REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــامعة أبي بكـــر بلـقـايد – تـلمســـــــــــــان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

Mémoire de fin d'étude.

Présenté pour l'obtention du **diplôme** de **Master**

En **: Génie Industriel.**

Spécialité : **Ingénierie des Systèmes**

Par : **MEDJAHEDI ABDERRAZAK**

&

LAASSIS ISLAM

Étude simulation et exploitation de la blockchain dans la traçabilité et le suivis des produits dans une chaine logistique.

Soutenu le 06 / 07 / 2021, devant le jury:

M. MEKAMCHA KHALID	**MCB**	**Président**
M. MALIKI FOUAD	**MCB**	**Examinateur**
M. GUEZZEN AMINE HAKIM	**MCB**	**Encadrant**

Année universitaire : 2020/2021

Remerciement :

Nous nous devons remercier **ALLAH** le tout puissant pour tout la volonté et le courage qu'il nous a données pour l'achèvement de ce travail.

Un très grand merci à nos **Parents** pour tous leurs efforts depuis notre naissance jusqu'à ces moments.

Aussi nous exprimons nos vifs remerciements envers notre encadrant **M. Guezzen Amine HAKIM**, de nous avoir encadré, orienter, aider et conseiller.

Nous adressons nos sincères remerciements **M. MEKAMCHA KHALID** et **M. MALIKI FOUAD** les membres du jury pour leur présence, pour leur lecture attentive de notre thèse ainsi que pour les remarques qu'ils nous adresseront lors de cette soutenance afin d'améliorer notre travail.

On tient à témoigner notre reconnaissance à **M. DEGDEG Hichem** qui nous a bien aidés à réaliser ce mémoire.

Et très grand merci aux personnes qui nous aiment et qu’ils nous ont soutenu.

Abstract:

Blockchain is widely regarded as one of the important technology in many industries. It improves trust, transparency, traceability and security in the supply chain. Especially, it has attracted great attention in the field of supply chain. In this Thesis, it is described how blockchain can improve supply chain. Finally, it answers the question of what are the application and challenges of Blockchain technology in mobility, SCM, logistics, and shipping. Recently, large companies decided to use blockchain in the supply chain and logistics and they have had positive results. It is obvious that theoretically, the use of blockchain leads to great and positive results, but is it right about the practice ? There is no doubt that in the future, it would be easier to use and the weaknesses and threats would be minimized or eliminated.

Résumé:

La blockchain est largement considérée comme l'une des technologies importantes dans de nombreuses industries. Il améliore la confiance, la transparence, la traçabilité et la sécurité dans la chaîne logistique. En particulier, il a attiré une grande attention dans le domaine de la chaîne logistique. Dans cette thèse, il est décrit comment la blockchain peut améliorer la chaîne logistique. Enfin, il répond à la question de savoir quelles sont les applications et les défis de la technologie Blockchain dans la mobilité, le GCL, la logistique et l'expédition. Récemment, de grandes entreprises ont décidé d'utiliser la blockchain dans la chaîne logistique et elles ont eu des résultats positifs. Il est évident que théoriquement, l'utilisation de la blockchain conduit à des résultats grands et positifs, mais est-ce juste sur la pratique ? Il ne fait aucun doute qu'à l'avenir, il serait plus facile à utiliser et les faiblesses et les menaces seraient minimisées ou éliminées.

الملخص:

تعتبر سلسلة الكتل أو بلوك تشين على نطاق واسع واحدة من التقنيات المهمة في العديد من الصناعات. يحسن الثقة والشفافية وإمكانية التتبع والأمن في سلسلة التوريد. على وجه الخصوص، لقد جذبت اهتمامًا كبيرًا في مجال سلسلة التوريد. في هذه الأطروحة ، تم وصف كيف يمكن لـ بلوك تشين تحسين سلسلة التوريد. أخيرًا ، يجيب على سؤال ما هي التطبيقات والتحديات التي تواجه تقنية بلوك تشين في التنقل ، تسيير سلسة التوريد ، الخدمات اللوجستية والشحن. في الآونة الأخيرة ، قررت الشركات الكبيرة استخدام بلوك تشين في سلسلة التوريد وحققت نتائج إيجابية. من الواضح أن استخدام بلوك تشين نظريًا يؤدي إلى نتائج كبيرة وإيجابية ، ولكن هل هو عادل من الناحية العملية؟ ليس هناك شك في أنه سيكون من الأسهل استخدامه في المستقبل وسيتم تقليل نقاط الضعف والتهديدات إلى الحد الأدنى أو القضاء عليها.

Table des matières

Abstract: 2

Résumé: 2

الملخص: 2

Table des matières 3

Liste des Figures 6

Introduction générale 8

Chapitre I 11

Généralités sur la chaine logistique et la technologie Blockchain 11

I.1 Introduction : 12

I.2 La chaine logistique : 12

I.3 Les défis : 14

I.4 L'histoire de la Technologie Blockchain : 15

I.5 Réseaux des nœuds d'un système pair-à-pair 16

I.5.1 Réseau des nœuds distribué publique (blockchain publique) : 17

I.5.2 Grand livre distribué publique : 18

I.5.3 Réseaux des nœuds distribués privé (Blockchain privé) : 18

I.5.4 Grand livre distribué privé : 18

I.5.5 Réseaux des nœuds distribués permissionné (blockchain permissionné) : 18

I.6 Algorithme de consensus dans la Blockchain : 19

I.6.1 Les principaux algorithmes de consensus : 20

I.7 La Cryptographie : 23

I.7.1 Cryptographie symétrique 23

I.7.2 Cryptographie Asymétrique : 24

I.7.3 Fonctions de Hachage : 26

I.8 Contrat intelligente : 28

I.8.1 Intermédiaires, automatisation et gain de temps : 28
I.8.2 Sécurité : 28
I.8.3 Précision et transparence : 29
I.8.4 Coût : 29
I.9 Principales caractéristiques de la technologie Blockchain : 29
I.9.1 Transactions transparentes et contrôlées : 29
I.9.2 Immuable : 30
I.10 Conclusion : 30
Chapitre II Domaines d'application de la Technologie Blockchain 31
II.1 Introduction 32
II.2 Historique 32
II.3 Blockchain et industrie 4.0 32
II.3.1 Définition de l'Industrie 4.0 32
II.3.2 Application de la blockchain dans l'industrie 4.0 33
II.4 L'utilisation de la blockchain dans l'industrie 34
II.4.1 Partage des informations pour la traçabilité et la transparence 34
II.4.2 Validation des conditions de travail tout au long de la chaîne logistique 35
II.4.3 Dans la chaîne logistique alimentaire 35
II.4.4 Industrie de la logistique 36
II.4.5 Secteur financier 37
II.4.6 Industrie de l'énergie 38
II.4.7 Industrie de la robotique 39
II.4.8 Dans l'industrie de pharmaceutique : 40
II.4.9 L'utilisation de « smart contracts » 41
II.5 Conclusion : 42
Chapitre III 43

Préparation de l'environnement pour simuler la Blockchain dans une chaine logistique..... 43
III.1 Introduction:..... 44
III.2 Traitement des données Médicales :..... 44
III.3 Problèmes avec la gestion actuelle des données de santé :..... 44
III.4 Comment la Blockchain résout ces problèmes de gestion des données :..... 45
III.4.1 Problème de visibilité :..... 45
III.4.2 Problème des consentements réglementaires :..... 46
III.4.3 Problème d'expédition de la chaîne du froid :..... 46
III.5 Méthodologie proposée pour la conception :..... 46
III.6 Les outils utilisés pour la réalisation :..... 47
III.6.1 Visual Studio Code éditeur :..... 47
III.6.2 Les outils d'application web :..... 48
III.6.3 Les outils de la Blckchain :..... 55
III.7 Conclusion :..... 59
Chapitre IV..... 60
Réalisation et Simulation d'un système Blockchain pour la traçabilité des produits pharmaceutiques dans une chaine logistiques :..... 60
IV.1 Introduction :..... 61
IV.1.1 Les Diagramme UML de Système Blockchain :..... 62
IV.1.2 Création d'une plateforme DApp (Front-End) :..... 67
IV.1.3 Programmation des contrats intelligents (Back-End) :..... 70
IV.1.4 Déploiement et l'exécution de Contrat intelligente du réseau Blockchain :..... 71
IV.2 Inspection et vérification des résultats obtenue :..... 73
IV.3 Analyse des résultats obtenue :..... 76
IV.4 Conclusion :..... 77
Conclusion générale..... 78

Les Références : 79

Liste des Figures

FIGURE I-1 EXEMPLE D'UNE CHAINE LOGISTIQUE GLOBAL 14
FIGURE I-2 LES TYPES DE RESEAUX 17
FIGURE I-3 SCHEMA MONTRE LE FONCTIONNEMENT DES RESEAUX PAIR-A-PAIR 17
FIGURE I-4 ACCESSIBILITE DES DONNES DANS LES 3 RESEAUX 19
FIGURE I-5 LES MACHINES ASIC CONÇU POUR ALGORITHME POW 21
FIGURE I-6 LE CHIFFREMENT SYMETRIQUE 24
FIGURE I-7 EXEMPLE DE CRYPTOGRAPHIE ASYMETRIQUE 25
FIGURE I-8 EXEMPLE DE FONCTION DE HACHAGE 27
FIGURE I-9 LE SHA256 27
FIGURE II-1 INDUSTRIE 4.0 33
FIGURE II-2 BLOCKCHAIN DANS UNE CHAINE LOGISTIQUE ALIMENTAIRE 36
FIGURE II-3 SCHEMA D'UNE COMMUNAUTE ENERGETIQUE UTILISANT LA TECHNOLOGIE BLOCKCHAIN 38
FIGURE II-4 BLOCKCHAIN DANS LE DOMAIN MEDICAL 41
FIGURE III-1 PROBLEMES DE TRAITEMENT DES DONNEES DANS LE DOMAINE DE LA SANTE. 45
FIGURE III-2 SCHEMA SIMPLIFIER DE NOTRE IDEE 47
FIGURE III-3 INTERFACE DE VISUAL STUDIO 48
FIGURE III-4 LES CAS D'UTILISATION DE NODEJS 49
FIGURE III-5EXEMPLE WEB APP AVEC ANGULARJS 50
FIGURE III-6 LES AVANTAGES D'ANGULARJS 50
FIGURE III-7 EXEMPLE PROGRAMMATION DE JAVASCRIPT 51
FIGURE III-8EXEMPLE SIMPLE PROGRAMMATION HTML 52
FIGURE III-9 EXEMPLE PROGRAMMATION EN CSS 53
FIGURE III-10 LES TROIS LANGAGES DE DEV WEB SIMPLEMENT EXPLIQUE 53
FIGURE III-11 CONSOLE DE CHROME DEV 54
FIGURE III-12 LE FONCTIONNEMENT DE DAPP 56
FIGURE III-13 INTERFACE D'IDE REMIX 57
FIGURE III-14 SCHEMA D'ACCES VERS LA BLOCKCHAIN DEPUIS UN NAVIGATEUR WEB 58
FIGURE III-15 LE ROLE DE AWS DANS LE SYSTEME BLOCKCHAIN 59
FIGURE IV-1 DIAGRAMME DE CAS D'UTILISATION DE SYSTEME BLOCKCHAIN DE TRAÇABILITE DES PRODUITS PHARMACETIQUE 62
FIGURE IV-2 DIAGRAMME DE SEQUENCEMENT DE DAPP POUR CREER UN COMPTE D'OPERATEUR 63
FIGURE IV-3 DIAGRAMME DE SEQUENCEMENT L'OPERATEUR POUR AJOUTER UN PRODUIT DANS LE DAPP 64

FIGURE IV-4 DIAGRAMME DE SEQUENCEMENT POUR VERIFIER LA TRANSACTION DES DONNEES DANS DAPP 65
FIGURE IV-5 DIAGRAMME DE CLASSE DE SYSTEME BLOCKCHAIN 66
FIGURE IV-6 PROGRAMMATION DE LA PLATEFORME DAPP 67
FIGURE IV-7 L'ACCUEILLE (HOME) DE L'INTERFACE DAPP 68
FIGURE IV-8 PRESENTATION DE LA CHAINE LOGISTIQUE DANS LE SITE WEB DAPP 68
FIGURE IV-9 L'ACCES ADMIN RESPONSABLE DE LA DAPP POUR GERER LA PLATEFORME 69
FIGURE IV-10 L'AJOUT D'OPERATEUR POUR ACCEDER A LA PLATEFORME ET GERER LES DONNEES DES MEDICAMENTS 69
FIGURE IV-11 INTERFACE DE DAPP OU L'OPERATEUR IL DOIT INSERER LES DONNEES DES PRODUITS PHARMACEUTIQUES 70
FIGURE IV-12 PROGRAMMATION DE CONTRANT INTELLIGENTE SUR REMIX IDE 70
FIGURE IV-13 SYNTAXE DE CONTRAT INTELLIGENTE D'ACCES ADMIN 71
FIGURE IV-14 SYNTAXE DE CONTRAT INTELLIGENTE DE DECLARATION D'UN NOUVEL OPERATEUR 71
FIGURE IV-15 METAMASK CONNECT VERS LE RESEAU DE BLOCKCHAIN 72
FIGURE IV-16 DEPLOIE DE CONTRAT INTELLIGENTE DE MEDICAMENT DANS LE RESEAU BLCKCHAIN. 72
FIGURE IV-17 L'ADMINISTRATEUR PEUT ACCEDER A DES INFORMATIONS PRECISES SUE LA TRAÇABILITE DE PRODUIT PHARMACEUTIQUE 73
FIGURE IV-18 INSERER L'IDENTIFIENT DU PRODUIT POUR CHERCHER LE PRODUIT PHARMACEUTIQUE SPECIFIQUE. 73
FIGURE IV-19 L'ACCES VERS LE RESULTAT DE RECHERCHE 74
FIGURE IV-20 EXEMPLE N°1 DE RESULTAT DE RECHERCHE OBTENU 75
FIGURE IV-21 UN EXEMPLE N°2 DE RESULTAT DE RECHERCHE OBTENU 76

Introduction générale

Notre société devient de plus en plus consumériste, la plupart des habitants des pays développés ayant un pouvoir de consommation élevé et des normes de vie élevées. Les chaînes logistiques modernes ressentent la pression de cette croissance, entraînant une demande d'une gestion efficace. La plupart des entreprises font des efforts à cette fin, et, même si une partie de la réponse à une gestion efficace réside dans le processus, une bonne gestion repose également sur l'utilisation des bonnes technologies, tel que la technologie Blockchain. Ainsi, le développement des technologies est capable de satisfaire les exigences de la gestion de la chaîne d'approvisionnement, pour toute industrie.La technologie Blockchain permet de créer un système sécurisé, publics, distribués et décentralisés. Bien qu'il ait été proposé pour la première fois dans sa forme actuelle par Satoshi Nakamoto [8], un groupe anonyme qui a publié un livre blanc en 2008, ce n'était pas la première référence à une telle technologie. Le premier travail sur une Blockchaine sécurisée par cryptographie a été décrit en 1991 par Stuart Haber et W. Scott Stornetta [9], et affiné en 1992 par Bayer & Haber, en incorporant des arbres de Merkle [10]. Depuis lors, il a parcouru un long chemin, générant de multiples utilisations et applications différentes de la technologie.

Ses caractéristiques font le développement des solutions distribuées et en permanence, à l'échelle mondiale systèmes disponibles possibles, ce qui est un paradigme qui suscite l'intérêt de diverses industries.

La gestion de la chaîne logistique est un domaine en particulier dans lequel nous pensons que la blockchain pourrait apporter de grandes améliorations. La gestion de la chaîne logistique a connu une augmentation de la complexité au cours des dernières décennies, en raison de la mondialisation du marché, avec des entreprises entrelacées de bien des manières différentes, leurs relations s'étendant bien au-delà de ce qu'elles trouvé par Filiz Isik [11]. Cette augmentation de la complexité est quelque peu difficile à gérer et certaines CL s'étendent et englobent tellement d'entreprises qu'en raison de leur logiciel n'étant pas préparé pour cela, les informations ne sont pas toujours transmises depuis de bout en bout, laissant des trous d'informations entre les liens qui rejoignent chaque entreprise, conduisant ainsi à beaucoup de chaos et d'incertitude quant à l'état des éléments clés de la chaîne [12].

Comme motivation, puisque la cause possible des problèmes pourrait être l'utilisation de logiciel qui ne peut pas suivre l'évolution des exigences des chaînes logistiques modernes. Les chaînes logistiques d'aujourd'hui ont des normes élevées pour leurs exigences et même lorsque le logiciel fonctionne très bien, peut-être qu'il n'est pas assez récent ou qu'il n'a pas été spécifié et construit pour répondre à ces exigences.

Les chaînes logistiques couvrent de nombreuses zones géographiques et impliquent plusieurs phases où les données circulent dans les deux sens des fournisseurs, fabricants, distributeurs, détaillants, aux clients. Dans ces données le flux est nécessaire pour soutenir les activités critiques et des décisions qui peuvent avoir un impact sur le coût du produit et la part de marché. Les systèmes d'information centralisés actuels de la chaîne logistique ne sont pas en mesure de prendre en charge la transparence, l'évolutivité et la sécurité en temps réel nécessaires. Ce travail propose une solution de la Technologie blockchain pour le partage d'informations entre partenaires commerciaux en temps réel. Les événements de garde d'échange liés aux expéditions. Ces événements sont uniquement partagés entre partenaires commerciaux ou clients, protégeant ainsi la vie privée des participants. Le Block d’information est créé pour chaque envoi permettant à l'ensemble du réseau de prendre en charge un nombre d'expéditions via un modèle de communication hybride pair-à-pair.

Les caractéristiques des architectures blockchain semblent être une bonne solution à de nombreux problèmes identifiés dans la chaîne d'approvisionnement pour les réduire ou les neutraliser. Ces architectures sont le moyen idéal pour parvenir à la traçabilité et la transparence d'une chaîne logistique, et donc, elles sont également bonnes pour obtenir la provenance. En même temps, ils constituent un moyen sécurisé, incorruptible et immuable de stocker des informations, avec un temps de synchronisation rapide, et sont disponibles en permanence pour toute personne autorisée, n'importe où sur le réseau. Ce serait également le moyen de combler les lacunes analogiques, de transformer la chaîne entièrement numérique, conduisant à la possibilité d'une vue d'ensemble mondiale.

Notre travail se concentrera sur la gestion de la chaîne logistique et sur la manière dont les blockchains peuvent éventuellement être appliquées pour améliorer ce domaine, entraînant des impacts positifs dans l'industrie de la logistique et finissant par trouver des avantages pour le consommateur.

L'objectif principal de ce mémoire est de déterminer si la technologie blockchain est un bon moyen de résoudre les problèmes les plus courants de la gestion de la chaîne logistique

plus précisément la transparence et la traçabilité dans la chaine logistique, et également de découvrir les exigences technologiques d'une chaîne logistique moderne. Il existe une multitude de petites tâches que la blockchain pourrait automatiser dans la CL ce mémoire tentera donc de déterminer celles auxquelles la blockchain s'applique le mieux.

- Ce mémoire comporte 4 chapitres, représentés comme suivant :
- Chapitre 1 : « Généralités sur la chaine logistique et la technologie Blockchain » : Fournit les concepts et les structures nécessaires à la compréhension de la technologie Blockchain.
- Chapitre 2 : « les différente domaines application de la technologie Blockchain » : l'application de la blockchain à la chaîne logistique et dans des différentes industries est discutée plus en détail, y compris les avantages et les défis possibles.
- Chapitre 3 : « Préparation de l'environnement pour simuler la Blockchain dans une chaine logistique. » : étude de la chaine logistique des produits pharmaceutiques, et préparer l'environnement de Blockchain pour la traçabilité des produits pharmaceutiques
- Chapitre 4 : « Réalisation et Simulation d'un système Blockchain pour la traçabilité des produits pharmaceutiques dans une chaine logistiques » : simuler la blockchain dans une chaine logistique pharmaceutique depuis une application décentralisée et l'analyse de résultat dans la fin de ce chapitre
- Conclusion Générale : présente un aperçu du travail effectué dans la ce mémoire.

Chapitre I

Généralités sur la chaine logistique et la technologie Blockchain

I.1 Introduction :

Ce chapitre présente les principaux aspects techniques de la Technologie blockchain et les améliorations les plus pertinentes pour d'autres projets. Nous examinerons ensuite d'autres termes plus généraux, tels que « Technologie du grand livre distribué » (DLT) ou « crypto technologies », qui fait référence à toutes les technologies capables de transférer et / ou de stocker des données en utilisant un protocole de consensus de groupe sur les systèmes de bases de données distribuées. Les termes « Technologie du grand livre distribué » et « blockchain » sont utilisés de manière interchangeable, la terminologie évolue encore.

I.2 La chaine logistique :

Les chaînes logistiques peuvent être trouvées, sous une forme ou une autre, dans presque toutes les entreprises, couvrant de nombreux différents domaines d'opération. Traditionnellement, une chaîne d'approvisionnement englobe tous les processus et les activités qui mènent des matières premières initiales au produit fini final, ainsi que toutes les fonctions et services à l'intérieur et à l'extérieur d'une entreprise. La chaîne peut également être définie comme le réseau d'entités à travers lequel les matières circulent. Ces entités peuvent être identifiées en tant que fournisseurs, transporteurs, sites de fabrication, distribution centres, détaillants et clients [1]. Naturellement, avec l'amont et l'aval des flux de ces matériaux et ressources, vient de nombreuses informations sur eux et sur le processus, personnes et organisations auxquels ils sont associés. De manière réaliste, le flux n'est pas toujours arborescent, car il y a de nombreuses considérations à prendre et des décisions à prendre être fait. Les chaînes d'approvisionnement et les chaines logistiques ont plusieurs produits finis avec des composants, des installations et des capacités partagés [2]. En conséquence, les chemins empruntés par les ressources et les informations ne sont pas simples, mais entrelacés, divergent et convergent à différents points.

Les activités et les processus englobés par une chaîne logistique comprennent : l'approvisionnement en matières premières, matériaux et pièces, fabrication et assemblage, entreposage et suivi des stocks, saisie des commandes et gestion des commandes, distribution sur tous les canaux, livraison au client, et gérer les systèmes d'information nécessaires pour surveiller l'ensemble de ces Activités.

