevoir le numéro unique du lot qui va être enregistré dans la blockchain(*batch_id*), le numéro unique de l'expéditeur (*sender_id*) et la taille du lot à envoyer (*quantity*).
- */chain* : permet de demander à un nœud la blockchain complète que celui-ci stocke.
- */mine* : permet de demander à un nœud de « miner » les transactions non confirmées actuellement et d'ajouter celles-ci à la blockchain.
- */unconfirmed_transactions* : permet de lister l'ensemble des transactions non confirmées actuellement pour un nœud.

4.2. Interaction avec la base de données

L'interaction avec la base de données se fait à partir du client. Mais ces routes permettent aussi aux acteurs d'appeler les routes des nœuds auxquels ceux-ci sont connectés. La plupart des transactions dans la blockchain ont besoin du support de la base de données (pour récupérer les identifiants des lots par exemple), et donc en interagissant avec la base de données grâce à ces routes, les acteurs passent par la base de données pour construire les requêtes qui s'adressent à la blockchain.

- */* : route de l'index qui permet d'afficher la blockchain. Cette route est publique, n'importe quel type d'acteur peut y accéder. Cette route fait appel à la route du nœud */chain*.
- */update_connected_node_address/<address>* : route prenant en paramètres une adresse de nœud auquel le client va se connecter.
- */actor/<actor_name>* : route prenant en paramètre le nom d'un acteur et qui renvoie son profil. Cette route est accessible à n'importe quel type d'acteur, car elle va permettre à un acteur non identifié d'obtenir des informations sur les différents acteurs par qui est passé le médicament qu'il vient d'acheter, et qui a manipulé le médicament.
- */actorID/<actor_id>* : route prenant en paramètre le numéro unique d'identification d'un acteur et qui renvoie le profil de l'acteur en question. Cette route, tout comme la précédente, permet à un consommateur d'avoir des informations sur qui a possédé le médicament qu'il vient d'acheter.
- */batch/<batch_id>* : route accédant à la page d'un lot grâce au passage de son numéro unique en paramètre, avec l'ensemble des informations du lot listées sur la page en question (le nom du médicament du lot, la taille du lot et les transactions du lot).
- */user_medicine* : route listant tous les médicaments liés à un fabricant. Cette route permet au fabricant d'arriver à une page depuis laquelle il peut ajouter des médicaments dans la base de données et créer de nouveaux lots.
- */request_mine* : route permettant à un acteur de requêter au nœud auquel il est connecté de miner un nouveau block.
- */fetch_medicine_for_user_id* : route permettant de récupérer l'ensemble des médicaments liés à un utilisateur, grâce au numéro unique de celui-ci.
- */new_medicine* : route permettant de créer un nouveau médicament et d'ajouter celui-ci en base de données pour un fabricant. Cette route a besoin de connaître le nom du médicament à ajouter et le numéro GTIN de celui-ci.
- */new_batch* : route permettant, pour un fabricant, de créer un nouveau lot de médicaments avec une date de péremption et une quantité associée et d'ajouter celui-ci à la blockchain.
- */send_batch* : route permettant pour un acteur identifié ou un fabricant d'envoyer un batch à un autre acteur grâce au numéro unique. L'expéditeur doit spécifier la taille du lot à envoyer. La date de péremption du lot envoyé reste la même que celle du lot initial.

- */user_transactions* : route listant l'ensemble des transactions « actives » (c'est-à-dire pour lesquelles un acteur peut prendre les décisions d'accepter un lot, de refuser un lot et d'envoyer un lot) liées à un acteur.
- */submit_accept_transaction* : route permettant à un acteur d'accepter ou de refuser un lot lorsque celui-ci est envoyé par un autre acteur.
- */decode_datamatrix* : route prenant en entrée un datamatrix, reliant ce datamatrix à un lot et affichant la page du lot en question. Si le lot n'existe pas, l'utilisateur est informé de son erreur.
- */login* : route permettant à un acteur de se connecter.
- */logout* : route permettant à un acteur de se déconnecter.
- */register* : route permettant à un acteur de s'enregistrer.

4.3. Validation des récits d'utilisateurs

Utiliser les récits d'utilisateurs comme références va permettre de confirmer le bon fonctionnement du programme et l'atteinte des objectifs du mémoire. Pour rappel, les récits d'utilisateurs furent découpés en trois catégories : ceux des acteurs non identifiés, ceux des acteurs identifiés et ceux des fabricants de médicaments.

4.3.1. Récits d'utilisateurs des acteurs non identifiés

- *En tant que consommateur, je veux lire un datamatrix afin d'obtenir des informations sur le médicament que je viens d'acheter.*

Pour valider ce récit d'utilisateur, il faut pouvoir lire un datamatrix et relier celui-ci à la page du lot lié à ce datamatrix. Cette page doit lister l'ensemble des informations du lot.