Comme le décrit Lummus [1], ces activités peuvent être approximativement mappées au 4 processus essentiels: planifier, approvisionner, fabriquer, livrer. La coordination de tous ces éléments n'est pas une tâche facile, c'est pourquoi la discipline de la chaîne

d'approvisionnement prend vie. Selon Ballou [3], le Conseil des professionnels de la Gestion de CL définit comme :

« *La planification et la gestion de toutes les activités liées au sourcing et à l'approvisionnement, conversion et toutes les activités de gestion logistique. Surtout, cela inclut également la coordination et collaboration avec les partenaires de distribution, qui peuvent être des fournisseurs, des intermédiaires, des tiers fournisseurs de services et clients. En substance, Gestion de CL intègre la gestion de l'offre et de la demande au sein et entre les entreprises* ».

On constate de cette définition que Gestion de CL traite beaucoup à la fois de la coordination et de la collaboration entre les entités, et donc, la gestion du flux d'informations et de ressources entre elles est très importante. L'objectif est toujours, bien entendu, de minimiser le coût total de ces flux entre et parmi les étapes [4]. Et c'est là que la Gestion de CL brille et montre à quel point elle peut être utile. Il est difficile de gérer tous les processus d'une CL, tout en maintenant la sécurité, la qualité et le respect du calendrier. Un événement d'un côté du monde, grand ou petit, que ce soit causes humaines ou naturelles, peuvent facilement perturber les maillons de la CL. Par exemple, cela pourrait perturber la fourniture d'un composant ou d'un service critique. Les retards sont donc courants et les conséquences de telles perturbations pourraient avoir un impact grave sur les finances, la croissance et la réputation des entreprises concernées. [5]. Le problème avec les normes non existantes est que les entreprises doivent discuter des détails à partager ou non, ce qui fait perdre du temps et des ressources.

Figure I-1 Exemple d'une Chaine logistique global

La gestion de la CL diminue l'impact de ces perturbations et s'efforce activement de les éviter ou de les réduire, tout en optimisant le fonctionnement de la chaîne d'approvisionnement. C'est pourquoi la gestion de CL est une discipline si importante, que nous devons mieux comprendre et améliorer, avec tous les moyens possibles, et cela inclut, bien sûr, la recherche sur des technologies nouvelle comme la **blockchain**.

I.3 Les défis :

Ayant déjà introduit les concepts de la chaine d'approvisionnement et Chaine logistique et la Gestion de CL, il est désormais possible pour présenter brièvement certains des problèmes qui les affectent.

- Le premier problème, et le plus généraliste d'une chaîne logistique, est la facilité avec laquelle **un événement inattendu peut entraîner des retards**, Ces événements ne sont pas toujours prévisibles et doivent être contenus le plus rapidement possible. Un événement en particulier qui, souvent, entraîne des retards est **les problèmes de synchronisation dans les processus et systèmes d'information d'une entreprise** [6].
- Un autre problème est que, souvent il y a des difficultés à partager des informations entre les entreprises. **Cela est dû à la fois au fait que les entreprises apprécient leur confidentialité et la sécurité de leurs informations**, ce qui signifie qu'ils ne voudront

peut-être pas partager trop d'informations, ou qu'ils pourraient uniquement les partager via des canaux sécurisés, et par le manque de normes pour l'envoi d'informations et la communication [7]

- Plus important encore, dans l'industrie, l'utilisation d'outils et de travaux manuels traditionnels est encore trop répandue. Les e-mails sont envoyés, les documents sont imprimés et envoyés par la poste, au lieu de transmettre les informations de manière plus automatique, directe et sécurisée via le réseau. Ce point met également en lumière le prochain problème des chaînes logistiques : le manque apparent d'interopérabilité entre certains logiciels (qui pourrait être un sous-produit du manque de normes).
- Enfin, la provenance et la traçabilité des produits sur une CL sont un objectif majeur pour les entreprises. Mais les technologies actuelles utilisées dans la CL n'accomplissent la provenance et la traçabilité que dans une portée limitée, car l'information a certaines entités possède est généralement également limité. Et donc, il est très difficile pour quiconque d'avoir une vue d'ensemble de la CL. Bien que cela ne soit pas prouvé, il est possible que certains, sinon la plupart, de ces problèmes dans la CL soient causés par l'utilisation des logiciels qui ne permettent pas intégration complète des données. Une CL optimale doit être aussi efficace et efficiente que possible, tout en étant sécurisée et en satisfaisant toutes les exigences de traçabilité. Peut-être, il est temps d'essayer de nouvelles solutions qui remplacent ou augmentent les solutions existantes, de manière à ce que la gestion de la CL puisse mieux répondre aux exigences requises.

I.4 L'histoire de la Technologie Blockchain :

L'un des documents les plus importants du 21e siècle commence pour de bon :

« *Une version purement pair-a-pair de la monnaie électronique permettrait d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière*. » Satoshi Nakamoto [8]

Il y a plus de dix ans, une ou plusieurs personnes opérant sous le surnom de « **Satoshi Nakamoto** » ont introduit Bitcoin et officialisé le concept de blockchain dans le monde. **Satoshi** est une figure embourbée dans le mystère. Leur identité a été spéculée à l'infini. Leur innovation n'était rien de moins que du génie. Et pourtant, l'idée sous-jacente qui a conduit leur invention était plutôt simple : nous n'avons pas besoin de banques.

La série d'articles qui suivent décomposera ce qu'est la blockchain en : racontant sa brève histoire (Bitcoin), expliquant son évolution vers une technologie de deuxième génération (Ethereum).

La blockchain est un paradigme applicable à presque tous les domaines de la vie auxquels vous pouvez penser : la finance, la médecine, le gouvernement, la vente au détail, le divertissement, etc. Mais pour cela - la première partie d'une série de trois articles sur le sujet - nous nous en tiendrons au sujet original que Satoshi Nakamoto a mis en avant : les banques. L'affirmation de Satoshi était que vous pouviez construire un réseau informatique capable de remplacer la fonction des banques. Mais comment ferait-on cela ?

I.5 Réseaux des nœuds d'un système pair-à-pair

Estiment que l'ingéniosité clé de la blockchain, comme mentionné dans le livre blanc de Nakamoto, est l'utilisation du réseau de nœuds pair-à-pair. Le réseau reçoit puis ajoute des transactions dans une chaîne de blocs de données appelée grand livre **distribué**. Au lieu d'utiliser des entités tierces de confiance, la blockchain utilise un réseau de nœuds distribué pour enregistrer les transactions, évitant ainsi les transactions à double dépense. En diffusant des transactions vers un réseau de nœuds indépendants, ils deviennent difficiles à falsifier d'un point de vue informatique sans retombées dans des pénalités sévères de la part des autres participants du réseau. Dans la blockchain publique, le nombre de nœuds peut s'élever à des milliers, car tout le monde peut rejoindre et quitter le réseau. Chaque nœud participant au sein du réseau construit et maintient sa propre version indépendante de la blockchain sur la base d'un ensemble commun de règles ; il n'est pas nécessaire que les nœuds se connaissent ou se fassent confiance. Dans la blockchain privée, le nombre de nœuds est petit car seuls les participants préapprouvés peuvent rejoindre le réseau.

Le réseau, pour qu'il soit immuable, nécessite des protocoles que les nœuds et les parties prenantes respectent. Les règles sont simples, mais un ensemble de règles régissant la diffusion, la validation et l'ajout de transactions aux blocs. Les protocoles sont ajoutés et modifiés par de nombreuses variables prédéterminées telles que le nombre de nœuds, le nombre de participants et la puissance de calcul (le Hachage).

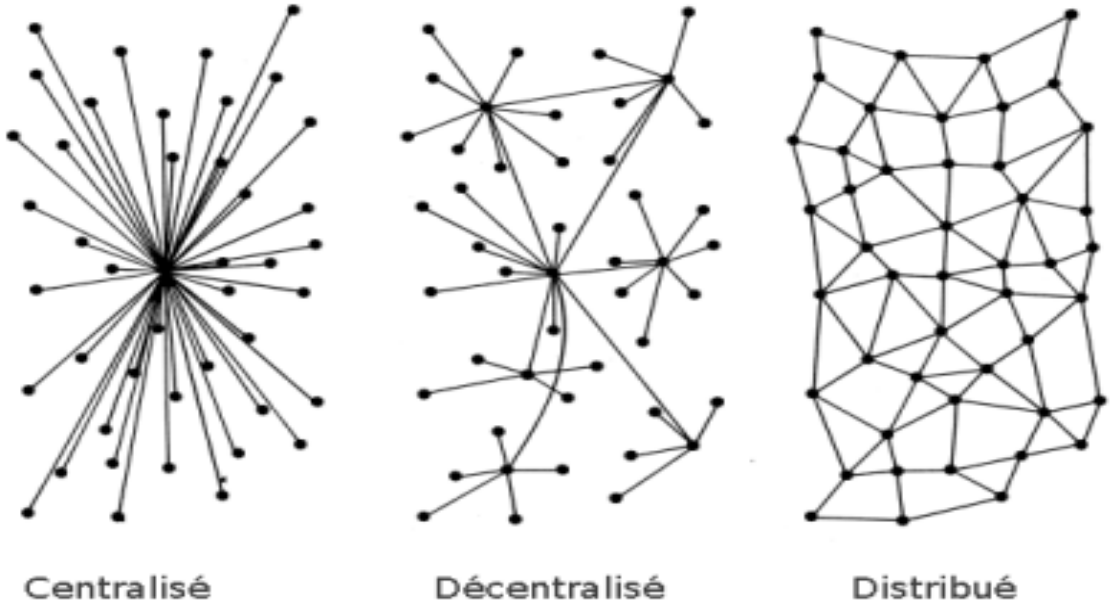


Figure I-2 les types de réseaux

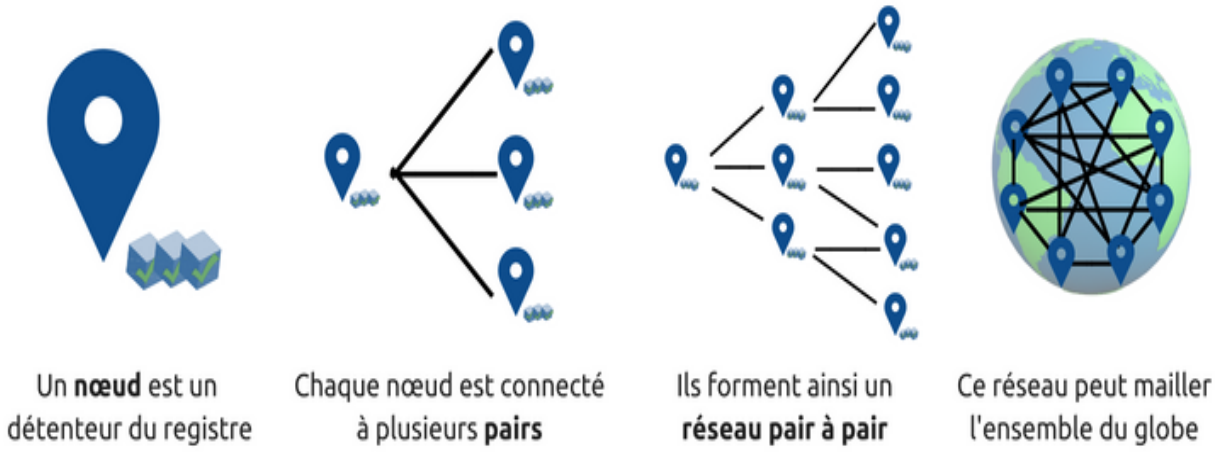


Figure I-3 schéma montre le fonctionnement des réseaux pair-à-pair

I.5.1 Réseau des nœuds distribué publique (blockchain publique) :

La blockchain publique est sans autorisation. Tout le monde peut rejoindre le réseau et lire, écrire ou participer à la blockchain. Une blockchain publique est décentralisée et n'a pas une seule entité qui contrôle le réseau. Les données dans le réseau public sont sécurisées car il n'est pas possible de modifier les données une fois qu'elles ont été validées sur la blockchain.

I.5.2 Grand livre distribué publique :

Il existe un registre public automatique. Le grand livre public s'organise en une longue chaîne de blocs d'informations. Lorsqu'un acheteur et un vendeur s'engagent dans une transaction, la blockchain vérifie l'authenticité de leurs comptes. Cela se fait en utilisant le grand livre public et en vérifiant si les fonds sont disponibles procède aux transactions. Toutefois, si les fonds ne sont pas disponibles sur le compte de l'acheteur ou sont promis à une autre partie, la vente est alors empêchée, ce qui rend le double achat impossible.

I.5.3 Réseaux des nœuds distribués privé (Blockchain privé) :

Une blockchain privée est une blockchain autorisée. Les blockchains privées fonctionnent sur la base de contrôles d'accès qui restreignent les personnes qui peuvent participer au réseau. Il existe une ou plusieurs entités qui contrôlent le réseau, ce qui conduit à compter sur des tiers pour effectuer des transactions. Dans une blockchain privée, seules les entités participant à une transaction en auront connaissance, tandis que les autres ne pourront pas y accéder.

I.5.4 Grand livre distribué privé :

Le grand livre distribué privé qui fonctionne comme une base de données fermée et sécurisée basée sur des concepts de cryptographie. Techniquement parlant, tout le monde ne peut pas exécuter un nœud complet sur la blockchain privée, effectuer des transactions ou valider / authentifier les modifications de la blockchain.

I.5.5 Réseaux des nœuds distribués permissionné (blockchain permissionné) :

La troisième catégorie est celle des réseaux autorisés. Les blockchains autorisées permettent un mélange entre les blockchains publiques et privées et prennent en charge de nombreuses options de personnalisation. Il s'agit notamment de permettre à quiconque de rejoindre le réseau autorisé après une vérification appropriée de son identité et d'attribuer des autorisations sélectionnées et désignées pour effectuer uniquement certaines activités sur le réseau.

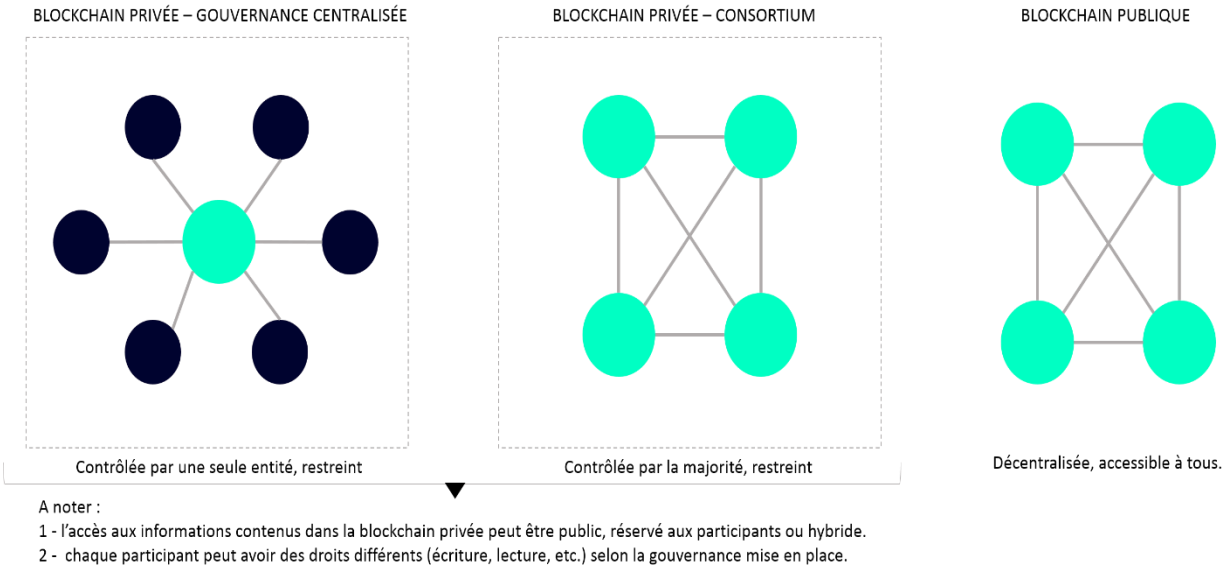


Figure I-4 accessibilité des donnés dans les 3 réseaux

I.6 Algorithme de consensus dans la Blockchain :

Un algorithme de consensus est un mécanisme qui permet aux utilisateurs ou aux machines de se coordonner dans un environnement distribué. Il doit garantir que tous les agents du système peuvent s'entendre sur une seule source de vérité, même si certains agents échouent. En d'autres termes, le système doit être tolérant aux pannes.

Dans une configuration centralisée, une seule entité a le pouvoir sur le système. Dans la plupart des cas, ils peuvent apporter des modifications à leur guise - il n'existe pas de système de gouvernance complexe pour parvenir à un consensus entre de nombreux administrateurs.

Mais dans une configuration décentralisée, c'est une tout autre histoire. Supposons que nous travaillons avec une base de données distribuée - comment parvenir à un accord sur les entrées à ajouter ?

Surmonter ce défi dans un environnement où les étrangers ne se font pas confiance était peut-être le développement le plus crucial qui a ouvert la voie aux blockchains.

Pourquoi prendraient-ils la peine de risquer leurs propres ressources ? Eh bien, il y a aussi une récompense disponible. Il s'agit généralement de la crypto-monnaie native du protocole et des frais payés par d'autres utilisateurs, d'unités de crypto-monnaie fraîchement générées, ou des deux.

La dernière chose dont nous avons besoin est la transparence. Nous devons être capables de détecter quand quelqu'un triche. Idéalement, il devrait être coûteux pour eux de produire des blocs, mais bon marché pour quiconque de les valider. Cela garantit que les validateurs sont tenus en échec par les utilisateurs réguliers.

I.6.1 Les principaux algorithmes de consensus :

Ils existent plusieurs types d'algorithmes de consensus mais on quelques-uns comme :

I.6.1.1 Preuve de travail (proof of work) Pow :

La Proof of Work (ou preuve de travail en français) est le plus ancien des protocoles de consensus blockchain. Sa première application moderne en 1996 ne concerne cependant pas Bitcoin, qui n'apparaît que bien plus tard, mais un anti-spam utilisé pour les boîtes mails. Cette preuve de travail utilise déjà l'algorithme SHA 256, à l'instar du protocole Bitcoin plus d'une décennie après. Aujourd'hui, la Proof of Work est connue comme le principal mécanisme de consensus des blockchains, en particulier celles de première génération. Son fonctionnement, bien que très sécurisé, n'est pas sans poser certains problèmes de gouvernance et de consommation énergétique.

Une blockchain utilisant la Proof of Work fait appel à des mineurs pour vérifier les données entrantes sur le registre, valider l'authenticité des transactions et créer de nouveaux blocs. Pour récompenser l'ensemble des mineurs pour leur travail, la preuve de travail doit établir des règles permettant de choisir le mineur qui aura le droit d'émettre le prochain bloc de la chaîne.

Les règles du consensus de Proof of Work permet donc de désigner un mineur auquel on accorde un droit d'écriture pour prolonger la chaîne de blocs. Elle doit, bien entendu, dissuader les éventuels utilisateurs malveillants pour protéger l'intégrité de la chaîne.

Concrètement, la preuve de travail consiste à demander aux mineurs de résoudre un problème mathématique complexe nécessitant une puissance de calcul informatique importante. Le premier à pouvoir résoudre ce problème sera également le prochain à créer un bloc sur la blockchain. Le mineur applique donc un algorithme de hachage à un même groupe de données jusqu'à trouver le résultat cherché.

Figure I-5 les machines ASIC conçu pour Algorithme Pow

- ASIC : « Application Specific Integrated Circuit » est une puce électronique, entièrement dédiée au calcul d'algorithmes complexes dans le cadre du processus de minage d'une cryptomonnaie. À l'origine, les mineurs effectuaient ce travail par l'intermédiaire du seul processeur de leur ordinateur.

I.6.1.2 Preuve d'enjeu (proof-of-stake) Pos :

Alors que dans le cadre de la preuve de travail, le mineur doit faire des investissements lourds dans du matériel de minage pour pouvoir avoir une puissance de calcul permettant de résoudre un problème mathématique complexe, le protocole "Proof of Stake" (PoS) nécessite un investissement tout à fait différent.

Pour participer aux opérations de validation et de sécurisation du réseau d'une blockchain PoS, il faut avoir accumulé une quantité minimale et suffisante de jetons de la crypto-monnaie échangée sur le réseau. Le nombre de jetons nécessaires varie d'un réseau à l'autre. Plus une personne ou une entité disposera de jetons d'une crypto-monnaie, plus on considérera que la sécurité du réseau est un enjeu important pour elle. On parle alors de « preuve d'enjeu », ou « Proof of Stake ».

Dans les blockchains qui utilisent le consensus PoS, les validateurs sont appelés forgeurs. Ici, le forgeur devra démontrer qu'il possède une certaine quantité de crypto-monnaies avant de pouvoir valider de nouveaux blocs et toucher la récompense. Dans ce cas, nul besoin de matériel de pointe énergivore ! L'intervention sur la blockchain par le forgeur suppose qu'il mette en dépôt une certaine quantité de crypto-monnaies. C'est ensuite un algorithme qui désignera, au hasard parmi les forgeurs éligibles, celui qui pourra valider le dernier bloc sur la blockchain.

En résumé, il s'agit un peu d'un « tirage au sort » parmi des candidats qui détiennent une certaine quantité d'actifs et qui les mettent en dépôt afin d'avoir le droit de participer aux opérations de validation des transactions. Si le premier candidat sélectionné ne crée pas le bloc dans l'intervalle de temps qui lui est proposé, l'algorithme sélectionnera automatiquement un deuxième candidat validateur à la place du premier. Dans l'environnement PoS, la chaîne la plus longue est celle qui est considérée par défaut comme valide.

I.6.1.3 Tolérance aux fautes byzantines (BFT)

L'objectif du consensus est de permettre que tout se passe de la bonne façon, sans pannes (bugs, erreurs, actes malveillants…)

On peut alors se poser les questions suivantes :

- Qu'est qu'il se passe si un intervenant choisit de ne pas respecter les règles et d'altérer l'état de la blockchain ?
- Que se passe-t-il si ces entités frauduleuses sont nombreuses dans le réseau ?

C'est en se posant ces questions que nous parvenons à comprendre pourquoi il est vraiment important qu'un protocole de consensus puisse être tolérant à de multiples types de pannes, comme les pannes Byzantines.

Dans ce problème, plus de deux généraux doivent s'accorder sur le moment où il faut attaquer un ennemi. En sachant qu'un ou plusieurs d'entre eux peuvent alors être un (des) traître(s).

Cela veut dire que s'ils comptent garder leur choix initial, notamment sur des critères tels que la date et l'heure de l'attaque, alors il faudra trouver une solution.