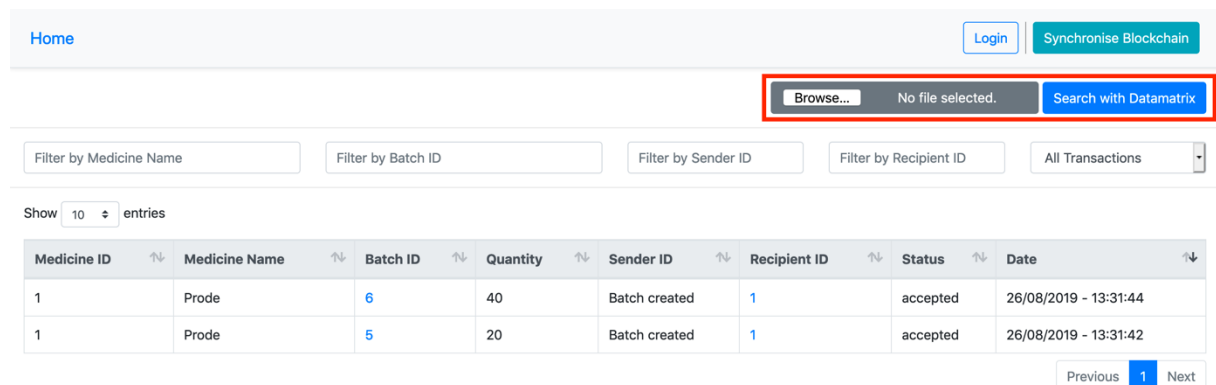


Figure 16: Page d'index

Dans la figure 16, on retrouve la page d'index avec la zone d'importation d'un datamatrix. Une fois qu'un datamatrix est importé, et si les données de celui-ci correspondent à un lot de médicament, l'utilisateur est alors redirigé vers le lot de médicament en question.

Home

Login

Synchronise Blockchain



Batch 5

Medicine: Prode [ID number: 1]

Quantity: 20

Sender ID	Recipient ID	Batch ID	Quantity	Status	Date
1	1	5	20	accepted	26/08/2019 - 13:31:42

Figure 17: Page d'un lot de médicament, avec les transactions de ce lot

La figure 17 liste les informations d'un médicament dans la partie supérieure. La partie inférieure liste les différentes transactions et les différents propriétaires d'un médicament.

- En tant que consommateur, je veux lister les différents propriétaires d'un médicament afin de s'assurer de la provenance et de l'origine du médicament.

Home

Login

Synchronise Blockchain



Batch 8

Medicine: Nouvel [ID number: 2]

Quantity: 10

Sender ID	Recipient ID	Batch ID	Quantity	Status	Date
2	1	8	10	accepted	26/08/2019 - 15:08:47
2	1	8	10	waiting	26/08/2019 - 15:08:31
2	2	8	10	accepted	26/08/2019 - 15:08:21

Figure 18: Informations sur les propriétaires successifs d'un médicament

A la suite de l'import d'un datamatrix, un consommateur peut lister les différents propriétaires d'un lot, le statut du lot après chaque transaction, et les dates des transactions. Le consommateur peut alors sélectionner les identifiants de l'expéditeur (*sender*) et du récepteur (*recipient*) pour avoir des informations sur la localisation de ceux-ci.

- En tant que consommateur, je veux visualiser la blockchain afin d'avoir des informations sur les différents acteurs de la chaîne d'approvisionnement de l'industrie pharmaceutique.

Pour lister la blockchain, un consommateur doit se rendre sur la page d'index et visualiser les différentes transactions des médicaments. Il peut aussi filtrer les transactions grâce à plusieurs filtres : le nom du médicament, le numéro de lot, le numéro de l'expéditeur, le numéro du récepteur et le statut du lot.

Home
Login
Synchronise Blockchain

Browse...
No file selected.
Search with Datamatrix

Filter by Medicine Name
Filter by Batch ID
Filter by Sender ID
Filter by Recipient ID
All Transactions

Show 10 entries

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Recipient ID	Status	Date
2	Nouvel	8	10	2	1	accepted	26/08/2019 - 15:08:47
2	Nouvel	8	10	2	1	waiting	26/08/2019 - 15:08:31
2	Nouvel	8	10	Batch created	2	accepted	26/08/2019 - 15:08:21
2	Nouvel	7	30	Batch created	2	accepted	26/08/2019 - 15:08:19
1	Prode	6	40	Batch created	1	accepted	26/08/2019 - 13:31:44
1	Prode	5	20	Batch created	1	accepted	26/08/2019 - 13:31:42

Previous
1
Next

4.3.2. Récits d'utilisateurs des acteurs identifiés

- *En tant qu'intermédiaire, je veux pouvoir recevoir des lots de médicaments afin de les ajouter à mon stock.*

Le cœur de la blockchain est de pouvoir gérer des transactions entre différents acteurs. Les principaux acteurs de ces transactions sont les intermédiaires. Pour recevoir un lot de médicaments, un intermédiaire nécessite de s'enregistrer afin d'obtenir un numéro d'identification. Ce numéro d'identification va ensuite servir d'adresse lorsqu'un autre utilisateur souhaite lui envoyer un lot.