Le paradigme qui est mis en évidence dans ce célèbre problème est la mise en place d'une configuration commandant et lieutenant, permettant de parvenir à un consensus, solution la plus adéquate pour tous.

De cette façon, la solution la plus adéquate a été trouvée. Le commandant doit parvenir à un accord avec tous les lieutenants pour appliquer la même décision.

En quelques mots, la tolérance aux pannes byzantines (BFT) caractérise un système capable de résister à la l'éventail de pannes dérivées du Problème des généraux byzantins. Cela signifie qu'un système BFT est capable de continuer à fonctionner même si certains des nœuds échouent ou agissent de manière malveillante.

Il existe plus d'une solution possible au problème des généraux byzantins et, par conséquent, de multiples façons de construire un système BFT. De même, il existe différentes approches permettant à une blockchain d'atteindre la tolérance de panne byzantine, ce qui nous conduit aux algorithmes de consensus.

I.7 La Cryptographie :

La cryptographie est une méthode de développement de techniques et de protocoles pour empêcher un tiers d'accéder et d'acquérir des informations sur les données des messages privés au cours d'un processus de communication. La cryptographie est également composée de deux termes grecs anciens, Kryptos et Graphein, le premier terme signifiant « caché » et le second étant « écrire ». Il existe plusieurs termes liés à la cryptographie, qui sont énoncés comme suit :

- Cryptage : Il s'agit d'un processus de texte brut (texte normal) vers un texte chiffré (séquence aléatoire de bits).
- Décryptage : processus inverse de cryptage, conversion du texte chiffré en texte brut.
- Chiffrer : La fonction mathématique, c'est-à-dire un algorithme cryptographique qui est utilisé pour convertir du texte brut en texte chiffré.
- Clé : Une petite quantité d'informations qui est nécessaire pour induire la sortie de l'algorithme cryptographique.

Pour comprendre la cryptographie dans la blockchain, il faut comprendre les types de cryptographie. Il existe principalement trois façons différentes d'exécuter des algorithmes cryptographiques, à savoir la cryptographie symétrique, la cryptographie asymétrique et les fonctions de hachage.

I.7.1 Cryptographie symétrique

Dans cette méthode de cryptage, il y a une seule clé dans l'application. Cette clé commune est utilisée à la fois pour le cryptage et le processus de décryptage. L'utilisation d'une clé unique

commune crée un problème de transfert sécurisé de la clé entre l'expéditeur et le destinataire. Il est également appelé cryptographie à clé secrète.

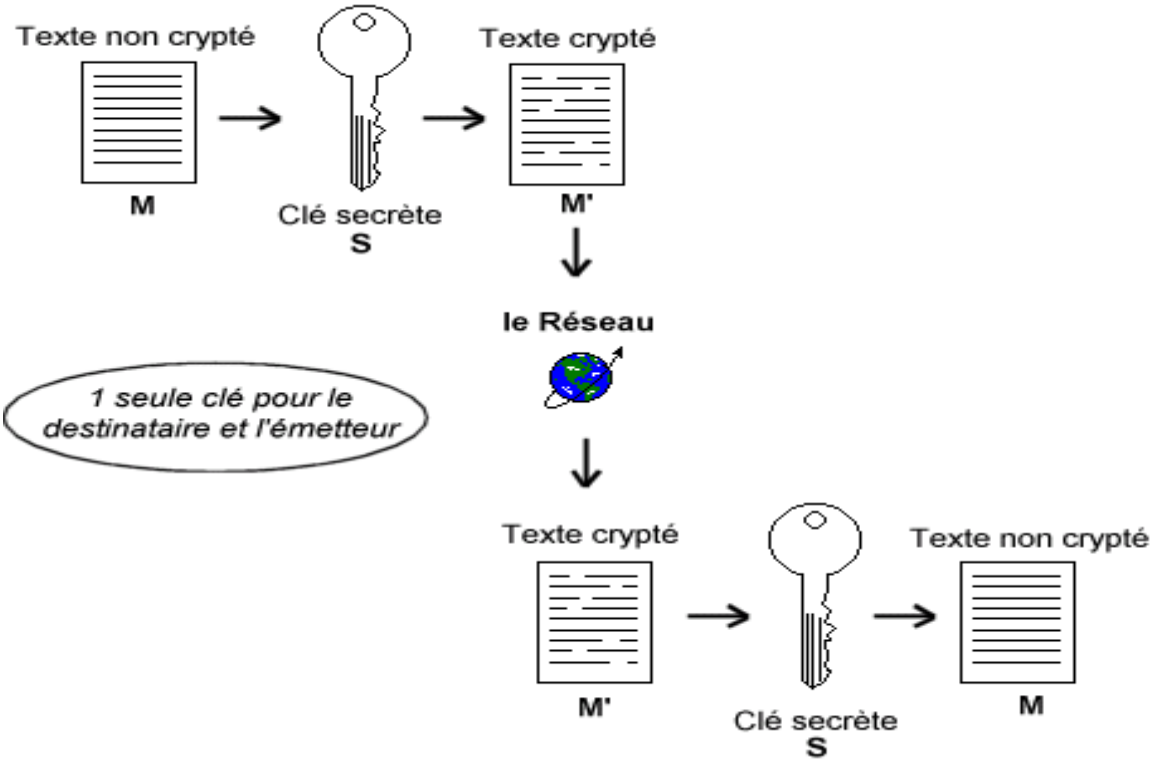


Figure I-6 le chiffrement symétrique

I.7.2 Cryptographie Asymétrique :

Cette méthode de chiffrement utilise une paire de clés, une clé de chiffrement et une clé de déchiffrement, nommées respectivement **clé publique** et **clé privée**. La paire de clés générée par cet algorithme se compose d'une clé privée et d'une clé publique unique qui est générée à l'aide du même algorithme. Il est également appelé cryptographie à clé publique.

La cryptographie à clé publique est le plus souvent utilisée pour crypter des messages entre deux personnes ou deux ordinateurs de manière sécurisée. N'importe qui peut utiliser la clé publique de quelqu'un pour chiffrer un message, mais une fois chiffré, le seul moyen de déchiffrer ce message consiste à utiliser la clé privée correspondante.

La cryptographie asymétrique est un élément fondamental de la technologie blockchain - c'est la technologie sous-jacente pour les portefeuilles et les transactions. Lorsqu'un utilisateur crée un portefeuille sur une blockchain, il génère une paire de clés publique-privée.

L'adresse de ce portefeuille, ou la façon dont il est représenté sur la blockchain, est une chaîne de chiffres et de lettres générée à partir de la clé publique. En raison de la nature de la technologie blockchain, cette adresse est publique pour tout le monde et peut être utilisée pour vérifier le solde de ce portefeuille ou lui envoyer des pièces.

La clé privée associée à un portefeuille est de savoir comment prouver la propriété et contrôler le portefeuille. C'est le seul moyen d'en envoyer des pièces, et une clé privée perdue signifie que les pièces à l'intérieur seront bloquées là pour toujours.

Une transaction sur la blockchain n'est rien de plus qu'un message diffusé qui dit essentiellement : « Prends X pièces de mon portefeuille et crédite X pièces dans un autre portefeuille ». Une fois confirmée, la transaction est immuablement inscrite dans le grand livre et les soldes sont mis à jour.

Cependant, ce message de transaction nécessite une signature de la clé privée du portefeuille d'envoi pour être valide. Après la diffusion, n'importe qui peut utiliser la clé publique de ce portefeuille pour s'assurer que la signature numérique provenant de la clé privée est authentique. C'est l'un des rôles des validateurs de bloc avant d'ajouter une transaction (c'est-à-dire un message) à la blockchain.

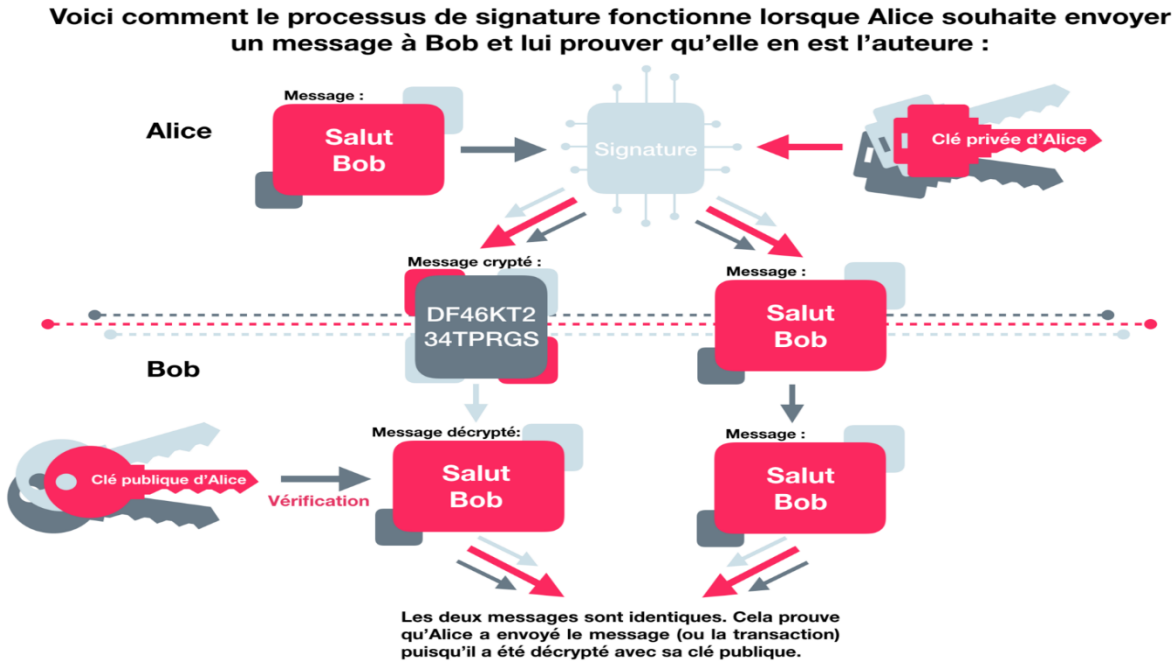


Figure I-7 Exemple de cryptographie asymétrique

I.7.3 Fonctions de Hachage :

Le hachage cryptographique génère une chaîne de caractères de longueur fixe à partir d'un ensemble de données de n'importe quel volume. Cet ensemble de données peut être un mot, une phrase, un texte plus long ou un fichier entier.

- Le hachage cryptographique peut être utilisé à des fins de sécurité, il est le pilier fondateur de la crypto sécurité.
- Le hachage transforme un input de données aléatoire (clés) en une chaîne d'octets de longueur et de structure fixes (valeur de hachage).
- Le hash d'une transaction facilite l'identification de cette dernière sur la blockchain.

Le hachage est une procédure mathématique facile à exécuter mais incroyablement difficile à inverser. La différence entre le hachage et le chiffrement est que le chiffrement peut être inversé ou déchiffré à l'aide d'une clé spécifique. Les fonctions de hachage les plus utilisées sont MD5, SHA1 et SHA-256. Certains processus de hachage sont considérablement plus difficiles à déchiffrer que d'autres.

Les fonctions de hachage cryptographiques sont des fonctions de hachage qui ont ces propriétés cruciales :

- Déterministe : peu importe le nombre de fois que vous donnez à la fonction une entrée spécifique, elle aura toujours la même sortie.
- Irréversible : Il est impossible de déterminer une entrée à partir de la sortie de la fonction.
- Résistance aux collisions : deux entrées ne peuvent jamais avoir la même sortie.

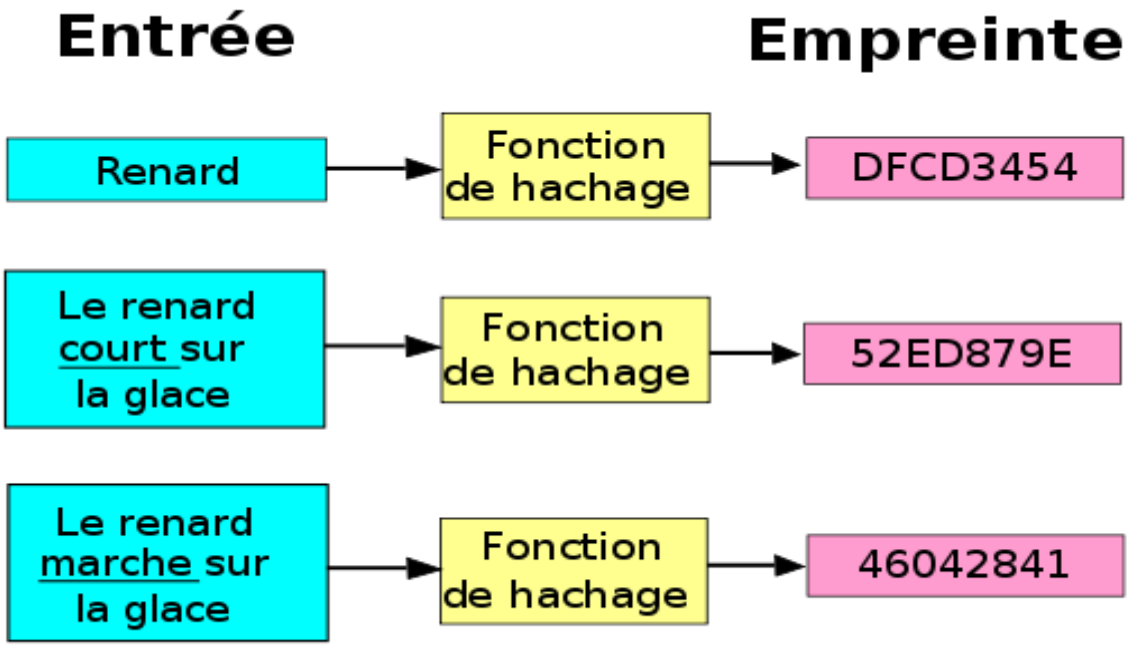


Figure I-8 Exemple de fonction de hachage

SHA256 autrement dit Secure Hash Algorithm c'est le cerveau de la blockchain, est un algorithme représentant une famille de fonctions de hachage mises en place par la National Security Agency des États-Unis. Il faut savoir qu'à l'origine Sha-2 a été créé en se basant sur Sha-0 ainsi que sur Sha-1, il représente donc la suite logique de ces algorithmes.

Quand on parle de SHA256 il s'agit en fait d'une signature pour les fichiers de données. Par exemple pour SHA256, il est ainsi possible de générer une signature de 32 octets (soit 256 bits).

Figure I-9 Le SHA256

I.8 Contrat intelligente :

Les contrats intelligents sont des contrats auto-exécutables contenant les termes et conditions d'un accord entre pairs. Les termes et conditions de l'accord sont écrits dans le code. Le contrat intelligent s'exécute sur la plate-forme décentralisée de la blockchain Ethereum. Les accords facilitent l'échange d'argent, d'actions, de biens ou de tout actif. Il existe deux langages de programmation largement utilisés pour écrire des contrats intelligents Ethereum - Solidity et Serpent. Solidity est un langage de programmation de haut niveau utilisé pour mettre en œuvre des contrats intelligents sur la plate-forme blockchain Ethereum. Il permet aux développeurs de blockchain de vérifier le programme au moment de l'exécution plutôt qu'au moment de la compilation.

Traditionnellement, lorsque deux parties concluent un contrat, elles utilisent les services d'un tiers de confiance pour exécuter l'accord. Cela se fait de cette façon depuis des siècles. Cependant, l'introduction des contrats intelligents et des technologies associées automatise ce qui a été un processus manuel laborieux. Dans cet article, nous explorerons la technologie derrière les contrats intelligents et comment ils peuvent être utilisés. Tout d'abord, comprenons certains des principaux avantages des contrats intelligents par rapport aux contrats traditionnels :

I.8.1 Intermédiaires, automatisation et gain de temps :

Le grand nombre d'intermédiaires et de couches intermédiaires impliqués dans l'exécution d'un contrat traditionnel ralentit le processus, prenant souvent des jours, voire des semaines.

Les contrats intelligents peuvent prendre quelques minutes, car ils sont automatisés et programmables, s'exécutant sur un ordinateur dans des conditions prédéfinies. Aucun tiers n'est impliqué.

I.8.2 Sécurité :

La confidentialité et la sécurité sont des préoccupations liées aux contrats traditionnels. Avec autant de parties intermédiaires impliquées, la sécurité peut être compromise à n'importe quelle étape du processus. La sécurité est assurée par la cryptographie, la clé publique et les clés privées lors de l'utilisation de contrats intelligents. Maintenues dans un système décentralisé, les données sont presque impossibles à modifier. Les contrats intelligents sont signés numériquement à l'aide de clés privées et ne peuvent être décodés que par la clé publique partagée par les parties concernées.

I.8.3 Précision et transparence :

Les termes et conditions sont prédéfinis et pré-intégrés dans un contrat intelligent. Dès qu'une condition est remplie, la remise se fait automatiquement et est enregistrée. Si un versement est impliqué dans un contrat traditionnel, il s'agit d'un processus manuel impliquant des flux de travail d'approbation. Traditionnellement, la transparence est dictée par les parties impliquées, les entités périphériques et les intermédiaires. C'est un système imparfait. Les contrats intelligents, cependant, sont 100% transparents, disponibles en ligne 24 * 7 * 365. Tout le monde peut examiner, auditer et valider les transactions archivées. L'archivage est difficile avec les contrats traditionnels, car ils sont sur papier et maintenus hors ligne. Le traçage des transactions est fastidieux. Les transactions dans les contrats intelligents peuvent être tracées dès le point d'origine, et l'archivage se produit automatiquement, créant un historique entièrement accessible.

I.8.4 Coût :

Les contrats traditionnels sont chers par rapport aux contrats intelligents simplement parce que tous ces intermédiaires doivent être payés. Les contrats intelligents n'ont pas d'intermédiaires et les seuls frais de transaction proviennent de l'infrastructure sous-jacente du réseau blockchain exécutant le contrat intelligent.

I.9 Principales caractéristiques de la technologie Blockchain :

Ce qu’on constater que la technologie Blockchain n'est pas seulement un réseau de transfert pour les crypto-monnaies, mais elle offre beaucoup plus comme le transfert et le transfert de données et des informations entre les nœuds de réseau décentralisé. Alors, quelles sont les fonctionnalités clés de la blockchain qui la rendent si irrésistible et capable d’offrir plus de service ?

I.9.1 Transactions transparentes et contrôlées :

La blockchain n'a pas d'intermédiaire (par exemple, une banque, un serveur). Il en résulte des règlements plus rapides et plus transparents, car le grand livre distribué est mis à jour automatiquement. Les conditions de paiement ou de transfert de données peuvent être préprogrammées automatiquement, y compris la visibilité d'une transaction, afin qu'elle ne puisse être visible que par les participants autorisés.

I.9.2 Immuable :

Toutes les transactions sont immédiatement visibles pour les parties autorisées, ce qui signifie que personne ne peut falsifier, supprimer ou dissimuler les informations ajoutées à la blockchain. Les données stockées dans la blockchain sont immuables et ne peuvent pas être modifiées.

I.10 Conclusion :

La technologie blockchain augmente et s'améliore jour après jour et elle a un très bel avenir dans les années à venir. Les caractéristiques de transparence, de confiance et de preuve de tempérament ont conduit à de nombreuses applications comme Bitcoin, Ethereum, etc. C'est un pilier pour rendre les procédures commerciales et gouvernementales plus sûres, et la traçabilité plus efficientes et efficaces.

Chapitre II

Domaines d’application de la Technologie Blockchain

II.1 Introduction

Nous arrivons ainsi à la définition de la blockchain qui constitue une base de données distribuée sur un réseau de « blocs » et non plus contenue dans un seul épicentre. Ce réseau est souvent assimilé à un grand livre de compte dans lequel on enregistre toutes les données ou transactions échangées/passées au sein d’une entreprise et avec son environnement externe

L’intérêt de ce système, est la sécurité qu’il fournit, car cette base de données est accessible par tous les utilisateurs de cette chaîne de blocs. On la qualifie d’infalsifiable puisque toute information inscrite dans la base est ineffaçable et traçable. Chaque utilisateur peut donc se rendre compte d’un éventuel changement s’il y a une intrusion dans la chaîne (ce qui reste très peu probable). [13]

Aujourd’hui la blockchain utilisée surtout pour les échanges de monnaie virtuelle mais peux trouver des applications possibles qui pourraient être fructueuses pour le secteur de l’industrie.