- *En tant qu'intermédiaire, je veux pouvoir accepter ou refuser des lots de médicaments afin gérer mes réceptions de médicaments et détecter les lots défectueux.*

Lorsqu'un intermédiaire se trouve sur la page de gestion des transactions, il peut choisir d'accepter ou de refuser un lot. Il doit alors confirmer son choix.

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
1	Prode	11	5	1	✓ Accept Refuse	26/08/2019 - 16:48:47	Confirm

Figure 19: Acceptation ou refus d'un lot

- *En tant qu'intermédiaire, je veux pouvoir m'enregistrer, me connecter et me déconnecter de mon compte afin d'être le seul à pouvoir gérer mes transactions.*

Pour accéder à leur compte, les acteurs identifiés ont accès à une page d'identification. Sur cette page d'identification, l'utilisateur peut se connecter s'il possède un compte, ou s'inscrire.

Figure 20: Page de login

Si l'utilisateur souhaite s'enregistrer, il peut accéder à la page d'enregistrement qui lui permet de rentrer les informations utiles de son profil. Il faut remarquer la présence d'un bouton à cocher « manufacturer » permettant de préciser si le profil utilisé est un profil de fabricant de médicament ou non.

Figure 21: Page d'inscription

Une fois connecté, un utilisateur peut se déconnecter à l'aide d'un bouton « Logout ».

Figure 22: Bouton de déconnection

- En tant qu'intermédiaire, je veux consulter mon profil afin de modifier des informations.

Sur la page de profil d'un utilisateur, celui-ci peut visualiser les informations le concernant, et cliquer sur le bouton d'édition de profil pour modifier les informations le concernant.

[Home](#)
Manage Transactions
Profile
Synchronise Blockchain

Your Profile

Transporteur

ID: 3

Informations

Email: transporteur@test.com

Manufacturer: False

Phone: +56945623400

Adress

Street: 200 Avenida Espana

City: Valparaiso

State: Valparaiso

ZIP Code: 2340000

Country: Chili

Edit

Figure 23: Profil d'un utilisateur

- En tant qu'intermédiaire, je veux pouvoir lister les lots de médicaments en ma possession afin d'obtenir un état des lieux de mon stock actuel.

Un utilisateur peut visualiser son stock de médicaments actuel grâce à l'onglet « Manage Transactions ».

[Home](#)
Manage Transactions
Profile
Synchronise Blockchain

Batch ID
Quantity
Recipient ID
Send Batch
Show All the Batches
Filter the Waiting Batches

Search by ID
Search by Medicine Name
Search by Batch ID
Search by Sender ID
All Transactions

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
2	Nouvel	8	10	1	accepted	26/08/2019 - 16:21:20	
1	Prode	9	10	1	Accept	26/08/2019 - 16:21:03	Confirm

Figure 24: Visualisation du stock d'un utilisateur

- En tant qu'intermédiaire, je veux pouvoir envoyer un lot de médicament afin de vendre ceux-ci.

L'envoi d'un lot de médicament se fait depuis la page de gestion des transactions.

8
10
2
Send Batch

Figure 25: Envoi du lot 8 de taille 10 à l'acteur ayant le numéro d'identification 2

- En tant qu'intermédiaire, je veux filtrer les lots de médicaments afin de visualiser les médicaments pour lesquelles une action de ma part doit être effectuée.

Les lots sur lesquels un acteur doit réaliser une action sont ceux ayant le statut « waiting ». Lorsqu'un lot a ce statut, l'acteur peut soit accepter soit refuser la transaction. Pour filtrer les lots ayant

ce statut, il existe dans la page de gestion des transactions d'un utilisateur un bouton « Filter the Waiting Batch » qui permet de lister uniquement les lots ayant le statut « waiting ».

The interface includes filters for Batch ID, Quantity, and Recipient ID, along with buttons for 'Send Batch', 'Show All the Batches', and 'Filter the Waiting Batches' (highlighted with a red box). Below the filters are search boxes for ID, Medicine Name, Batch ID, and Sender ID, and a dropdown for 'All Transactions'. A table displays transaction details:

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
1	Prode	9	10	1	Accept	26/08/2019 - 16:21:03	Confirm

Figure 26: Filtrage des médicaments

- En tant qu'intermédiaire, je veux pouvoir demander au nœud auquel je suis connecté d'actualiser la blockchain afin de confirmer mes transactions et d'ajouter celles-ci à la blockchain.

Pour demander à actualiser la blockchain, un utilisateur peut cliquer sur le bouton « synchronise blockchain ».

The interface shows a 'Manage Transactions' section with a 'Profile' dropdown and a 'Synchronise Blockchain' button (highlighted with a red box).

Figure 27: Bouton de demande de synchronisation de la blockchain

- En tant qu'intermédiaire, je veux diviser un lot de médicament afin de répondre à la demande d'un client.

Lorsqu'un acteur envoie un lot moins grand que la taille du lot original, le lot se divise en deux sous lots et l'un des sous lots est envoyé au destinataire du lot.

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Recipient ID	Status	Date
1	Prode	12	5	1	2	waiting	26/08/2019 - 16:42:31
1	Prode	12	5	Batch created	1	accepted	26/08/2019 - 16:42:31
1	Prode	11	5	Batch created	1	accepted	26/08/2019 - 16:42:31
1	Prode	10	10	Batch created	1	accepted	26/08/2019 - 16:39:22

Figure 28: Division d'un lot en deux, et envoi de l'un des sous lots

- En tant qu'intermédiaire, je veux générer des datamatrix afin d'actualiser les boîtes de médicaments qui transitent par moi.

Lorsqu'il visualise un lot de médicament, le datamatrix lié au lot est disponible sur la page du lot.



Batch 12

Medicine: Prode [ID number: 1]

Quantity: 5

Sender ID	Recipient ID	Batch ID	Quantity	Status	Date
1	2	12	5	waiting	26/08/2019 - 16:42:31
1	1	12	5	accepted	26/08/2019 - 16:42:31
1	1	10	10	split	26/08/2019 - 16:39:22

Figure 29: Visualisation du datamatrix d'un lot

4.3.3. Récits des fabricants de médicaments

Les fabricants de médicaments ont accès à un onglet spécifique depuis lequel ils peuvent gérer les médicaments. Cet onglet s'appelle « Manage Medicine ».

- En tant que fabricant de médicament, je veux pouvoir ajouter des médicaments avec leur numéro de GTIN lié afin de créer des lots de ceux-ci dans la blockchain.

[Home](#)
Manage Medicine
Manage Transactions
Profile
Synchronise Blockchain

Add New Medicine

#	Medicine Name	GTIN	Expiration Date	Quantity	
1	Prode	3450	01/01/2020		Add New Batch

Figure 30: Ajout d'un nouveau médicament dans la base de données

Depuis l'onglet de gestion des médicaments, un fabricant peut ajouter un nouveau médicament en indiquant le nom du médicament et le GTIN de celui-ci.

- En tant que fabricant de médicament, je veux gérer des lots de médicaments avec la date d'expiration et la quantité liée à ceux-ci afin de commencer la traçabilité de ceux-ci.

[Home](#)
Manage Medicine
Manage Transactions
Profile
Synchronise Blockchain

Add New Medicine

#	Medicine Name	GTIN	Expiration Date	Quantity	
1	Prode	3450	01/01/2020		Add New Batch

Figure 31: Ajout d'un nouveau lot de médicament

Une fois un médicament ajouté à la base de données, un fabricant peut créer des lots lorsqu'il le souhaite et ajouter ces lots dans la blockchain et la base de données.

4.4. Exemples de tentatives de corruption de la blockchain

Une seconde étape de la validation de la solution est la vérification que celle-ci permet bien d'empêcher la corruption de la chaîne d'approvisionnement par un tiers. Pour cela, deux cas

d'exemples concrets vont être présentés : le cas où un transporteur souhaite ajouter des médicaments extérieurs, et le cas où un lot de médicaments est gonflé afin de modifier la quantité du lot.

4.4.1. Ajout de médicaments extérieurs par un transporteur

Un premier exemple de tentative de corruption de la chaîne d'approvisionnement serait la tentative de la part d'un transporteur d'ajouter des médicaments extérieurs dans la blockchain. L'ajout d'un médicament extérieur, et son suivi dans la blockchain ne peut être réalisé uniquement par un fabricant de médicaments (afin d'obtenir un identifiant unique pour le lot de médicament). Un transporteur ne pourrait donc pas ajouter de médicament extérieur. Mais il a la possibilité de remplacer un lot de médicaments par un autre lot de médicaments (et de deux médicaments différents). Le remplacement d'un lot par un autre présente cependant un problème. Lorsque le transporteur en question va tenter de transférer le lot à un autre propriétaire, celui-ci va se rendre compte que le médicament qu'il souhaite se procurer n'est pas celui qu'il reçoit. Cette distinction va le pousser à refuser le lot transféré, et le transporteur conserve le lot en conséquence. Pour le transporteur, sa seule solution est de réintroduire le médicament initial, afin d'effectuer le suivi de celui-ci.