II.2 Historique

Ces dernières années ont vu une explosion de l'utilisation commerciale de la blockchain. La technologie à un grand potentiel pour stimuler la simplicité et l'efficacité des services financiers, et elle est en passe de stimuler la prochaine vague d'innovation dans les services financiers. L'intérêt pour l'exploitation de la blockchain dans d'autres secteurs, tels que la fabrication et la santé, augmente et les déploiements prennent de l'ampleur. Pourtant, le taux d'adoption est lent et les organisations ne font que commencer à gratter la surface en ce qui concerne les applications potentielles de cette technologie. Mis en œuvre correctement, les avantages commerciaux peuvent être substantiels. [19]

II.3 Blockchain et industrie 4.0

II.3.1 Définition de l'Industrie 4.0

La quatrième révolution industrielle (ou Industrie 4.0) est l'automatisation continue des pratiques de fabrication et industrielles traditionnelles, à l'aide d'une technologie intelligente moderne. La communication de machine à machine à grande échelle (M2M) et l'Internet des objets (IoT) sont intégrés pour une automatisation accrue, une communication et une auto-surveillance améliorées, ainsi que la production de machines intelligentes capables d'analyser et de diagnostiquer les problèmes sans intervention humaine. [16]

L'industrie 4.0 fait référence à une nouvelle phase de la révolution industrielle qui se concentre fortement sur l'inter connectivité, l'automatisation, l'apprentissage automatique et les données en temps réel. L'industrie 4.0, également parfois appelée **IoT** ou fabrication intelligente, associe la production physique et les opérations à la technologie numérique intelligente, à l'apprentissage automatique et au Big Data pour créer un écosystème plus holistique et mieux connecté pour les entreprises qui se concentrent sur la fabrication et la gestion de la chaîne d'approvisionnement. Bien que chaque entreprise et organisation opérant aujourd'hui soit différente, elles sont toutes confrontées à un défi commun : le besoin de connectivité et l'accès à des informations en temps réel sur les processus, les partenaires, les produits et les personnes. [17]

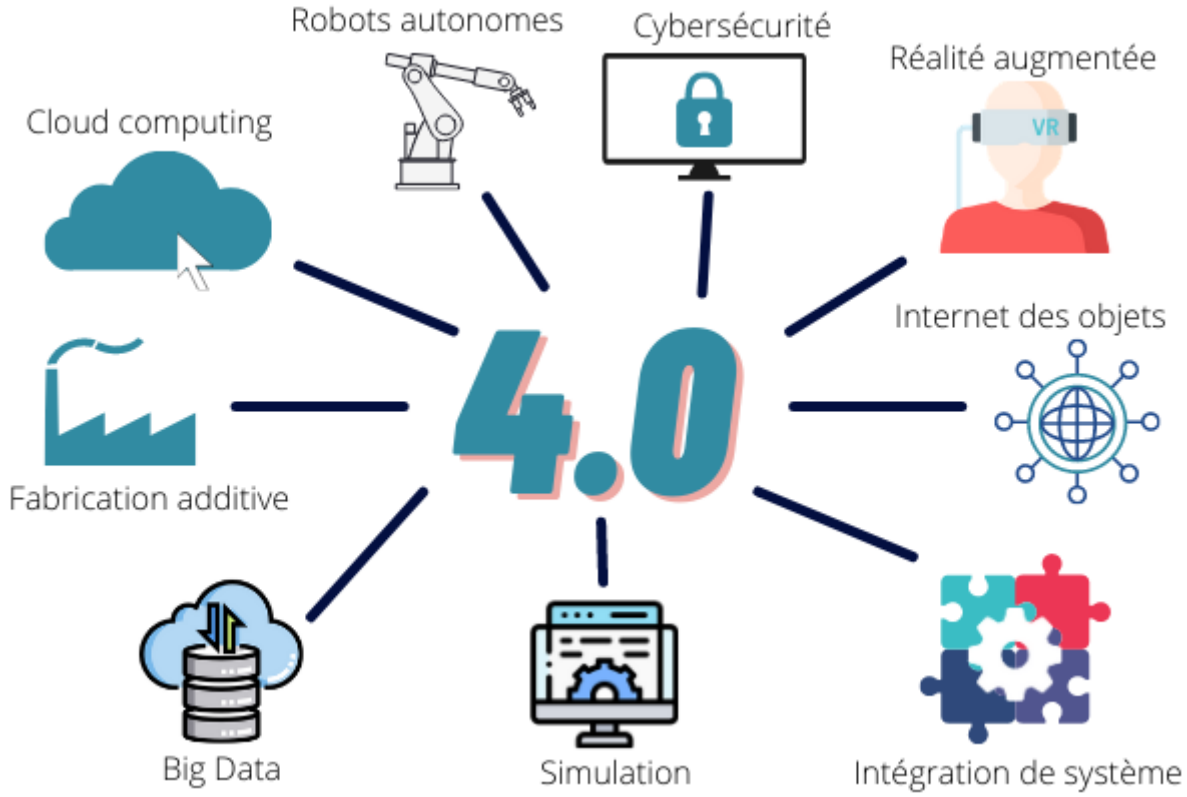


Figure II-1 Industrie 4.0

II.3.2 Application de la blockchain dans l'industrie 4.0

En adoptant la vision de l'Industrie 4.0, de nombreux secteurs industriels envisagent le potentiel de faire progresser leurs systèmes pour atteindre une productivité, une rentabilité, une fiabilité, une qualité et une flexibilité accrues. L'industrie manufacturière est un secteur important qui peut grandement bénéficier de l'adoption des principes et technologies de

l’Industrie 4.0. Cela contribuera à créer l'ère de la fabrication intelligente où les technologies et les systèmes avancés de l'Industrie 4.0 amélioreront les différents processus au sein de la chaîne de valeur de fabrication et augmenteront l'efficacité et la rentabilité. Cependant, l'Industrie 4.0 nécessite une intégration efficace de nombreuses technologies et systèmes et des opérations transparentes sur tous les composants. Cela crée de nombreux défis lors de la création d'applications pour une fabrication intelligente, notamment la sécurité, la confiance, la traçabilité, la fiabilité et l'automatisation des accords au sein de la chaîne de valeur de la fabrication. Plusieurs de ces défis peuvent être relevés à l'aide de la blockchain. [18]

II.4 L’utilisation de la blockchain dans l’industrie

II.4.1 Partage des informations pour la traçabilité et la transparence

Utiliser la blockchain pour suivre l’intégralité des étapes du cycle de vie d’un produit, de la matière première au produit fini. Cela offrirait une traçabilité permettant d’optimiser la logistique (délais de livraison, tracer des fournisseurs ayant fourni des produits non conformes…). [13]

La technologie Blockchain peut permettre de répondre à ces questions tout en apportant de la valeur sur la chaine logistique : elle garantit de façon quasi immédiate une traçabilité à moindre coût dans un environnement où les acteurs sont parfois très nombreux. [14]

Les informations sur un produit final doivent être aussi complètes, fiables et facilement accessibles que possible. Le code QR peut permettre le partage de telles informations, par exemple, qui donne accès à toutes les informations disponibles sur l'origine des composants individuels ou les conditions de production, le transport et l'emballage. Dans l'industrie agroalimentaire, de telles informations traçables et fiables sont également importantes pour les parties prenantes de la chaîne de production, afin qu'elles puissent s'assurer qu'elles respectent les réglementations nécessaires et documenter cette conformité. Mais avant que les données à travers plusieurs étapes de la chaîne d'approvisionnement puissent être incorporées dans la blockchain, elles doivent être vérifiées par toutes les personnes impliquées dans le réseau. Cela fournira au consommateur une chaîne d'information ininterrompue qui peut être examinée à tout moment, et garantira que le produit a été fabriqué et transporté dans des conditions optimales. [15]

II.4.2 Validation des conditions de travail tout au long de la chaîne logistique

Les entreprises du secteur alimentaire et les détaillants ont une tâche difficile de vérifier qu'aucune pratique déloyale de travail n'a été utilisée tout au long de la chaîne d'approvisionnement. Une fois que chaque travailleur a une identification de confiance représentée sur la blockchain, les agriculteurs ou les fournisseurs peuvent alors créer et enregistrer un contrat de travail qui spécifie des informations telles que les conditions de paiement, les heures de travail ou le rendement prévus, la durée du contrat et les conditions de travail. Les travailleurs peuvent ensuite recevoir un paiement numériquement, dont le reçu est automatiquement enregistré dans la blockchain et la confirmation de paiement est partagée avec les organisations en aval. Bien que la blockchain soit capable d'enregistrer les données, le succès de ce cas d'utilisation dépend de son adoption et de son application. À l'instar d'autres certifications de pratiques de travail, les agriculteurs et les coopératives pourraient être incités à adopter cette solution et à leur tour augmenté la valeur de leurs produits transformer l’audit et le traçage agroalimentaire [15]

II.4.3 Dans la chaîne logistique alimentaire

La chaîne logistique alimentaire est confrontée à des défis sans précédent concernant la santé humaine, la sécurité et la sûreté alimentaires, le changement climatique et le bien-être animal. Pour relever ces défis, garantir la transparence et la traçabilité dans la chaîne d'approvisionnement alimentaire devient une question de plus en plus importante pour réduire les pertes et gaspillages alimentaires et garantir la sécurité alimentaire. En particulier, la numérisation et les nouvelles technologies de l'information qui se développent rapidement avec l'Industrie 4.0 et leurs applications à la chaîne d'approvisionnement conduisent à des améliorations significatives des systèmes de traçabilité. L'une de ces nouvelles technologies est la blockchain. [15]

La technologie Blockchain permet, dans ce contexte, d’offrir un système dans lequel chaque étape du cycle de production peut être cartographiée en temps réel et enregistrée de manière sécurisée et immuable. Ainsi tous les acteurs de la filière peuvent connaître le parcours des produits et l’implication de chacun de leurs partenaires, et le contrôle de la conformité du cycle de production par les régulateurs et auditeurs externes est instantané.

De nombreux projets ont été lancés, et notamment par Carrefour qui expérimente une solution Blockchain pour assurer la traçabilité de son poulet d’Auvergne [14]

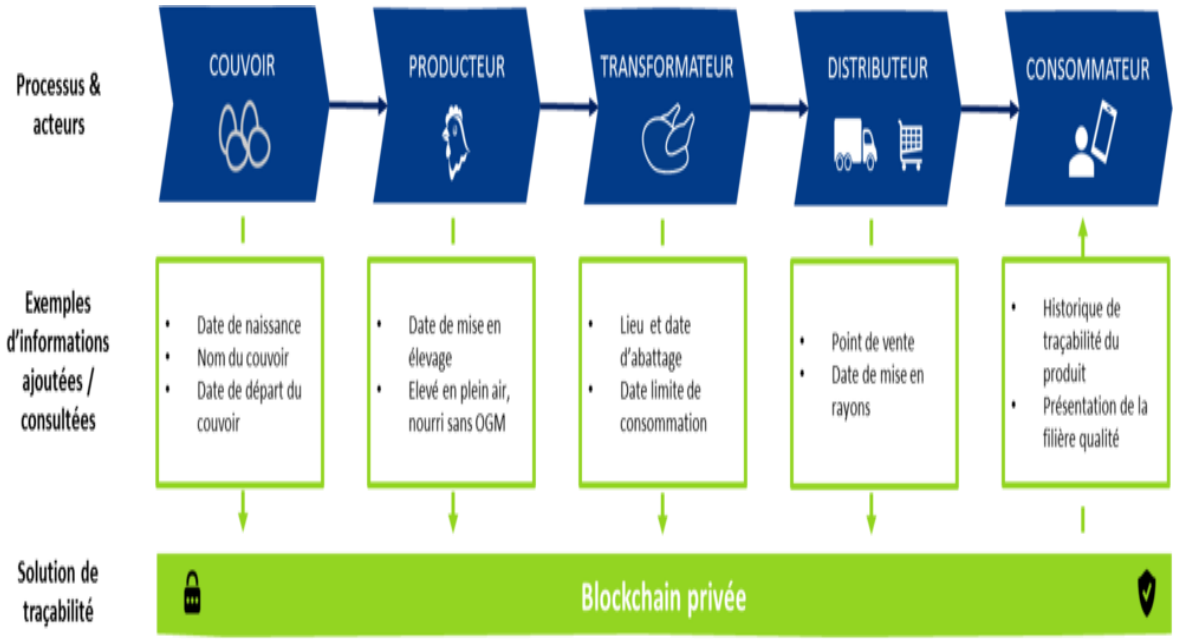


Figure II-2 Blockchain dans une chaine logistique alimentaire

II.4.4 Industrie de la logistique

Les applications de gestion logistique sont des systèmes logiciels qui aident à gérer la livraison des matières premières, des produits et des services entre les producteurs / vendeurs et les destinations des consommateurs. Ceux-ci peuvent tous faire partie d'une seule organisation ou être exécutés dans plusieurs organisations et entités. La blockchain peut fournir un support puissant pour activer ces applications. La blockchain peut fournir un support puissant pour activer ces applications. L'une des complexités de la gestion logistique est l'implication de plusieurs entreprises dans les activités. Cela peut également inclure un certain nombre de sous-activités synchronisées exécutées par différentes sociétés telles que des usines, des sociétés de stockage, des sociétés de transport maritime et des autorités de régularité. Il est important pour toute application de gestion logistique de fournir un ensemble de fonctions pour planifier, planifier, coordonner, surveiller et valider les activités effectuées. Ces fonctions peuvent être prises en charge de manière efficace et sécurisée par la blockchain. L'utilisation des registres distribués partagés dans la blockchain pour vérifier, stocker et auditer les transactions logistiques aidera à réduire les délais, les coûts de gestion et les erreurs humaines. En outre, l'application de contrats intelligents facilitera les accords entre les

entreprises concernées et créera des contrats contraignants plus rapidement et à moindre coût. [21]

II.4.5 Secteur financier

Poussé par le succès de la blockchain dans la prise en charge des crypto-monnaies, il était logique que l'industrie financière la suive avec des applications de blockchain dans d'autres domaines financiers. En général, des tiers de confiance sont utilisés pour mener des activités financières entre les personnes et les organisations. Ces tiers assurent quatre fonctions [20] :

- Confirmer la réalité des métiers.
- Éviter les duplications de transactions financières.
- Enregistrement et validation des activités financières.
- Fonctionner en tant qu'agents à l'appui des clients ou des associés.

La blockchain peut généralement remplacer deux de ces rôles : éviter les doublons de transaction et enregistrer et valider les activités financières. Avec la blockchain, il est facile d'empêcher, par exemple, un client d'effectuer plusieurs paiements avec un montant total supérieur à ce qu'il doit. En fait, il est possible d'effectuer illégalement cet acte avec des contrôles réguliers. Cependant, il est impossible d'y parvenir avec la blockchain car toutes les activités financières doivent être vérifiées collectivement avant d'être exécutées. Dans le même temps, la blockchain peut servir de registre sécurisé pour les transactions financières effectuées. Ce registre ne peut être modifié par aucune entité impliquée après avoir été ajouté à la chaîne. Il peut également être utilisé pour valider les transactions effectuées par le biais de contrôles collectifs et de vérifications. Ces deux fonctionnalités permettent de nombreuses applications financières. [21]

II.4.6 Industrie de l'énergie

L'une des principales utilisations de la blockchain dans les applications liées à l'énergie est le micro réseaux. Un micro réseau est un ensemble localisé de sources d'énergie électrique et de charges intégrées et gérées dans le but d'améliorer l'efficacité et la fiabilité de la production et de la consommation d'énergie [22].

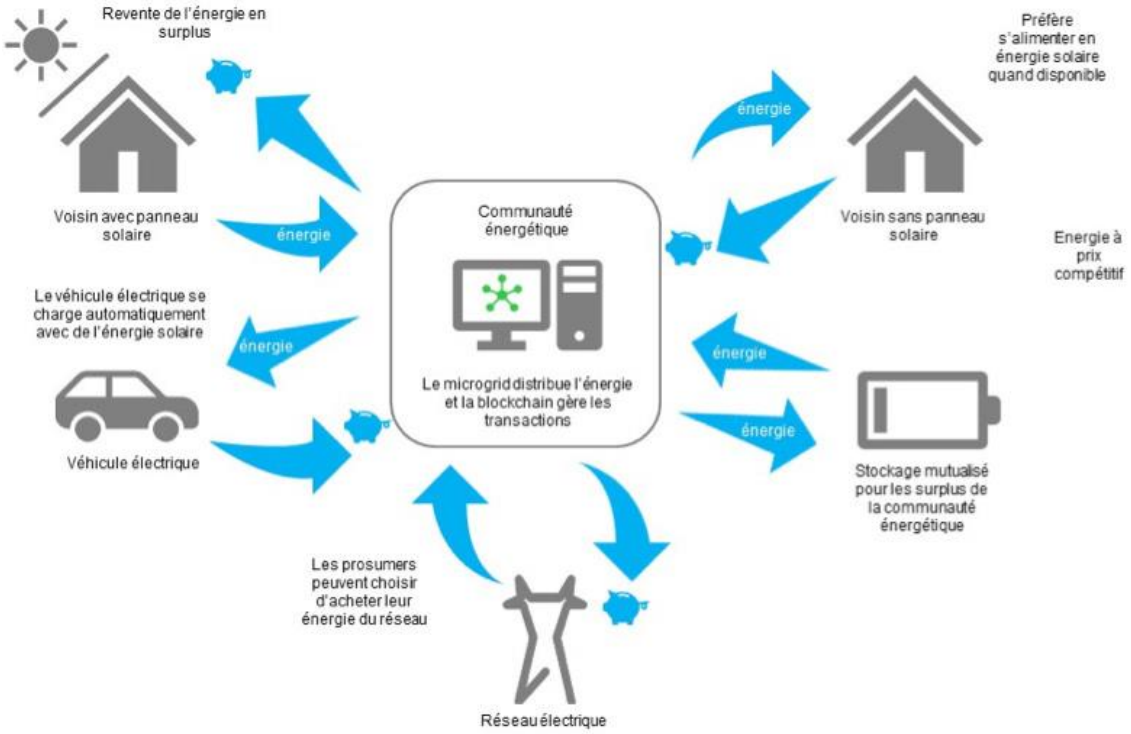


Figure II-3 Schéma d'une communauté énergétique utilisant la technologie Blockchain

Les sources d'énergie électrique peuvent être des générateurs d'énergie distribués, des stations d'énergie renouvelable et des composants de stockage d'énergie dans des installations créées et détenues par différentes organisations ou fournisseurs d'énergie. L'un des principaux avantages de la technologie des micro réseaux est qu'elle permet non seulement aux résidents et aux autres consommateurs d'électricité tels que les usines d'avoir accès à l'énergie nécessaire, mais ils peuvent également produire et vendre l'énergie excédentaire au réseau. La blockchain peut être utilisée pour faciliter, enregistrer et valider les transactions de vente et d'achat d'énergie dans les micro-réseaux [23]. Cela permet d'appliquer des restrictions et des réglementations en matière d'échange d'électricité, de gérer les paiements et de prendre des décisions partagées équitablement et efficacement entre les participants sans avoir besoin d'un contrôleur de micro réseau centralisé [24]. Pae exemple, la blockchain est utilisée dans un micro réseau qui regroupe 130 bâtiments à Brooklyn, New York [25], [26]. Cela minimise ou

élimine le besoin d'intermédiaires parmi ces bâtiments pour terminer leurs transactions de vente et d'achat d'énergie. De plus, la blockchain peut être utilisée dans les micro réseaux insulaires pour suivre les pertes d'énergie produites par les transactions énergétiques. Cela conduit à une meilleure adéquation entre la position physique et les pertes d'énergie sur le réseau de réseau et les coûts qui en résultent attribués aux participants [27].

De la même manière, la blockchain peut être utilisée à plus grande échelle pour permettre le commerce d'énergie dans les réseaux intelligents. Dans les réseaux intelligents équipés d'un flux de communication bidirectionnel, la blockchain peut être utilisée pour prendre en charge une surveillance de la consommation et un commerce d'énergie sécurisés et préservés par la confidentialité [28] sans avoir besoin d'un intermédiaire central. Il peut également être utilisé pour soutenir la gestion des programmes de réponse à la demande [29]. Les contrats intelligents peuvent être utilisés pour garantir les descriptions programmatiques des degrés de flexibilité de puissance prévus, la validation et la traficabilité des accords de réponse à la demande, et l'équilibre entre les besoins et la production d’électricité. [21].

II.4.7 Industrie de la robotique

La robotique a de nombreuses applications industrielles potentielles, notamment le transport de matériaux et l'agriculture de précision. Cependant, de nombreux défis empêchent ces technologies d'être développées et utilisées dans la pratique, notamment des capacités autonomes, des contrôles décentralisés et des comportements collaboratifs. Comme la technologie blockchain peut être utilisée entre plusieurs entités distribuées pour conclure des accords sans avoir besoin d'une autorité de contrôle, elle peut être utilisée dans des applications de robotique en essaim dans le même but et pour ajouter des fonctionnalités de sécurité, d'autonomie et de flexibilité. Cela permet de créer des applications de robotique en essaim plus sécurisées, capables de prendre de meilleures décisions de manière distribuée pour des opérations efficaces. L'utilisation de la blockchain peut également permettre de gérer des robots byzantins dans un scénario de prise de décision collective en robotique en essaim. Avec toutes ces capacités, de nouveaux modèles commerciaux et industriels pour les applications de robotique en essaim peuvent facilement être créés. Chaque sous-tâche du robot peut être représentée comme une transaction. Un ensemble de transactions synchronisées et coordonnées est généralement nécessaire pour mener à bien une mission. L'utilisation de la blockchain pour gérer ces transactions peut offrir certains avantages [21] :

- De nouvelles mesures de sécurité peuvent être appliquées pour protéger les applications de robotique en essaim. Étant donné que tous les efforts de coordination et de synchronisation doivent être communiqués sur un réseau, une communication et une vérification sécurisée des messages sont essentielles. La blockchain permet les communications robotiques en essaim et la vérification des transactions, facilitant ainsi davantage d'applications, y compris des applications critiques [21].
- Une application de mission spécifique peut être conçue, mise en œuvre et exécutée sans effort en négociant et en convenant de transactions spécifiques nécessaires à la mission, puis en les enregistrant dans un registre blockchain pour vérification, exécution et référence future [21].
- L'utilisation de la blockchain ajoute une grande flexibilité dans l'utilisation de la robotique en essaim pour différentes applications grâce aux capacités supplémentaires introduites [21].
- La blockchain peut être utilisée pour offrir une possibilité de confirmer que les robots n'exécuteront les transactions convenues que dans le cadre de responsabilités légales et de mesures de sécurité acceptables [21].

II.4.8 Dans l’industrie de pharmaceutique :

Compte tenu de la capacité de la technologie blockchain à permettre des transactions sécurisées et rapides dans le monde entier, une grande partie des efforts de l'industrie pharmaceutique pour tirer parti de ses capacités se concentrent sur l'amélioration de la chaîne logistique.

L'un des plus grands avantages de la technologie blockchain est la possibilité de créer une piste vérifiable et traçable pour d'établir la provenance des médicaments sur l'ensemble de la chaîne logistique. Avec la solution de blockchain décentralisée, les fabricants et leurs clients seraient en mesure de vérifier indépendamment la qualité et le point d'origine des médicaments rapidement et en toute sécurité.

La transparence et la sécurité sont deux autres avantages clés de la technologie blockchain pour les membres de la chaîne logistique pharmaceutique. Toutes les parties prenantes impliquées dans la chaîne logistique doivent être en mesure de partager et de mettre à jour les données tout en s'assurant que les données sont opportunes et exactes. Avec la technologie

blockchain, l'ensemble de la chaîne logistique peut être géré avec un seul logiciel qui est partagé entre les personnes autorisées. Les parties prenantes. En plus des fabricants de médicaments et de leurs fournisseurs, les payeurs, les prestataires, les pharmacies et les patients peuvent accéder aux données et voir quand elles sont mises à jour en temps quasi réel.

La technologie Blockchain a également le potentiel d'aider à prévenir le détournement, la contrefaçon et la falsification, car les produits pharmaceutiques peuvent être suivis depuis le moment où ils sont produits jusqu'au moment où ils atteignent les patients. Toute tentative de modification des enregistrements sera immédiatement visible pour toutes les parties.

Tout aussi important, les rappels sont beaucoup plus simples. Le produit peut être facilement retracé jusqu'au fabricant et associé à un lot de production, ce qui permet d'identifier d'autres produits potentiellement problématiques et l'endroit où ils ont été expédiés.