4.4.2. Modification de la quantité d'un lot

Un autre exemple de tentative de corruption du suivi est l'augmentation de la quantité de médicaments contenue dans un lot. Un acteur peut par exemple tenter de doubler la taille d'un lot, en ajoutant au lot des copies du médicament original. Cependant, cette tentative se déroulerait lors du transfert d'un lot (le seul moment lors duquel un acteur qui n'est pas fabricant peut modifier la taille d'un lot). Seulement, des garde-fous existent : la quantité de médicaments par lot est présente dans la blockchain, et tenter de transférer un lot plus important va entraîner le refus du transfert par la blockchain. Par ce moyen, il devient impossible pour un acteur de modifier la taille d'un lot : il peut uniquement envoyer un sous lot à un autre acteur, ou le lot complet.

Chapitre 5 : Conclusion

5.1. Conclusions générales

L'utilisation d'une blockchain, et l'amélioration de la traçabilité liée à cette utilisation, permet d'avoir une traçabilité claire d'un médicament, du fabricant au vendeur final. Cette traçabilité offre l'impossibilité pour des agents extérieurs de faire entrer dans la chaîne d'approvisionnement de l'industrie pharmaceutique des médicaments non autorisés. La blockchain permet en plus de créer un arbre de lots, dans lequel les lots se retrouvent divisés en sous-lots.

Pour réaliser cette traçabilité, la solution permet de suivre un médicament à l'aide d'un numéro de lot unique, et d'actualiser ce numéro de lot en cas de modification de la taille du lot. L'actualisation de ce numéro de lot passe par l'actualisation du datamatrix présent sur la boîte de médicament : aujourd'hui, cette solution est la plus adaptée pour une raison économique, mais à l'avenir, l'utilisation de puces RFID présente un fort potentiel, en comparaison avec l'utilisation de datamatrix.

Mettre en place une traçabilité précise des médicaments présente en revanche la limite de ne pas être tant favorable que cela pour les entreprises du secteur pharmaceutique. En améliorant la traçabilité des médicaments, les entreprises pharmaceutiques deviennent alors complètement transparentes pour les consommateurs, et ceux-ci peuvent alors savoir si un médicament acheté provient de leur pays, ou est importé d'un autre pays. Pour les entreprises pharmaceutiques, cela peut les empêcher de pouvoir réduire les coûts en fabriquant un médicament dans un pays où les coûts de productions sont faibles, et ainsi augmenter leur marge. Ce manque à gagner peut être une des raisons justifiant les failles actuelles de l'industrie pharmaceutique concernant la traçabilité.

La conception et le développement d'une blockchain ont permis de montrer que cette technologie est adaptée dans le cadre du suivi de lots, et plus généralement le suivi de n'importe quel objet possédant un identifiant unique, et cela avec des coûts de mise en place minimes au regard des enjeux.

5.2. Réalisation des objectifs

Dans l'introduction de ce mémoire, une série d'objectifs a été spécifiée. Ces objectifs ont pour but de démontrer que ce mémoire remplit bien son rôle. Ci-dessous sont présentés de nouveau ces objectifs, avec la démarche pour les atteindre :

- **Comprendre et connaître ce qu'est une blockchain, avec le fonctionnement de celle-ci et l'utilité future de la technologie.**

Dans la partie de l'état de l'art fut présenté ce qu'est une blockchain. Le fonctionnement de cette technologie, et son utilisation pour les chaînes d'approvisionnement fut réalisée amplement lors de ce mémoire (notamment lors de la construction de la solution). Les algorithmes spécifiques aux blockchains, principalement ceux concernant la résolution de conflits, furent aussi présentés. Globalement, l'ensemble de la composition et du fonctionnement d'une blockchain ont été présentés et analysés lors du développement de ce mémoire.

- **Analyser la chaîne d'approvisionnement de l'industrie pharmaceutique.**

Lors de l'analyse du cadre conceptuel de ce mémoire fut présentée la chaîne d'approvisionnement de Novartis, avec la spécificité propre à cette chaîne. À partir de l'analyse de cette chaîne d'approvisionnement fut ensuite créée une généralisation pour l'ensemble des chaînes de l'industrie pharmaceutique. C'est cette généralisation qui a rendu possible la création de la solution du mémoire, avec l'identification des différents acteurs de la chaîne.