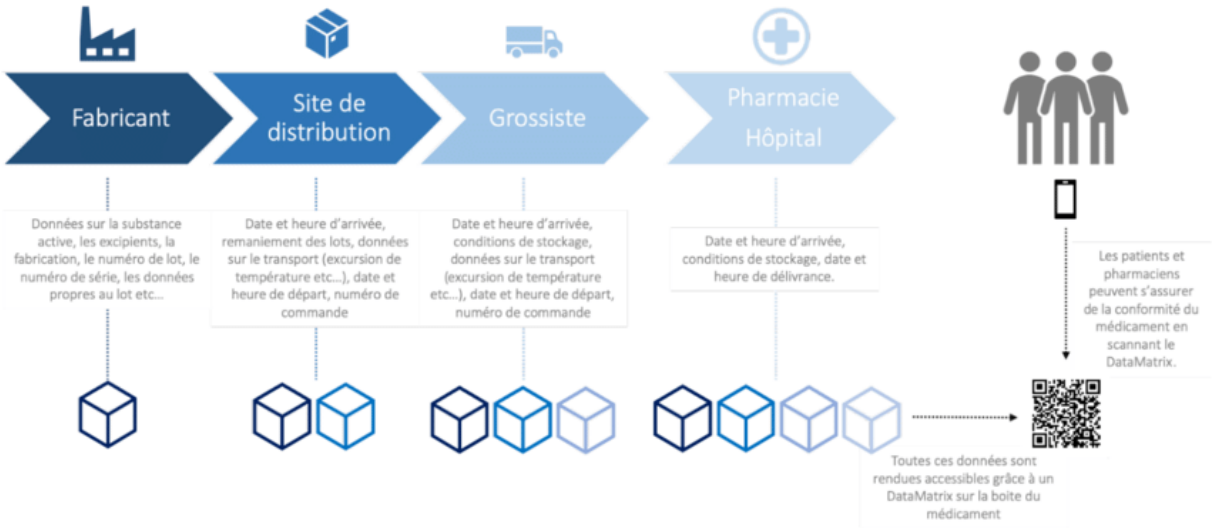


Figure II-4 Blockchain dans le Domain médical

II.4.9 L’utilisation de « smart contracts »

Ces contrats intelligents permettraient l’automatisation de la chaîne de production en complément d’un ERP traditionnel (par exemple commande sécurisée de matière première automatique lorsque niveaux de stocks bas). [13]

II.5 Conclusion :

Les Blockchains peuvent être configurées pour fonctionner de différentes manières, en utilisant différents mécanismes pour garantir un consensus sur les transactions, vues uniquement par les utilisateurs autorisés et refusées à tous les autres. Bitcoin est l'exemple le plus connu qui montre à quel point la technologie Blockchain est devenue énorme. Les fondateurs de Blockchain testent également de nombreuses autres applications pour étendre le niveau de technologie et d'influence de Blockchain. À en juger par son succès et son utilisation accrue, il semble que la Blockchain soit sur le point de régner sur le monde numérique dans un avenir proche.

Chapitre III

Préparation de l’environnement pour simuler la Blockchain dans une chaine logistique.

III.1 Introduction:

Comme on a vue dans le chapitre 2 que la Blockchain a été initialement inventée pour réaliser des transactions d'argent numérique sécurisées, mais la technologie à maintenant commencé à popularité dans divers autres domaines tels que le tourisme, l'immobilier, le vote, la bourse, la gestion de la chaîne logistique, etc. La technologie Blockchain gagne accumulation ultime dans le secteur de la santé. Le secteur de la santé se compose de données sensibles en croissance rapide qui doivent être préservées des menaces de confidentialité et des menaces d'intégrité. Parmi les nombreuses applications de la blockchain dans le domaine de la santé, les deux applications les plus importantes sont la gestion des données et la traçabilité des médicaments. De plus, Nous avons proposé un système basé sur la blockchain qui est capable de suivre le mouvement des médicaments tout au long de la chaîne logistique, du fabricant aux patients finaux. Ce système contribuera à lutter contre la contrefaçon de médicaments.

III.2 Traitement des données Médicales :

L'industrie de la santé est un secteur qui implique une grande quantité de données sensibles. Étant donné que le nombre de maladies et de patients ne cesse d'augmenter, les données qui doivent être traitées et gérées dans ce secteur sont également en augmentation considérable. Le traitement des données dans le domaine de la santé implique le contrôle d'accès, le partage et le stockage des données. Les données sont stockées sous forme de **dossiers de santé électroniques** (DSE). Un **DSE** contient essentiellement les antécédents médicaux d'un patient qui peuvent être partagés entre et utilisé par diverses organisations. Deux menaces majeures posées par le partage des DSE sont les menaces à la vie privée et à l'intégrité.

III.3 Problèmes avec la gestion actuelle des données de santé :

Actuellement, il existe de nombreux problèmes liés au traitement des données de santé, en particulier au contrôle d'accès, au partage et au stockage des données. Deux défis majeurs qui ont agacé les parties prenantes sont les normes de données variables et l'interopérabilité. Certaines autres menaces qui bloquent le stockage fluide des données dans les soins de santé sont l'évolutivité, les performances et la disponibilité des données.

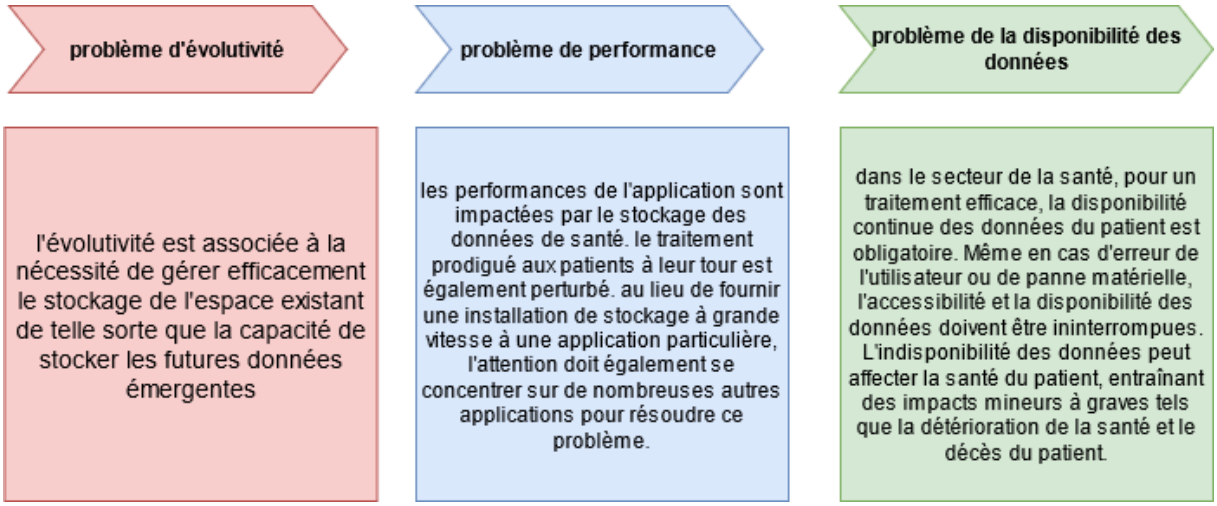


Figure III-1 Problèmes de traitement des données dans le domaine de la santé.

III.4 Comment la Blockchain résout ces problèmes de gestion des données :

Les systèmes traditionnels de traçabilité des médicaments sont inefficaces et manquent d'exigences majeures pour la gestion de la chaîne logistique pharmaceutique. Les problèmes suivants avec les approches générales de traçabilité des médicaments décrivent le besoin de blockchain dans la traçabilité des médicaments.

III.4.1 Problème de visibilité :

Le manque de visibilité dans les systèmes de santé actuels est un problème majeur qui accroît les problèmes tels que les pénuries de médicaments, les opioïdes et les contrefaçons. De plus, en raison du manque de transparence, les patientes et autres parties prenantes ne sont pas en mesure de suivre efficacement les mouvements de médicaments dans la chaîne logistique.

« La contrebande du médicament fait rage en Algérie. Le phénomène qui s'est installé progressivement tout au long de ces dernières années s'est malheureusement étendu à l'ensemble du territoire national au détriment des malades qui ignorent encore les risques pris en consommant des produits introduits frauduleusement.

Une importante quantité de médicaments a été saisie par les éléments de la Sûreté de wilaya de Tamanrasset, au cours de la semaine, une mise en cause dans une affaire de trafic illicite de produits pharmaceutiques et saisi ; 650392 comprimés, indique la Direction générale de la sûreté nationale (DGSN). » [30]

III.4.2 Problème des consentements réglementaires :

Une grande quantité d'ingrédients pharmaceutiques nécessaires à la fabrication de médicaments sont importés de l'extérieur du pays. Chaque étape, de la production à la distribution des médicaments, doit respecter les réglementations de la chaîne logistique des médicaments.

III.4.3 Problème d'expédition de la chaîne du froid :

De nombreux médicaments sont de nature sensible et nécessitent d'être conservés dans un environnement à température contrôlée. Mais dans les logiciels actuels, le stockage de ces informations d'expédition de la chaîne du froid se fait sur les bases de données centralisées qui sont très sujettes aux d’attaque cybernétique et aux manipulations de données.

III.5 Méthodologie proposée pour la conception :

Comme nous le savons l'importance de l'industrie pharmaceutique pour la vie humaine et du risque constant de produits/médicaments contrefaits. Pour surmonter cette lacune du système conventionnel de gestion de la chaîne logistique de l'industrie pharmaceutique, nous pouvons utiliser la blockchain. Actuellement, c'est la seule plate-forme disponible qui peut offrir une si grande fonctionnalité de sécurité. La blockchain semble avoir un avenir très prometteur en raison des fonctionnalités qu'elle propose. On peut voir que la blockchain a la solution à de nombreux problèmes auxquels l'industrie pharmaceutique est confrontée.

Tout modèle de chaîne logistique en général implique de nombreuses parties entre les parties, mais dans notre flux de travail, nous l'avons restreint à un modèle rigide consistant à n'avoir que quatre acteurs pour réduire la complexité. Ces acteurs peuvent appartenir à différentes organisations mais sont principalement classés en fabricants, distributeurs, pharmacie/hôpital et clients à la fin de la chaîne logistique pharmaceutique recevant la sortie. Les fabricants sont en fait les responsables de la création du médicament et, parallèlement à la création, de l'ajout de différents critères tels que la date de péremption, le prix et un champ de propriétaire actuel avec l'attribut de clé primaire connu sous le nom d'identifiant du médicament. Une fois qu'un médicament est créé par le fabricant d'une organisation, il ajoute ensuite ce médicament au stockage de la blockchain et est disponible chaque fois qu'un acteur détenant le médicament souhaite connaître l'historique de ce médicament. Ces identifiants de médicaments jouent un rôle clé dans l'identification des faux médicaments par rapport aux vrais.

Le propriétaire initial du médicament doit toujours être le fabricant, et ces données doivent toujours être récupérées à partir du même réseau blockchain et non à partir d'autres sources ou bases de données non fiables présentes sur Internet. Après cela, un fabricant peut transférer un produit/médicament à un autre acteur du réseau blockchain qui peut être un distributeur ou tout autre acteur de la chaîne d'approvisionnement. De nombreuses questions surgissent concernant ces tâches initiales de base, et celles-ci sont soigneusement étudiées et examinées afin de les résoudre avant que cette solution ne soit mise en pratique.

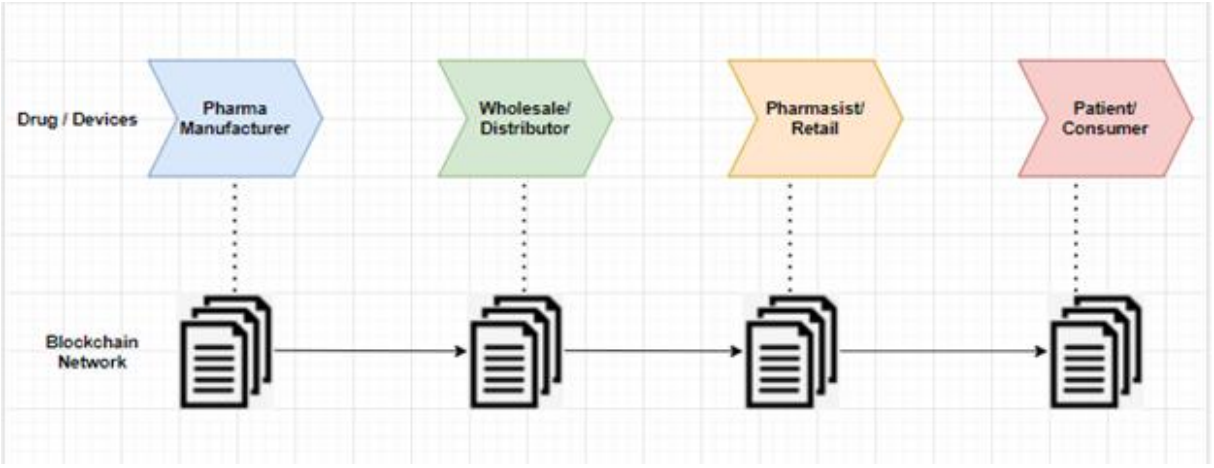


Figure III-2 Schéma simplifier de notre idée

III.6 Les outils utilisés pour la réalisation :

III.6.1 Visual Studio Code éditeur :

Visual Studio Code est un éditeur de code simplifié prenant en charge les opérations de développement telles que le débogage (signaler les erreurs dans le programme et essayer de les corriger), l'exécution de tâches et le contrôle de version. Il vise à fournir uniquement les outils dont un développeur a besoin pour un cycle de création de code-débogage rapide et laisse des flux de travail plus complexes à des IDE plus complets, tels que Visual Studio IDE.0, c'est l'un des produis de Microsoft et c'est complètement gratuit.

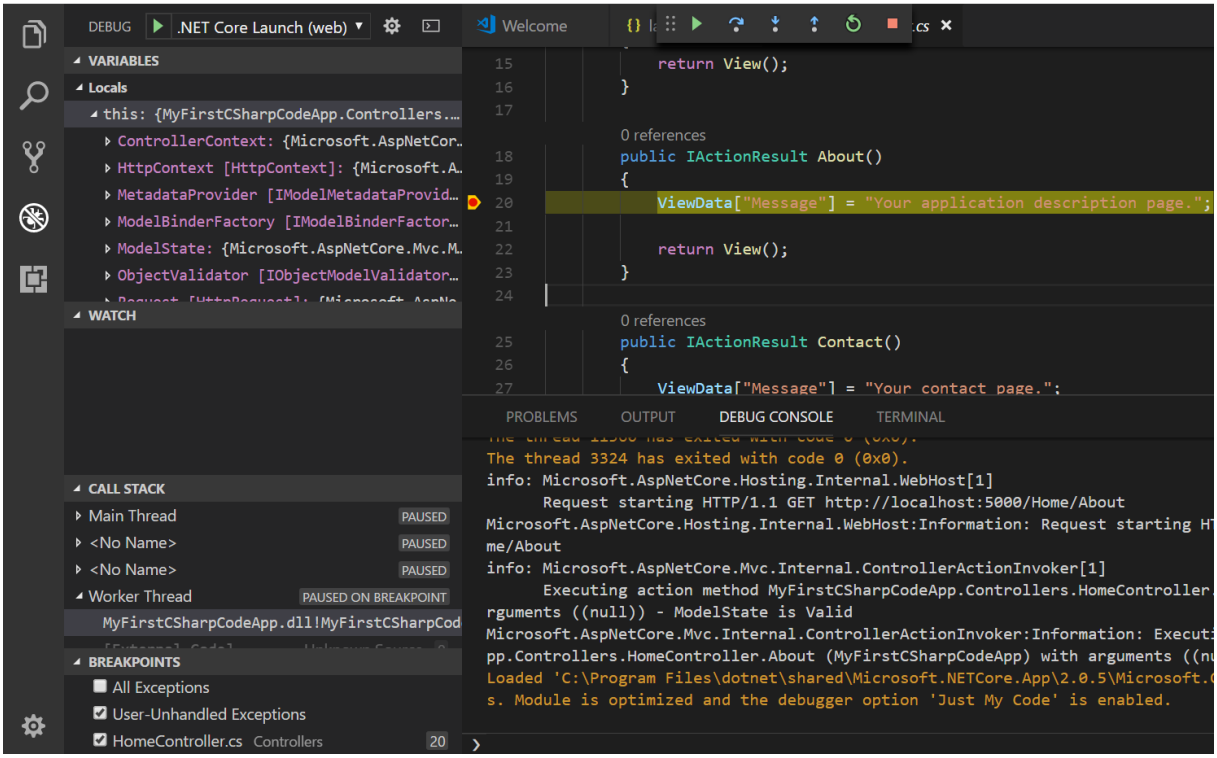


Figure III-3 Interface de visual studio

III.6.2 Les outils d'application web :

III.6.2.1 NodeJs :

NodeJS est un environnement d'exécution permettant d'utiliser le JavaScript côté serveur. Grâce à son fonctionnement non bloquant, il permet de concevoir des applications en réseau performantes, telles qu'un **serveur web**, une **API** ou un **CORN** JOB (est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance).

La solution apportée par Node.js repose sur trois bases fondamentales :

- Le moteur JavaScript V8 développé par Google, qui permet d'exécuter du code JavaScript à l'intérieur de Google Chrome et, grâce à Node, directement sur le serveur.
- Une boucle d'événements, appelée aussi event loop NodeJS, permettant d'exécuter plusieurs opérations simultanées de façon asynchrone et non bloquante en tirant profit des multiples fils d'exécution (multithreading) des noyaux des processeurs modernes.
- Une API de bas niveau basée sur la structure entrées-sorties (I/O) dénommée libuv, qui permet d'adopter une approche de programmation événementielle.

- Un ensemble d'un ou plusieurs modules est communément appelé paquet, et ces paquets sont eux-mêmes organisés par des gestionnaires de paquets. Node.js Package Manager (**npm**) est le gestionnaire de paquets par défaut et le plus populaire dans l'écosystème Node.

Node présente de nombreux avantages face aux méthodes et langages de développement web plus traditionnels côté serveur.

Figure III-4 les cas d'utilisation de Nodejs

III.6.2.2 Angular JS :

AngularJS est un **framework web** de Google. C'est un logiciel libre (licence MIT) dont l'essentiel des contributeurs travaillent pour Google. Il permet de réaliser des applications web en mode Single Page Application. C'est à dire une seule page qui ne se recharge jamais. L'idée de base est d'augmenter le langage HTML pour permettre la représentation des données métiers, qui sont-elles traitées et gérées avec le langage Javascript.

AngularJS est une bibliothèque très riche, elle couvre 100% des besoins fondamentaux dans la réalisation d'une application web.

```
<!DOCTYPE html>
<html>
<script
src="https://ajax.googleapis.com/ajax/libs/angularjs/1.6.9/angular.min.js">
</script>
<body>

<div ng-app="">

<p>insérer vos information:</p>
<p>Nom: <input type="text" ng-model="name"></p>
<p>Prénom: <input type="text" ng-model="name"></p>

<p ng-bind="name"></p>

</div>

</body>
</html>
```

insérer vos information:

Nom:

Prénom:

Figure III-5Exemple web App avec Angularjs

- AngularJS est distribué sous forme de fichier JavaScript et peut être ajouté à une page Web avec une balise de script :

```
<script src="https://ajax.googleapis.com/ajax/libs/angularjs/1.6.9/angular
.min.js"></script>.
```

Figure III-6 les avantages d'AngularJs

III.6.2.3 Javascript :

JavaScript est un langage de script, multi-plateforme et orienté objet. C'est un langage léger qui doit faire partie d'un environnement hôte (un navigateur web par exemple) pour qu'il puisse être utilisé sur les objets de cet environnement.

JavaScript contient une bibliothèque standard d'objets tels que Array, Date, et Math, ainsi qu'un ensemble d'éléments de langage tels que les opérateurs, les structures de contrôles et les instructions. Ces fonctionnalités centrales et natives de JavaScript peuvent être étendues de plusieurs façons en fournissant d'autres objets, par exemple :

1. L'utilisateur clique sur un lien ou entre une adresse.
2. Son navigateur charge la page Web. Il voit le texte, les couleurs, les images.
3. Si la page Web contient du code Javascript, le navigateur lit le code Javascript et suit les instructions du code.

Le code Javascript sert donc à donner du dynamisme à la page. Sans lui, la page ressemble à une page de livre, un peu animée (grâce à un autre langage appelé le HTML, CSS), mais qui ne change pas beaucoup.

```
<!DOCTYPE html>
<html>
<head>
<script>
function myFunction() {
  document.getElementById("demo").innerHTML = "Paragraph changed.";
}
</script>
</head>
<body>

<h2>exemple javascript </h2>

<p id="demo">cliquer ici pour Télécharger </p>

<button type="button" onclick="myFunction()">Télécharger</button>

</body>
</html>
```

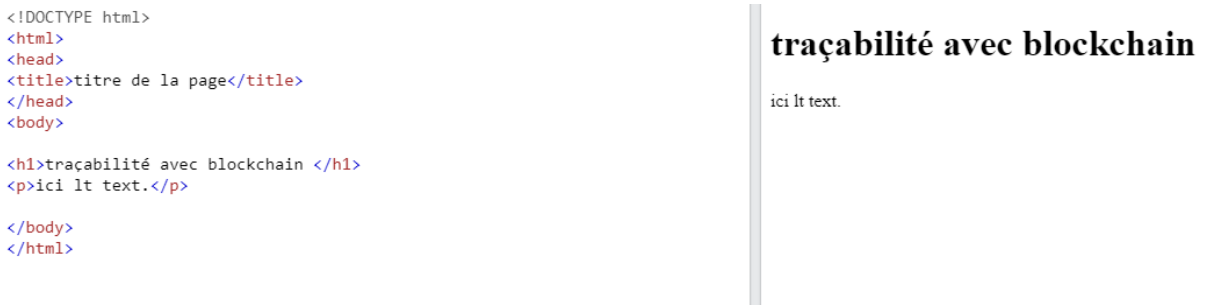
Figure III-7 Exemple programmation de Javascript

- on voit qu'une fonction JavaScript est placée dans la section **<head>** d'une page HTML.

III.6.2.4 HTML :

L'HyperText Markup Language, HTML, désigne un type de langage informatique descriptif. Il s'agit plus précisément d'un format de données utilisé dans l'univers d'Internet pour la mise en forme des pages Web. Il permet, entre autres, d'écrire de l'hypertexte, mais aussi d'introduire des ressources multimédias dans un contenu.

L'**HTML** est ce qui permet à un créateur de sites Web de gérer la manière dont le contenu de ses pages Web va s'afficher sur un écran, via le navigateur. Il repose sur un système de balises permettant de titrer, sous-titrer, mettre en gras, etc.



```
<!DOCTYPE html>
<html>
<head>
<title>titre de la page</title>
</head>
<body>

<h1>traçabilité avec blockchain </h1>
<p>ici lt text.</p>

</body>
</html>
```

traçabilité avec blockchain

ici lt text.

Figure III-8Exemple simple programmation HTML

- La déclaration <!DOCTYPE html> définit que ce document est un document HTML5
- L'élément <html> est l'élément racine d'une page HTML
- L'élément <head> contient des méta-informations sur la page HTML
- L'élément <title> spécifie un titre pour la page HTML (qui est affiché dans la barre de titre du navigateur ou dans l'onglet de la page)
- L'élément <body> définit le corps du document et est un conteneur pour tous les contenus visibles, tels que les en-têtes, les paragraphes, les images, les hyperliens, les tableaux, les listes, etc.
- L'élément <h1> définit un grand titre
- L'élément <p> définit un paragraphe.

III.6.2.5 CSS 3 :

Le terme **CSS** est l'acronyme anglais de **Cascading Style Sheets** qui peut se traduire par "feuilles de style en cascade". Le CSS est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML. Ainsi, les feuilles de style, aussi appelé les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML.

```html
<!DOCTYPE html>
<html>
<head>
<style>
body {
  background-color: lightblue;
}

h1 {
  color: white;
  text-align: center;
}

p {
  font-family: verdana;
  font-size: 20px;
}
</style>
</head>
<body>

<h1>titre exemple</h1>
<p>texte.</p>

</body>
</html>
```

titre exemple

texte.

Figure III-9 Exemple programmation en CSS

- P est un sélecteur en CSS (il pointe vers l'élément HTML que vous souhaitez styliser : <p>).
- La 'color' est une propriété et le Blanc est la valeur de la propriété.
- Text-align est une propriété et center est la valeur de la propriété.

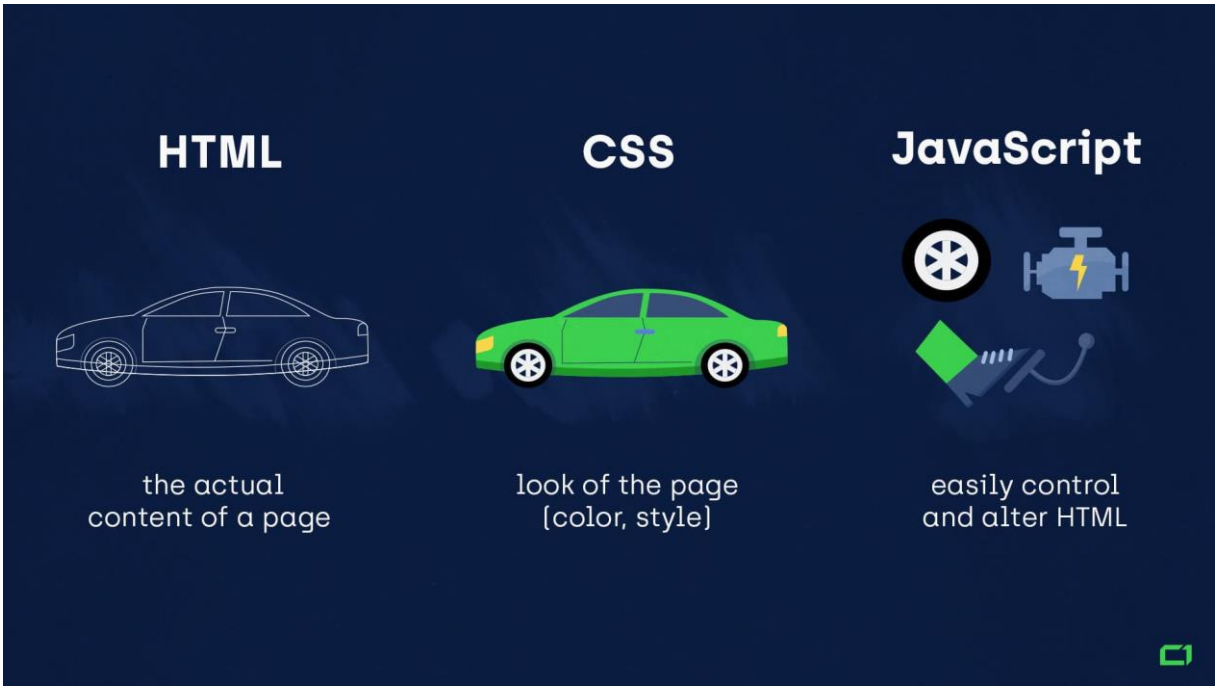


Figure III-10 Les trois langages de Dev web simplement expliqué

III.6.2.6 TypeScript :

TypeScript est un sur-ensemble de JavaScript qui fournit principalement un typage statique, des classes et des interfaces optionnels. L'un des grands avantages est de permettre aux IDE de fournir un environnement plus riche pour repérer les erreurs courantes pendant la programmation. Pour un grand projet JavaScript, l'adoption de TypeScript peut entraîner un logiciel plus robuste, tout en étant toujours déployable là où une application JavaScript normale s'exécuterait.

C'est open source, mais vous n'obtenez l'intelligent Intellisense que vous tapez si vous utilisez un IDE (**integrated development environment)** pris en charge. Au départ, il ne s'agissait que de Visual Studio de Microsoft (également noté dans un article de blog de Miguel de Icaza). De nos jours, d'autres IDE offre également la prise en charge de TypeScript. Donc L'objectif de TypeScript est d'aider à détecter les erreurs tôt dans un système de types et de rendre le développement JavaScript plus efficace.

III.6.2.7 Navigateur web google chrome :

On a choisi Chrome Dev come un web navigateur qu'il contient un environnement parfait pour exécuter notre programme. La version Dev de Chrome est plus sujette aux plantages, aux erreurs, aux problèmes de compatibilité des extensions, etc., car la mise à jour de cette version en est encore à ses débuts avec de nombreuses corrections de bogues et des correctifs en attente.

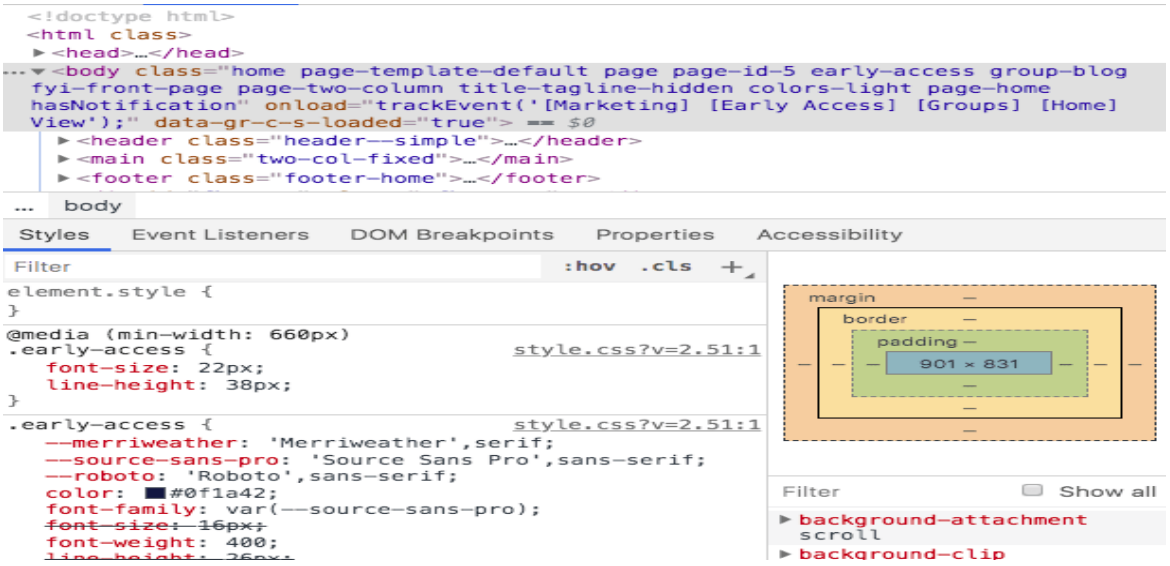


Figure III-11 console de Chrome dev

III.6.3 Les outils de la Blckchain :

III.6.3.1 Ethereum :

Ethereum est une plate-forme décentralisée, ce qui nous permet de déployer des DApps dessus. Les contrats intelligents sont écrits à l'aide du langage de programmation Solidity. Les DApps sont créés à l'aide d'un ou plusieurs contrats intelligents. Ethereum a une cryptomonnaie appelée Ether. Pour déployer des contrats intelligents ou pour appeler leurs méthodes, nous avons besoin d'Ether. Il peut y avoir plusieurs instances d'un contrat intelligent comme n'importe quel autre DApp, et chaque instance est identifiée par son adresse unique. Les comptes d'utilisateurs et les contrats intelligents peuvent contenir d'Ether.

Ethereum utilise une structure de données blockchain et un protocole de consensus de preuve de travail (proof of work). Une méthode d'un contrat intelligent peut être invoquée via une transaction ou via une autre méthode. Il existe deux types de nœuds dans le réseau : les nœuds réguliers et les mineurs. Les nœuds réguliers sont ceux qui n'ont qu'une copie de la blockchain, tandis que les mineurs construisent la blockchain en exploitant des blocs.

Pour créer un compte Ethereum, nous avons juste besoin d'une paire de clés asymétrique. Il existe différents algorithmes, tels que **RSA**, **ECC**, etc., pour générer des clés de chiffrement asymétriques. Ethereum utilise la cryptographie à courbe elliptique (ECC) (elliptic curve cryptography). ECC a plusieurs paramètres. Ces paramètres sont utilisés pour ajuster la vitesse et la sécurité. Ethereum utilise le paramètre secp256k1. Pour approfondir l'ECC et ses paramètres, il faudra des connaissances mathématiques, et il n'est pas nécessaire de les comprendre en profondeur pour créer des DApps à l'aide d'Ethereum.

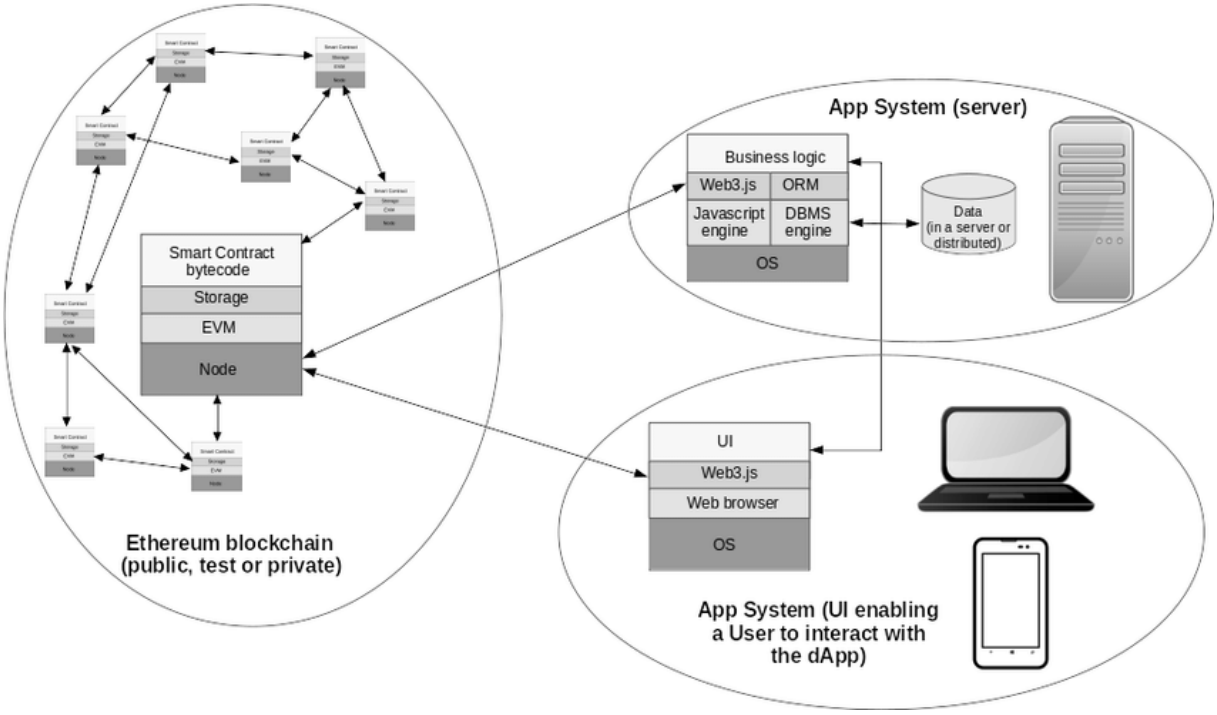


Figure III-12 le fonctionnement de DApp

III.6.3.2 Ethereum Virtual Machine :

EVM (ou machine virtuelle Ethereum) est l'environnement d'exécution de byte-code des contrats intelligents Ethereum. Chaque nœud du réseau exécute EVM. Tous les nœuds exécutent toutes les transactions qui pointent vers des contrats intelligents à l'aide d'EVM, de sorte que chaque nœud effectue les mêmes calculs et stocke les mêmes valeurs. Les transactions qui ne transfèrent que de l'Ether nécessitent également un certain calcul, c'est-à-dire pour savoir si l'adresse à un solde ou non et déduire le solde en conséquence.

III.6.3.3 Solidity :

Solidity est un langage de haut niveau orienté objet pour la mise en œuvre de contrats intelligents. Les contrats intelligents sont des programmes qui régissent le comportement des comptes au sein de l'état Ethereum. La solidité est un langage entre accolades. Il est influencé par C++, Python et JavaScript, et est conçu pour cibler la machine virtuelle Ethereum (EVM). Solidity est typé statiquement, prend en charge l'héritage, les bibliothèques et les types complexes définis par l'utilisateur, entre autres fonctionnalités. Avec Solidity, on peut créer des contrats pour des utilisations telles que le vote, le financement participatif, les enchères à l'aveugle les portefeuilles multi-signatures et les données des produits.

III.6.3.4 Remix IDE :

Remix IDE est une application Web et de bureau open source. Il favorise un cycle de développement rapide et dispose d'un riche ensemble de plugins avec des interfaces graphiques intuitives. Remix est utilisé pour tout le parcours de développement du contrat et constitue un terrain de jeu pour l'apprentissage et l'enseignement d'Ethereum. Remix IDE fait partie du projet Remix qui est une plate-forme pour les outils de développement utilisant une architecture de plugin. Il englobe des sous-projets, notamment Remix Plugin Engine, Remix Libs et bien sûr Remix-IDE.

Remix IDE est un puissant outil open source qui sert à rédiger des contrats Solidity directement depuis le navigateur.

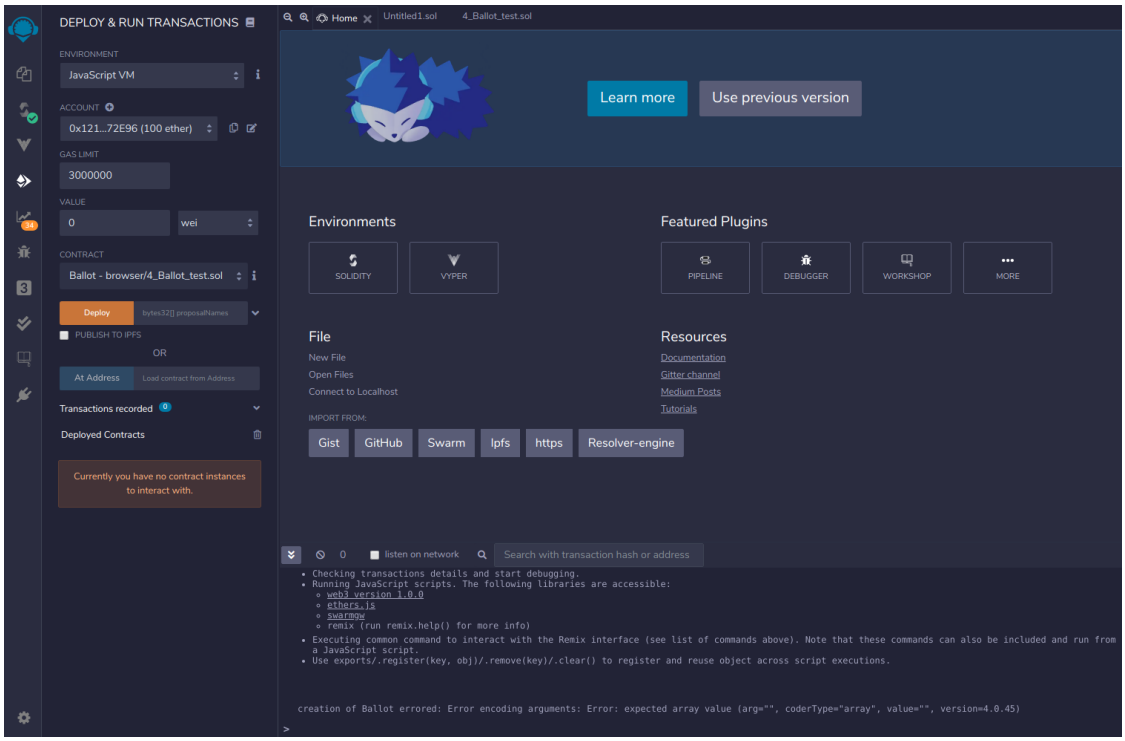


Figure III-13 interface d'IDE Remix

III.6.3.5 Web3 js :

Web3.js il fournit une abstraction pour masquer les travaux internes complexes des contrats intelligents sur la blockchain. En termes simples, une application Web implémentée en JavaScript communique avec un nœud Ethereum ou effectue des transactions avec un contrat

intelligent sur la blockchain à l'aide de la bibliothèque Web3.js en utilisant une connexion HTTP ou IPC.

III.6.3.6 Metamask :

MetaMask est une extension de navigateur conçue pour faciliter l'accès à l'écosystème Dapp d'Ethereum. Il sert également de portefeuille pour contenir des jetons ERC-20 permettant aux utilisateurs d'accéder aux services construits sur le réseau via le portefeuille.

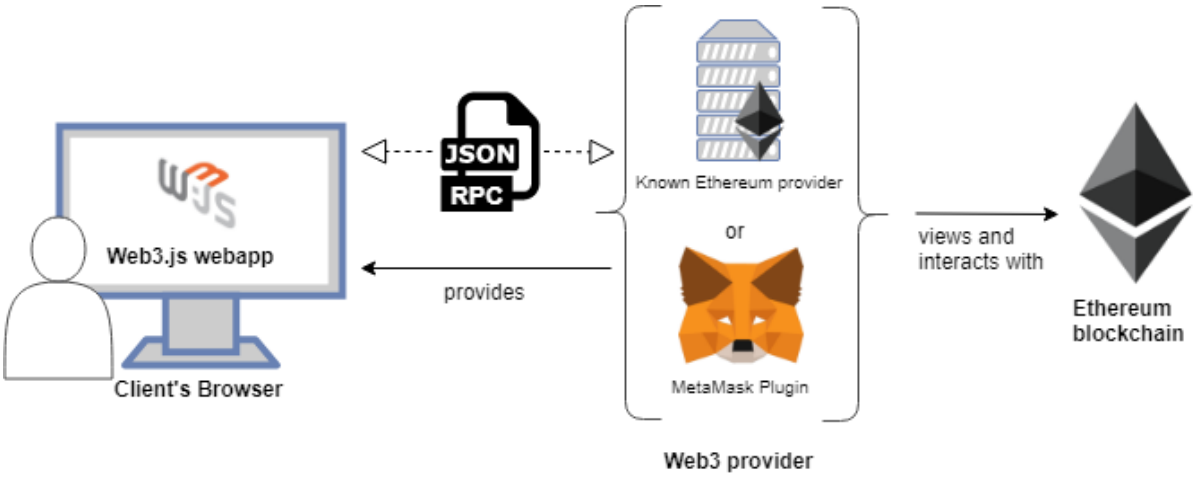


Figure III-14 Schéma d'accès vers la Blockchain depuis un navigateur web

III.6.3.7 Le système de fichiers interplanétaire (IPFS) :

IPFS est un système de partage de fichiers pouvant être exploité pour stocker et partager plus efficacement les fichiers volumineux. Il repose sur des hachages cryptographiques qui peuvent facilement être stockés dans la blockchain.

III.6.3.8 Amazon Web Service EC2 (ubuntu) :

Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Destiné aux développeurs, il est conçu pour faciliter l'accès aux ressources de cloud computing à l'échelle du Web. Il nous permet d'installer le (Hyperledger Fabric) sur le service cloud.

Hyperledger Fabric est une open source plateforme de technologie de grand livre distribué autorisée de niveau entreprise, conçue pour une utilisation dans des contextes d'entreprise, qui offre des capacités de différenciation clés par rapport à d'autres plates-formes populaires de grand livre distribué ou de blockchain.

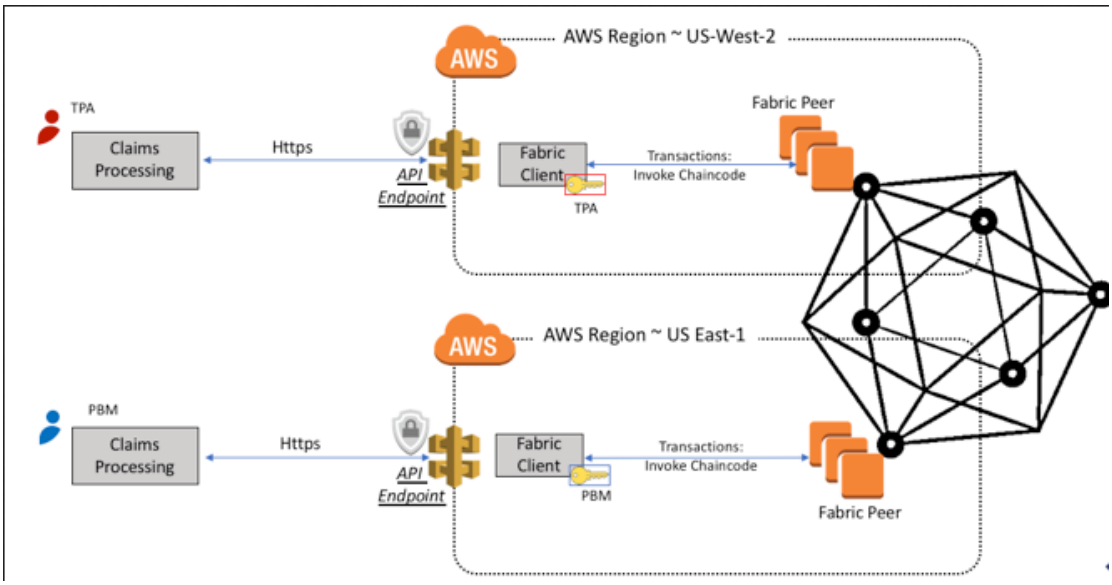


Figure III-15 le rôle de AWS dans le système Blockchain

III.7 Conclusion :

La création d'une application pour gérer la chaine logistique de l'industrie pharmaceutique reliée à un réseau de Blockchain demande plusieurs outils et plusieurs étapes, ils sont présentés dans ce chapitre.