- **Développer un programme permettant d'améliorer le suivi des médicaments grâce à une blockchain.**

L'objectif central de ce mémoire était de proposer une solution aux problèmes de contrefaçon de médicaments. Le programme développé à l'aide de Flask permet de répondre à cet objectif, avec l'utilisation d'une blockchain pour améliorer ce suivi.

5.3. Travaux futurs

Ce mémoire présente une base de l'amélioration de la traçabilité pour le secteur pharmaceutique. Potentiellement, l'amélioration de cette traçabilité peut être, sur le même principe de l'utilisation d'une blockchain, étendu aux autres produits médicaux, voir à des secteurs complètement éloignés (par exemple le suivi de la composition de nourriture pour la grande consommation). Avec plus de granularité, ce mémoire pourrait suivre la composition plus tôt (d'où viennent les excipients, d'où viennent les molécules...). La solution proposée actuellement suit uniquement le médicament fini.

Une autre étape pourrait être de transformer la solution en ERP (*Entreprise Ressource Planning*) complet pour les entreprises pharmaceutiques. La gestion des stocks étant déjà assurée par la solution actuelle, le programme offre une base d'ERP. Transformer la solution en ERP présenterait de nombreux avantages. Par exemple, les transporteurs (considérés comme acteurs dans la solution actuelle) pourraient gérer leur stock en flux tendu, et distribuer les médicaments qu'ils transportent au fur-et-à-mesure (sur le modèle de l'industrie automobile). Dans le cas où l'un des clients du transporteur refuse un lot, celui-ci pourrait proposer ce lot à l'ensemble des autres clients sur sa route, et ainsi optimiser le transport.

Enfin, la normalisation d'une blockchain afin d'effectuer la traçabilité des médicaments dans l'industrie pharmaceutique peut, grâce à des interfaces, permettre aux différentes entreprises du secteur d'adapter leur ERP interne afin d'accéder à cette blockchain. Cela laisserait aux administrations nationales le travail de gestion des routes des interfaces et la gestion des autorisations d'interaction avec la blockchain (définir les fabricants et les acteurs). Cette solution permettrait aux entreprises pharmaceutiques de devoir uniquement adapter leur système actuel à cette nouvelle traçabilité.

Bibliographie

- [1] (n.d.). Retrieved from http://archive.wikiwix.com/cache/?url=http://www.leem.org/htm/themes/article.asp?id_sous_rubrique=95&id_article=490
- [2] (n.d.). Retrieved from <http://rfidinhealthcare.org/>
- [3] Agnew, H. (2017, December 3). Sanofi leads charge against counterfeit drugs. Retrieved from <https://www.ft.com/content/7027df4e-d67a-11e7-8c9a-d9c0a5c8d5c9>
- [4] Armstrong, S., & ArmstrongShain, S. (2018, March 29). Gen2 V2: The Next Step In The Evolution of RFID. Retrieved from <https://blog.atlasrfidstore.com/g2v2>
- [5] (2019, August 13). Barcode. Retrieved from https://en.wikipedia.org/wiki/Barcode#Types_of_barcodes
- [6] Castro, M., & Liskov, B. (1999, February). Practical Byzantine Fault Tolerance. Retrieved from <http://pmg.csail.mit.edu/papers/osdi99.pdf>
- [7] Clark, F. (n.d.). Rise in online pharmacies sees counterfeit drugs go global ... Retrieved from [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(15\)00394-3/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(15)00394-3/fulltext)
- [8] (n.d.). COMBATING COUNTERFEIT DRUGS A Report of the Food and Drug ... Retrieved from <https://www.fda.gov/media/77086/download>
- [9] (n.d.). Composition du médicament/Généralités. Retrieved from https://fr.wikiversity.org/wiki/Composition_du_m%C3%A9dicament/G%C3%A9n%C3%A9ralit%C3%A9s
- [10] (n.d.). Détermination d'un état global - dpt-info.di.unistra.fr. Retrieved from https://dpt-info.di.unistra.fr/~stella/enseignement/algos_distr/chapitre6_12_13.pdf
- [11] (n.d.). El Mercado de Medicamentos en Chile - economia.gob.cl. Retrieved from <https://www.economia.gob.cl/wp-content/uploads/2013/04/Boletin-Mercado-de-Medicamentos.pdf>
- [12] (n.d.). EXISTING TECHNOLOGIES AND “TRACK AND TRACE” MODELS IN USE ... Retrieved from https://www.who.int/medicines/regulation/ssffc/mechanism/country-experience-table_updated-nov2017.pdf
- [13] Fox, M. (2011, June 16). Alan Haberman, Who Ushered In the Bar Code, Dies at 81. Retrieved from https://www.nytimes.com/2011/06/16/business/16haberman.html?_r=1&hp
- [14] (2014, December 5). Guide pratique: choisir un tag RFID. Retrieved from <http://www.nexess-solutions.com/fr/choisir-un-tag-rfid-pour-des-applications-industrielles/>
- [15] (2011). IMPACT International Medical Products Anti-counterfeiting ... Retrieved from <http://apps.who.int/medicinedocs/en/d/Js20967en/>
- [16] (n.d.). Implementation of RFID in the Pharmaceutical Industry. Retrieved from <https://www.iopp.org/files/public/CAPolytechJDHoward.pdf>