Dans le chapitre suivant, nous avons procédé à exploiter ces étapes pour la réalisation et simulation d'un système Blockchain pour la traçabilité des produits pharmaceutiques dans une chaine logistiques.

Chapitre IV

Réalisation et Simulation d’un système Blockchain pour la traçabilité des produits pharmaceutiques dans une chaine logistiques :

IV.1 Introduction :

Pour réaliser notre système Blockchain de traçabilité des produits pharmaceutique on doit passer à travers certaines étapes importantes, notre système proposé est divisé en deux catégories :

- **Les participants impliqués dans le réseau de la chaîne logistique :** L'interface système utilisée est généralement le blockchain Ethereum, Pour le rendre facilement accessible, c'est l'utilisation d'une application décentralisée (DAPP); En général, nous pouvons dire un site Web à travers lequel les opérateurs peuvent accéder à un réseau de blockchain, dans chaque trajet ou chaque station l'opérateur saisie les données des médicaments dans le réseau Blockchain à l'aide d'un DApps. Par conséquent, l'utilisateur n'aura pas de problème de niveau de profondeur, car ils peuvent facilement ajouter la transaction et voir la transaction sur le réseau à l'aide d'une autorisation d'utilisateur appropriée. Cette transaction une fois ajoutée au réseau est maintenant immuable.
- **Utilisateur final (Client / patient) :** après le transfert dans la plateforme de Blockchain l'utilisateur (patient) peut accéder aux informations d'un médicament spécifique à l'aide de son smart phone depuis une application (Android/Ios) en scannant le QR code qui se trouve sur la boite de médicament, avec cette technique l'application va directement afficher toutes les informations bien détaillées de ce médicament.

IV.1.1 Les Diagramme UML de Système Blockchain :

IV.1.1.1 Diagramme de Cas d'utilisation :

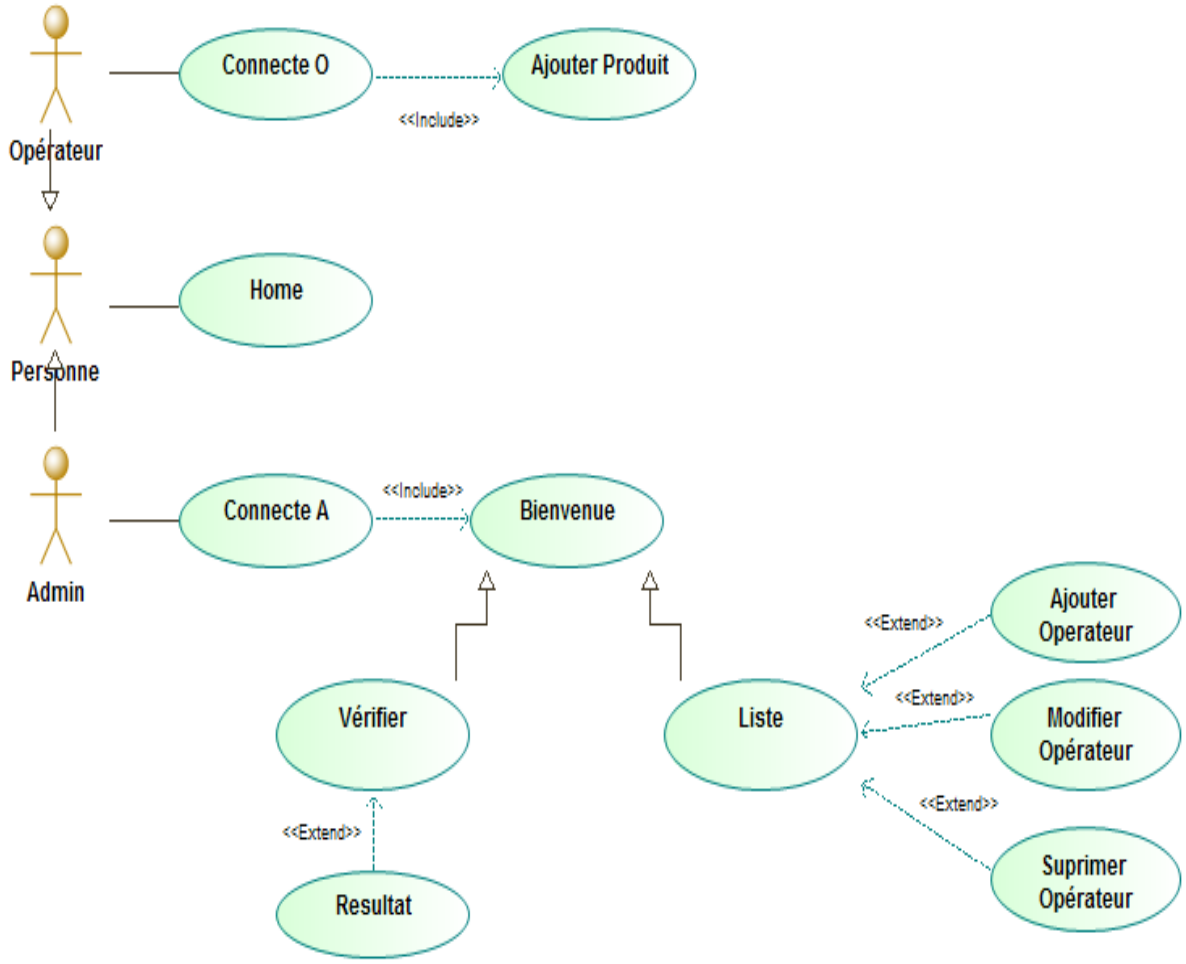


Figure IV-1 diagramme de cas d'utilisation de système Blockchain de traçabilité des produits pharmacetique

IV.1.1.2 Diagramme de séquencement :

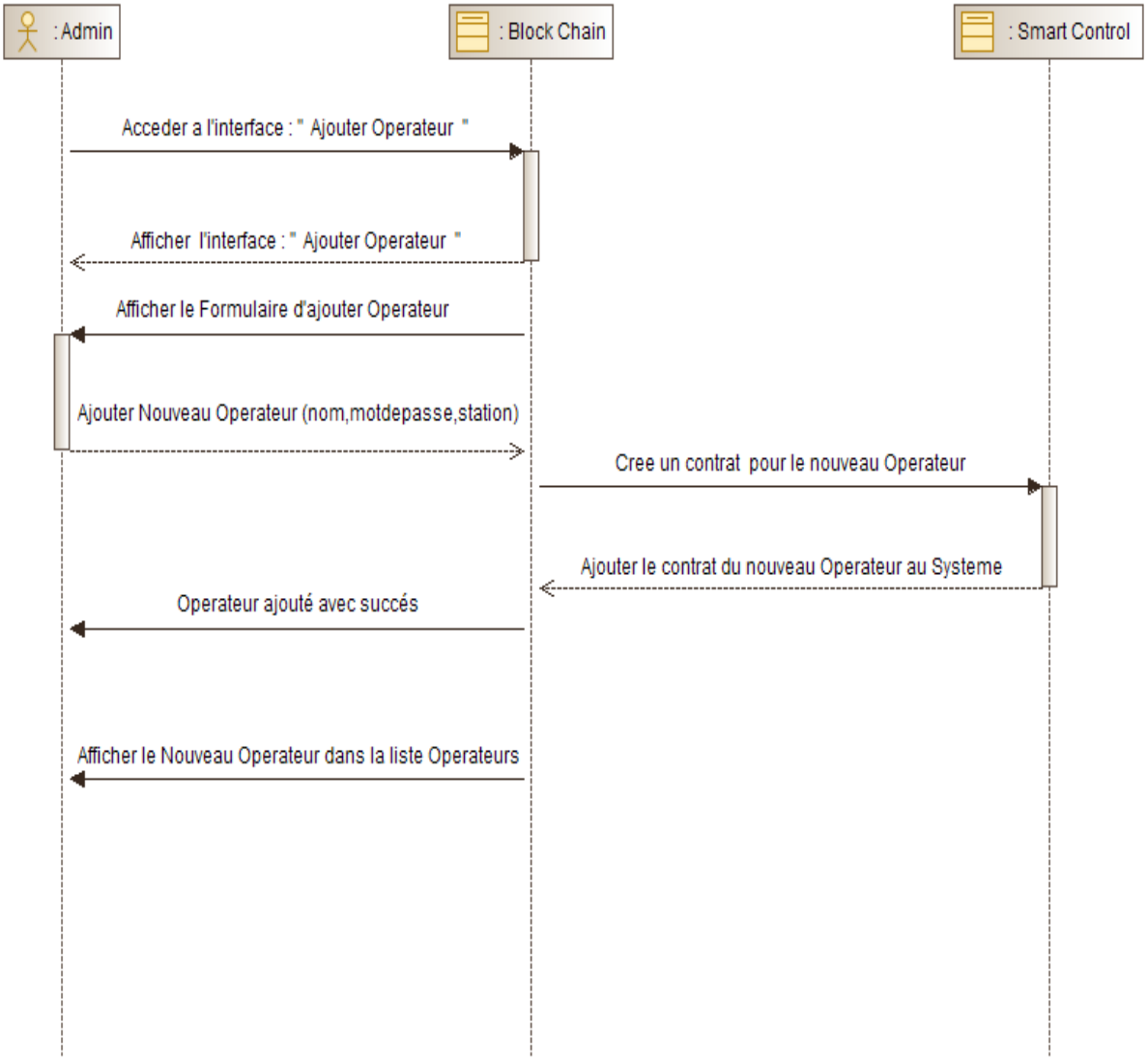


Figure IV-2 Diagramme de séquencement de DApp pour créer un compte d'opérateur

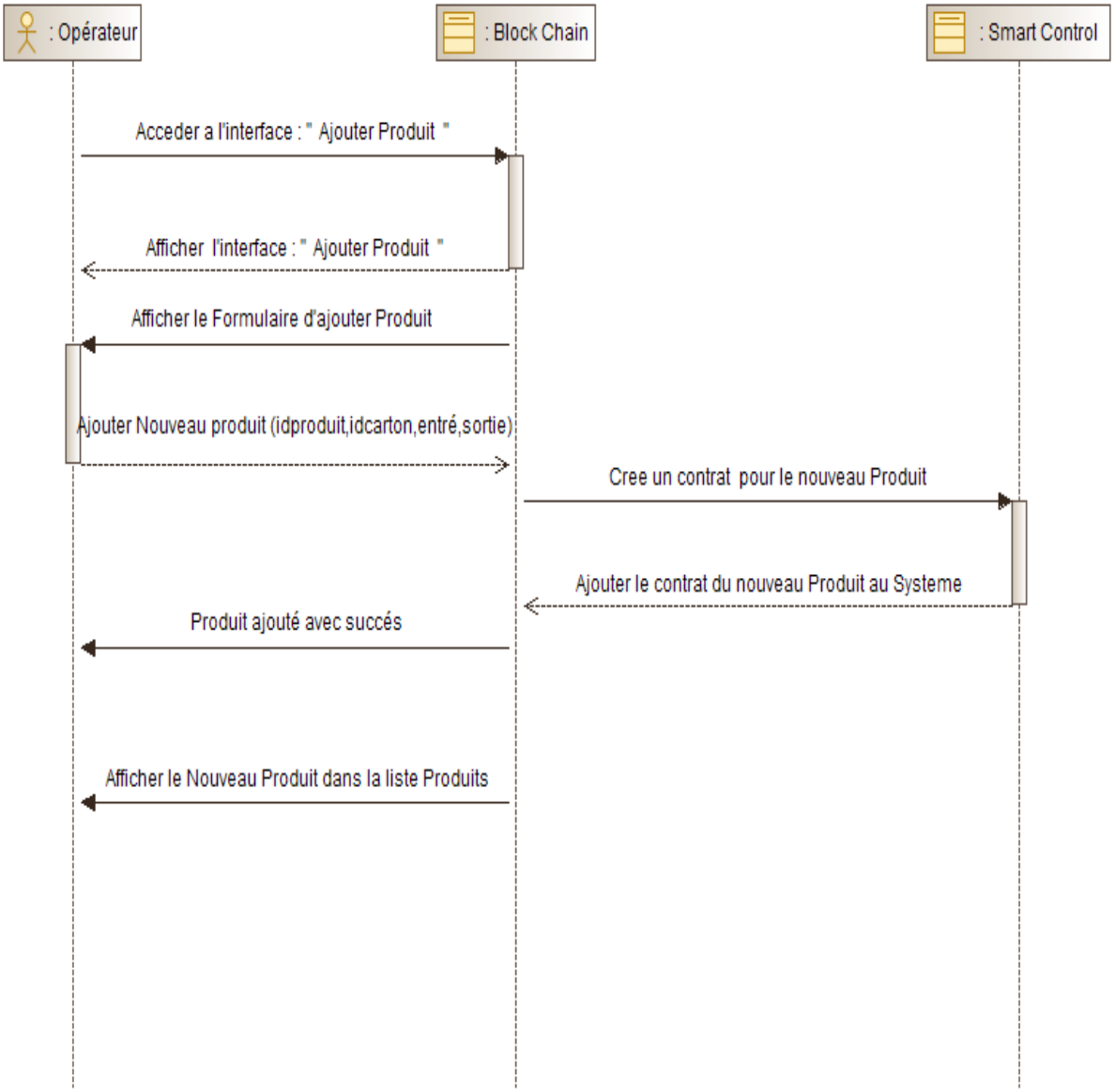


Figure IV-3 diagramme de séquencement l'opérateur pour ajouter un produit dans le DApp

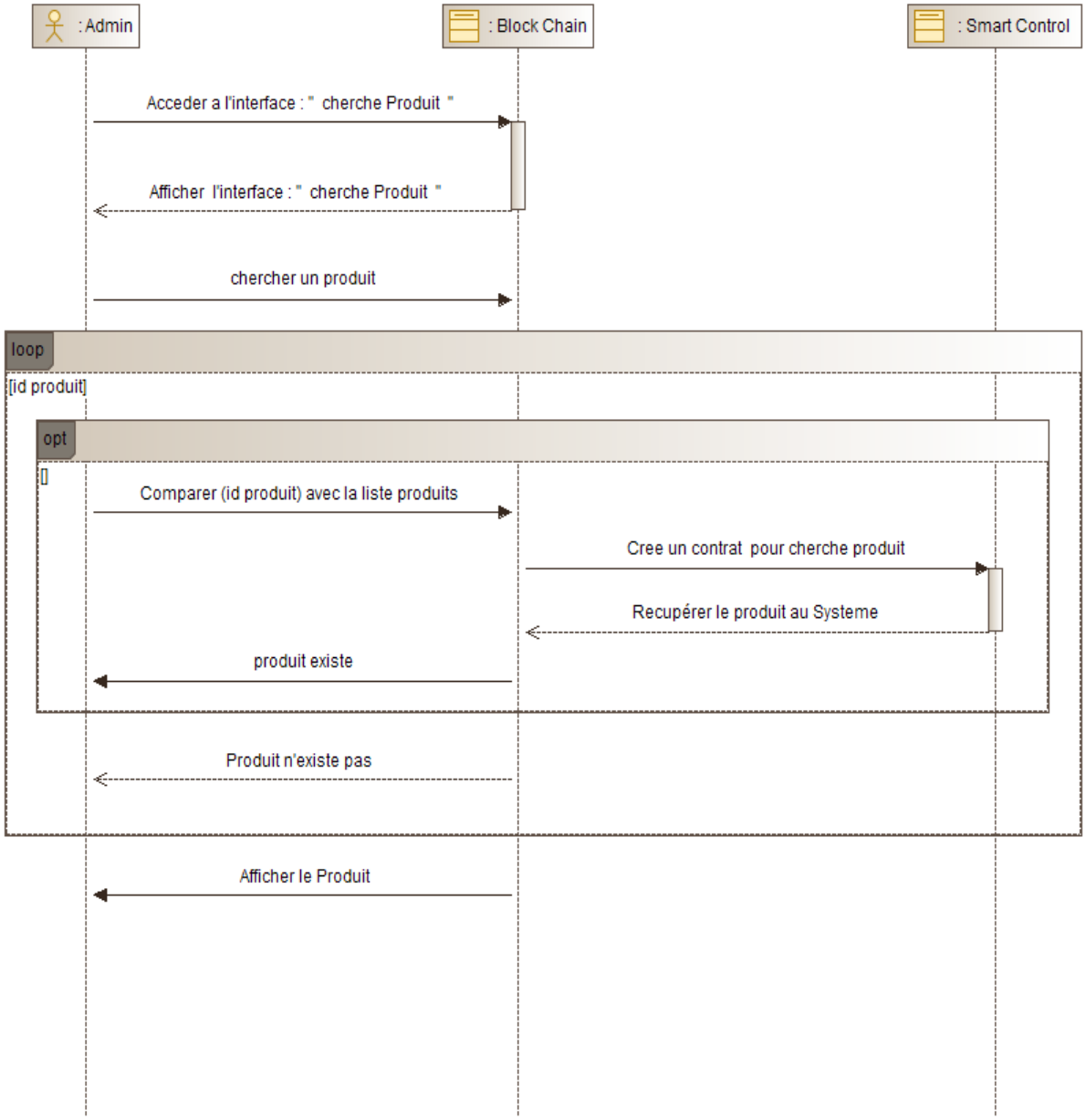


Figure IV-4 Diagramme de Séquencement pour vérifier la transaction des données dans Dapp

IV.1.1.3 Diagramme de Classe de Système Blockchain :

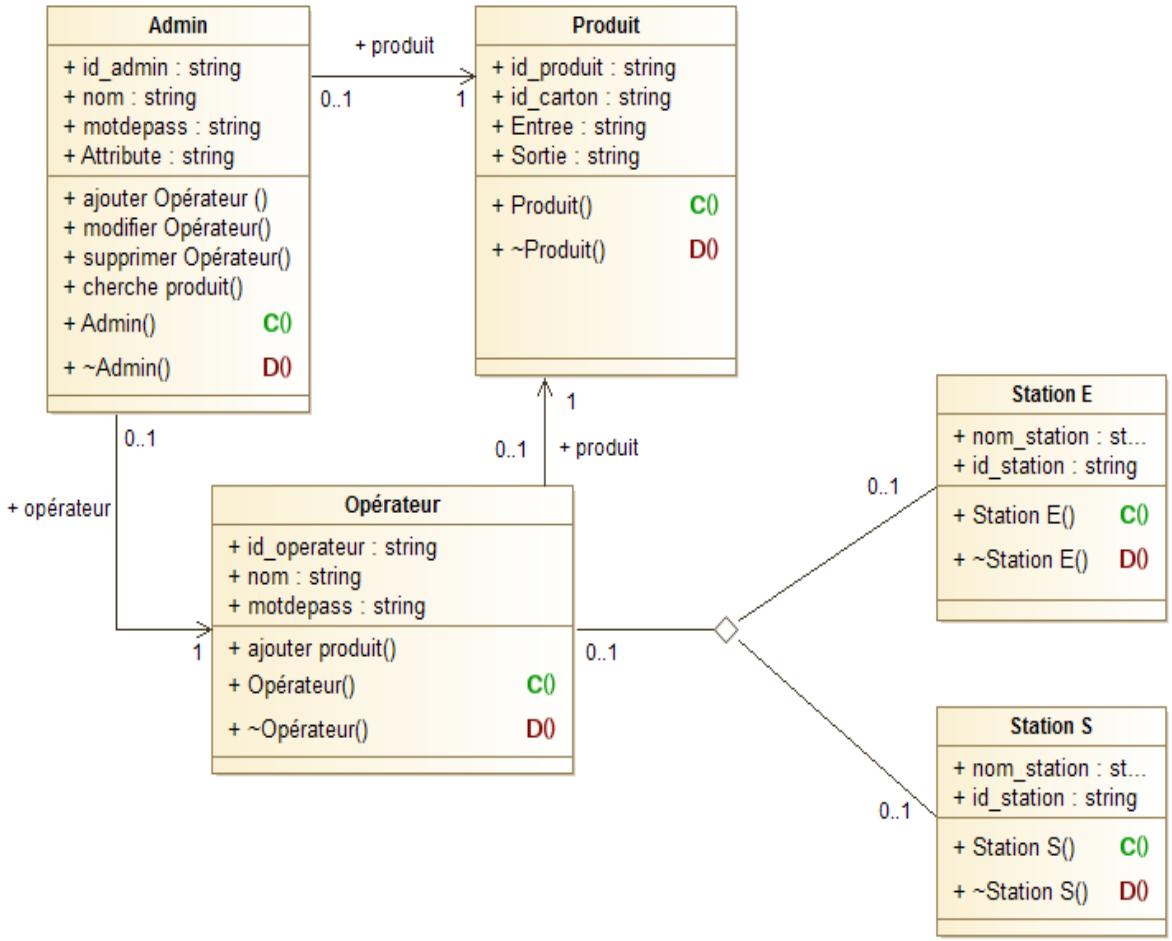


Figure IV-5 Diagramme de Classe de Système Blockchain

IV.1.2 Création d'une plateforme DApp (Front-End) :

IV.1.2.1 Programmation et Design de la plateforme :