- [17] (2014, October 24). ISO/IEC 16022:2006. Retrieved from <https://www.iso.org/standard/44230.html>
- [18] Kenney, J. T. (2014, June 25). The Health and Economic Effects of Counterfeit Drugs. Retrieved from <http://www.ahdbonline.com/issues/2014/june-2014-vol-7-no-4/1756-the-health-and-economic-effects-of-counterfeit-drugs>
- [19] King, S., & Nadal, S. (2012, August 19). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Retrieved from <https://decred.org/research/king2012.pdf>
- [20] Lamport, L. (n.d.). Time, Clocks, and the Ordering of Events in a Distributed ... Retrieved from <https://lamport.azurewebsites.net/pubs/time-clocks.pdf>
- [21] Lamport, L. (n.d.). The Part-Time Parliament - Leslie Lamports Home Page. Retrieved from <http://lamport.azurewebsites.net/pubs/lamport-paxos.pdf>
- [22] Lamport, L. (2001, November 1). Paxos Made Simple - Leslie Lamports Home Page. Retrieved from <https://lamport.azurewebsites.net/pubs/paxos-simple.pdf>
- [23] (n.d.). Legifrance - Le service public de l'accès au droit. Retrieved from <https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000006689867>
- [24] (2019, July 5). List of largest pharmaceutical companies by revenue. Retrieved from https://en.wikipedia.org/wiki/List_of_largest_pharmaceutical_companies_by_revenue
- [25] Nakamoto, S. (n.d.). A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/en/bitcoin-paper>
- [26] Nazrul, S. S. (2018, November 5). CAP Theorem and Distributed Database Management Systems. Retrieved from <https://towardsdatascience.com/cap-theorem-and-distributed-database-management-systems-5c2be977950e>
- [27] Ongaro, D., & Ousterhout, J. (n.d.). In Search of an Understandable Consensus Algorithm ... Retrieved from <https://raft.github.io/raft.pdf>
- [28] (2019, April 26). Pénicilline. Retrieved from <https://fr.wikipedia.org/wiki/Pénicilline#Historique>
- [29] (n.d.). QR Code vs. Data Matrix vs. Linear. Retrieved from <https://nationalband.com/qr-code-vs-data-matrix-vs-barcode/>
- [30] (n.d.). Lecteur RFID : comment cela marche ? - rfid nfc iot ido rtls ble - Internet des Objets Connectés. Retrieved from <http://www.filrfid.org/article-3373163.html>
- [31] Sanofi. (n.d.). Fighting counterfeit drugs starts with knowing it exists: Sanofi. Retrieved from <https://mediaroom.sanofi.com/en/articles/2017/fighting-counterfeit-drugs-starts-with-knowing-it-exists/>
- [32] (n.d.). SANTÉ 2030 : analyse prospective pour relever les défis de la santé de demain. Retrieved from http://www.leem.org/htm/themes/article.asp?id_sous_rubrique=95&id_article=490

- [33] Smiley, S., & SmileySuzanne, S. (2018, March 27). 7 Types of Security Attacks on RFID Systems. Retrieved from <https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems>
- [34] (n.d.). Substandard and falsified medical products. Retrieved from <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- [35] (n.d.). Supply Chain Excellence in the Pharmaceutical Industry ... Retrieved from [https://ctl.mit.edu/sites/ctl.mit.edu/files/SC2020 Thesis Novartis.pdf](https://ctl.mit.edu/sites/ctl.mit.edu/files/SC2020%20Thesis%20Novartis.pdf)
- [36] Tosetti, P. (2016, February 26). Medicines verification in Europe: What to expect in 2019. Retrieved from https://ec.europa.eu/health/sites/health/files/files/falsified_medicines/201602_stakeholders_workshop_final.pdf
- [37] (2019, February 10). Trading in Venezuela's pain: Border vendors do brisk business in meds. Retrieved from <https://www.france24.com/en/20190210-trading-venezuelas-pain-border-vendors-do-brisk-business-meds>
- [38] (n.d.). What is Hashing? » Learn about Blockchain: Lisk Academy. Retrieved from <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing>
- [39] Wu, J. (2015, May 22). Where does medicine come from? Retrieved from <http://sitn.hms.harvard.edu/flash/2011/where-does-medicine-come-from/>
- [40] (n.d.). ¿Cuándo se puede comercializar un medicamento genérico? Retrieved from <https://www.engenerico.com/cuando-se-puede-comercializar-un-medicamento-generico/>

Annexes

1. Exemple de blockchain

```
{
  "chain": [
    {
      "hash": "db22ee422d9cc3aefc571e093eb37bb89a8be980045f48b35ad11bac1ef6aa9e",
      "index": 0,
      "nonce": 0,
      "previous_hash": "00",
      "timestamp": 1566750163.615837,
      "transactions": []
    },
    {
      "hash": "006c5640b00aec6c5cbfdcf55d82224563ef7f08f7765a8b01a06dd6d90d7751",
      "index": 1,
      "nonce": 976,
      "previous_hash": "db22ee422d9cc3aefc571e093eb37bb89a8be980045f48b35ad11bac1ef6aa9e",
      "timestamp": 1566750262.134371,
      "transactions": [
        {
          "batch_id": 3,
          "quantity": 10,
          "recipient_id": 2,
          "sender_id": 2,
          "status": "accepted",
          "timestamp": 1566750257.638112
        },
        {
          "batch_id": 4,
          "quantity": 20,
          "recipient_id": 2,
          "sender_id": 2,
          "status": "accepted",
          "timestamp": 1566750259.762617
        }
      ]
    }
  ],
  {
    "hash": "0052d92fac470238f3d4678e08097913e1688a3d9e8f0c8a07390a8c63b8b81f",
    "index": 2,
    "nonce": 816,
    "previous_hash": "006c5640b00aec6c5cbfdcf55d82224563ef7f08f7765a8b01a06dd6d90d7751",
    "timestamp": 1566750272.456348,
```

```

    "transactions": [
        {
            "batch_id": 3,
            "quantity": 10,
            "recipient_id": 1,
            "sender_id": 2,
            "status": "waiting",
            "timestamp": 1566750271.120368
        }
    ]
}
],
"length": 3,
"peers": [
    "http://localhost:8000/",
    "http://localhost:8001/"
]
}

```

2. Code d'un block

```

class Block:
    def __init__(self, index, transactions, timestamp, previous_hash,
nonce=0):
        self.index = index
        self.transactions = transactions
        self.timestamp = timestamp
        self.previous_hash = previous_hash
        self.nonce = nonce

```

3. Code de la blockchain

```

class Blockchain:

    #Difficulty of the proof of work
    difficulty = 2

    def __init__(self):
        self.unconfirmed_transactions = []
        self.chain = []

    def create_genesis_block(self):
        """
        Function to generate the first block and the first hash
        """
        genesis_block = Block(0, [], time.time(), "00")
        genesis_block.hash = genesis_block.compute_hash()
        self.chain.append(genesis_block)

```

```

@property
def last_block(self):
    return self.chain[-1]

def proof_of_work(self, block):
    """
    Proof of work's function that verify that the start of our hash is
a    number of zeros.
    """
    block.nonce = 0
    computed_hash = block.compute_hash()
    while computed_hash.startswith('0' * self.difficulty) is False:
        block.nonce += 1
        computed_hash = block.compute_hash()

    return computed_hash

def add_block(self, block, proof):
    """
    Function to add a block to the chain
    """
    previous_hash = self.last_block.hash

    if previous_hash != block.previous_hash:
        return False

    if not Blockchain.is_valid_proof(block, proof):
        return False

    block.hash = proof
    self.chain.append(block)
    return True

@classmethod
def is_valid_proof(cls, block, block_hash):
    """
    Check if block_hash is valid hash of block and comply
    with the difficulty
    """
    return (block_hash.startswith('0' * Blockchain.difficulty) and
            block_hash == block.compute_hash())

def add_new_transaction(self, transaction):
    self.unconfirmed_transactions.append(transaction)

@classmethod
def check_chain_validity(cls, chain):

```

```

"""
Check is the hash is correct or no
"""
result = True
previous_hash = "0"

for block in chain:
    block_hash = block.hash
    delattr(block, "hash")

    if not cls.is_valid_proof(block, block.hash) or previous_hash
!= block.previous_hash:
        result = False
        break

    block.hash, previous_hash = block_hash, block_hash

return result

def mine(self):
    """
    Function who add all the unconfirmed transactions to a block and
    getting then the proof of work
    """
    #if there is no transaction
    if not self.unconfirmed_transactions:
        return False

    last_block = self.last_block

    new_block = Block(index=last_block.index + 1,
                      transactions=self.unconfirmed_transactions,
                      timestamp=time.time(),
                      previous_hash=last_block.hash)

    proof = self.proof_of_work(new_block)
    self.add_block(new_block, proof)

    self.unconfirmed_transactions = []
    announce_new_block(new_block)
    return new_block.index

```