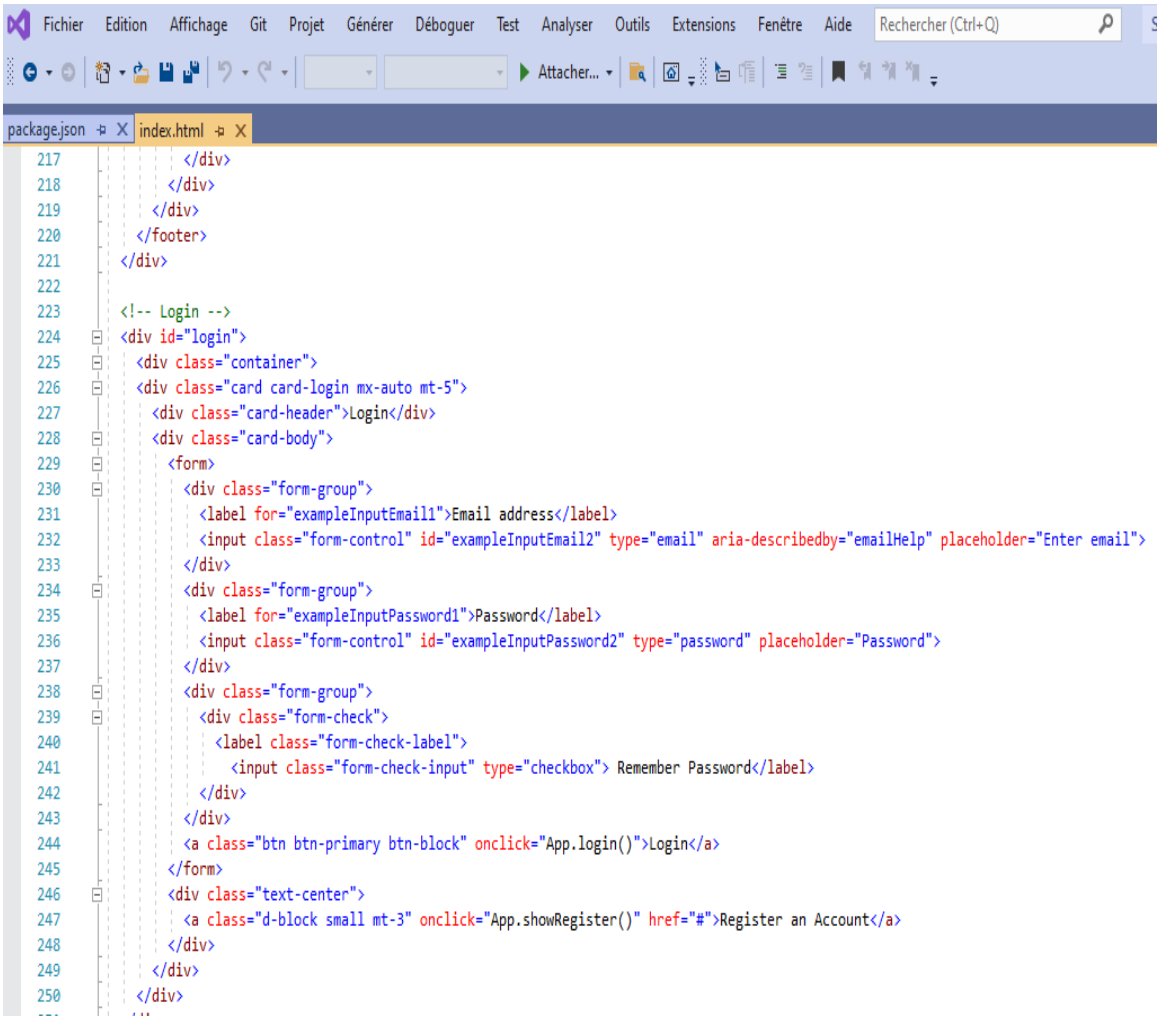


Figure IV-6 programmation de la plateforme DApp

- Nous avons utilisé Visual Studio pour programmer et concevoire notre plateforme DApp avec JAVASCRIPT HTML et CSS.
- En utilisant les bibliothèques et la fonction d'Angular js pour réaliser une page web moderne facile à utiliser.
- Nous avons structuré la plateforme à l'aide Node js pour qu'elle soit exécutable dans les navigateurs

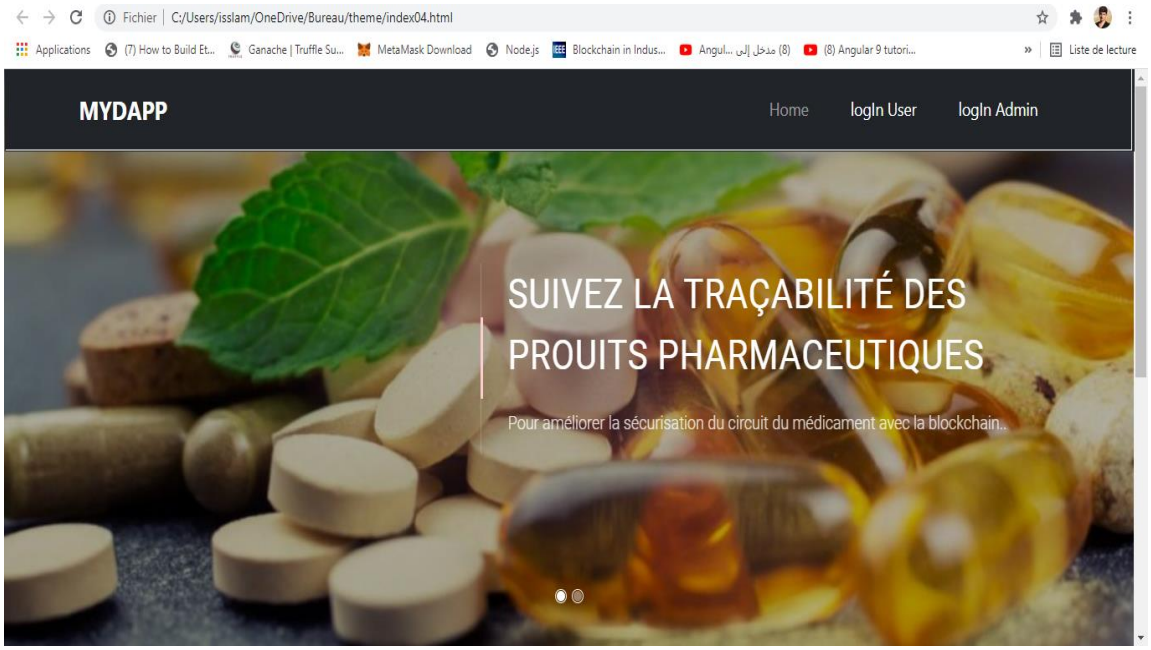


Figure IV-7 l'accueille (Home) de l'interface DApp

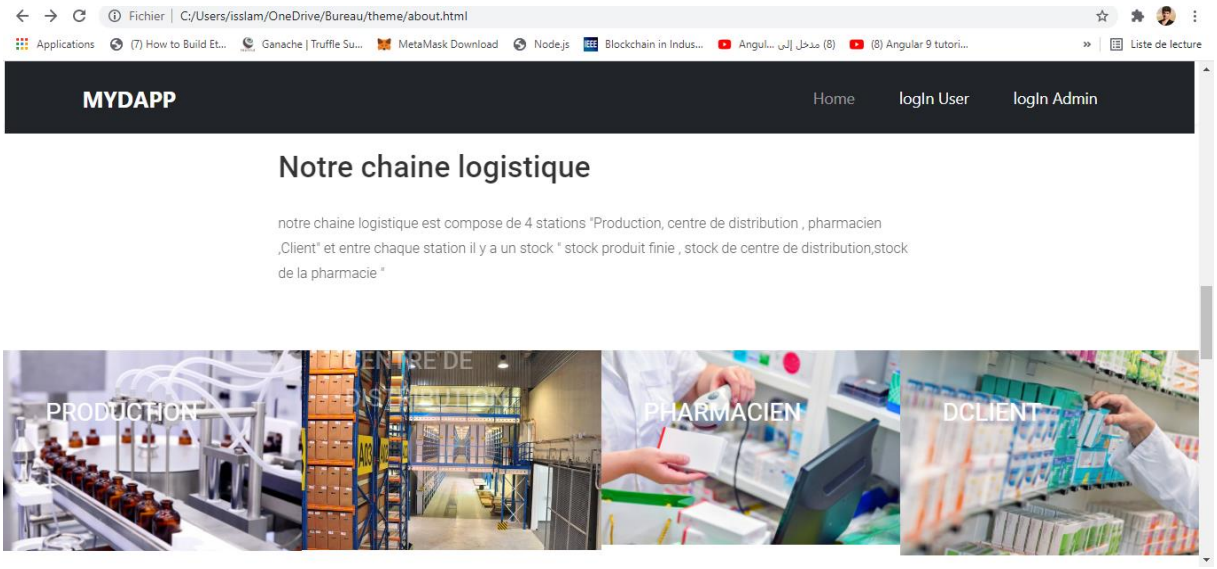


Figure IV-8 présentation de la chaine logistique dans le site web DApp

- Nous avons accédé à la plateforme DApp à l'aide de navigateur Google Dev pour exécuter et tester notre programme de Web page dans le Local Host.

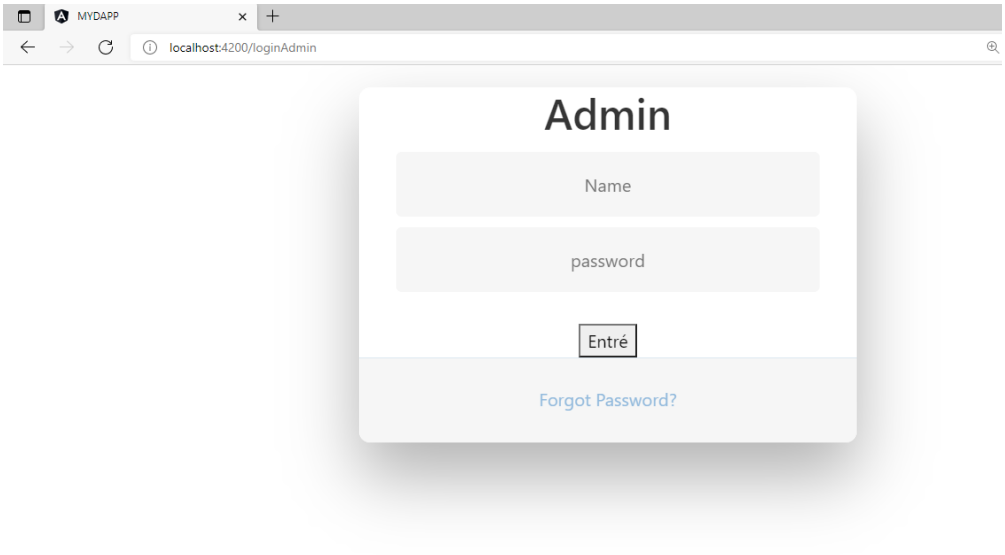


Figure IV-9 l'accès Admin responsable de la DApp pour gérer la plateforme

- Dans cette partie Admin, c'est le responsable de la DApp qui à le droit d'y accéder pour faire des modifications dans la page web.

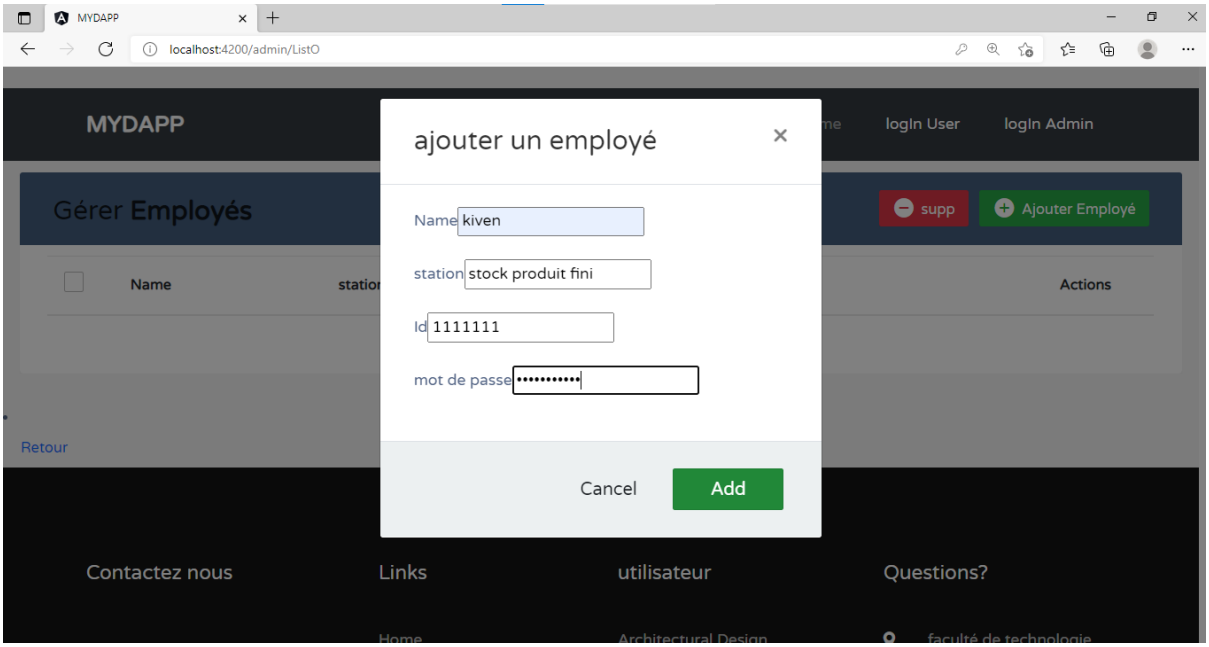


Figure IV-10 l'ajout d'opérateur pour accéder à la plateforme et gérer les données des médicaments

- Dans cette interface l'Admin peut ajouter ou supprimer le compte d'opérateur

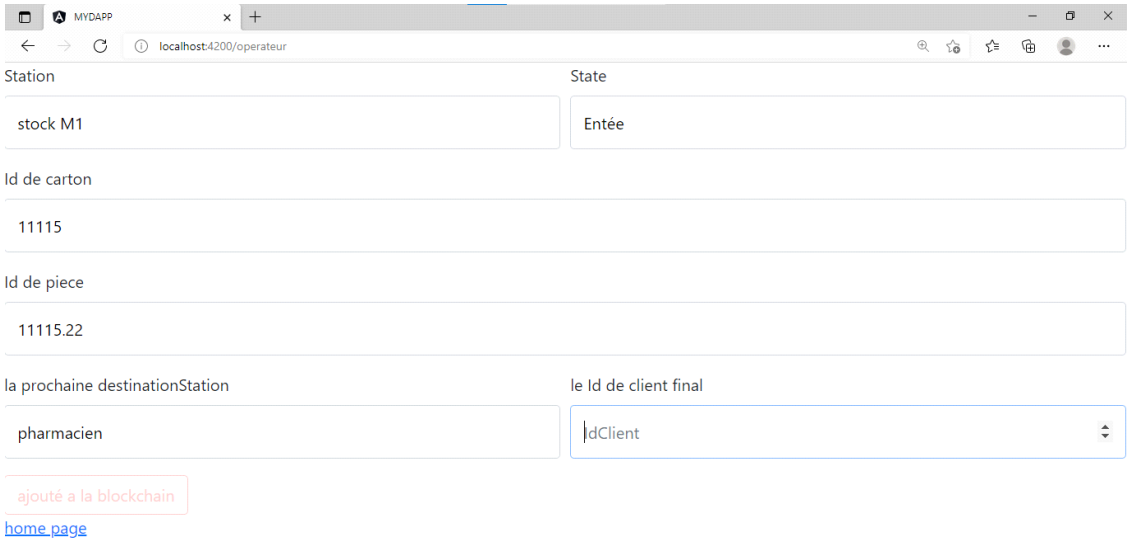


Figure IV-11 interface de DApp ou l'opérateur il doit insérer les données des produits pharmaceutiques

- Les données concernent les produits pharmaceutiques peuvent être saisie automatiquement en scannent le Code barre du produit.

IV.1.3 Programmation des contrats intelligents (Back-End) :

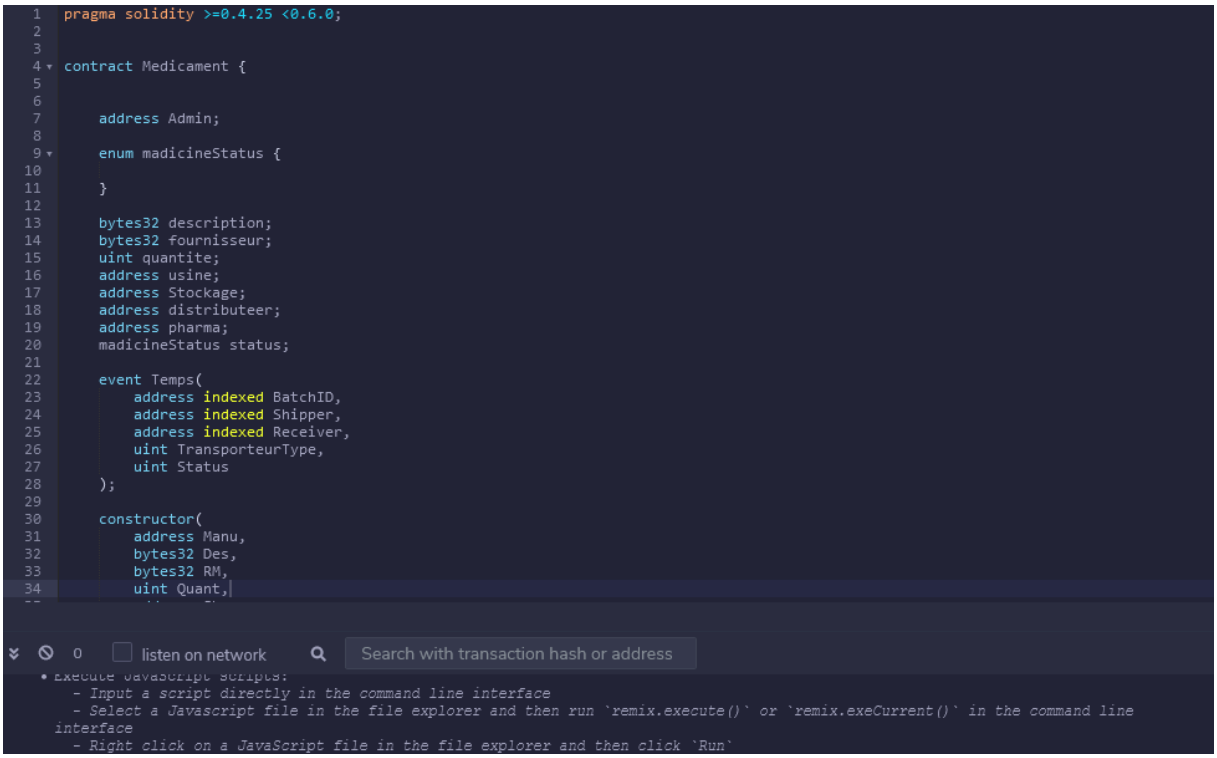


Figure IV-12 programmation de contrant intelligente sur Remix IDE

```
function initAdministrateur(
    string memory _idAdmin;
    string memory _nomeAdmin;
    string memory _passwordAdmin;
    )public{
        idAdmin =_idAdmin;
        nomeAdmin = _nomeAdmin;
        passwordAdmin = _passwordAdmin;
    }
```

Figure IV-13 Syntaxe de Contrat intelligente d'accès admin

```
contract Operateur {
    string idOperateur;
    string nomeOperateur;
    string passwordOperateur;
    string stationOperateur;
}
```

Figure IV-14 Syntaxe de Contrat intelligente de déclaration d'un nouvel opérateur

IV.1.4 Déploiement et l'exécution de Contrat intelligente du réseau Blockchain :

Après que le contrat intelligente est construite on doit la tester à l'aide de ganache pour voir les transactions et d'assurer qu'elle fonctionne bien, après on va connecter notre plateforme DApp avec le réseau de blockchain qui est générer par AWS EC2 a l'aide de web3 Js en utilisant l'extension Metamask.

Une fois que la connexion entre la plateforme DApp et le réseau blockchain est établie on déploie le contrat intelligent dans le réseau à travers le DApp, et on va simuler notre Blockchain de traçabilité.

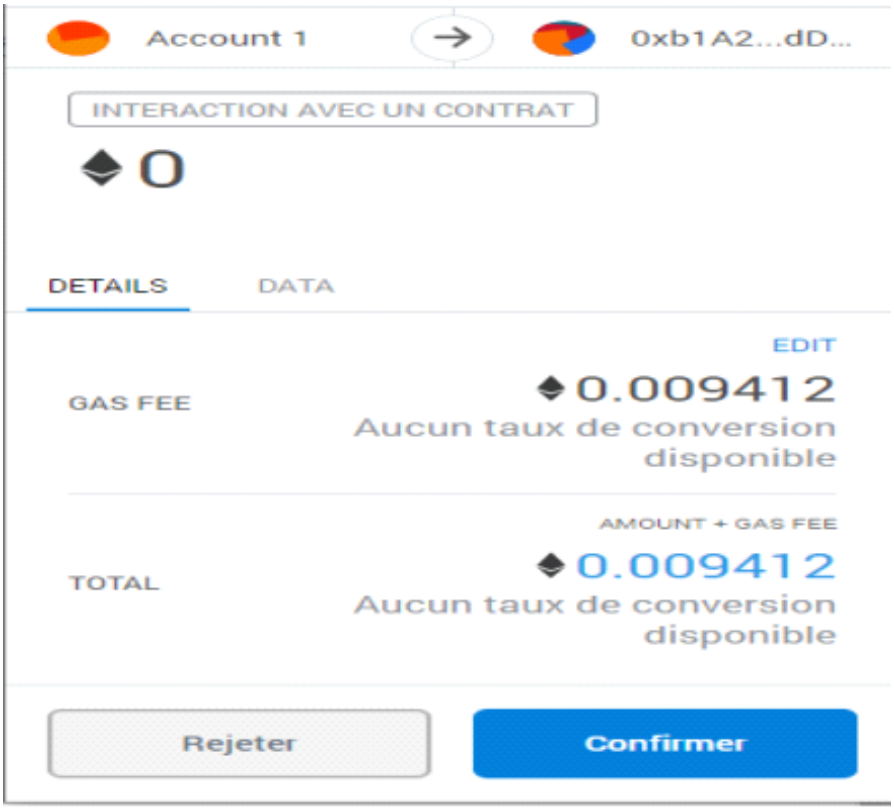


Figure IV-15 Metamask connect vers le réseau de Blockchain

```
1_deploy_contracts_Admin.js
===========================

   Replacing 'Administrateur'
   --------------------------
   > transaction hash:    0x9c853df3a56c6cd35c5dbf4dbef472debe25ef7283f00494a518
aff49714fdca
- Blocks: 0            Seconds: 0
   > Blocks: 0            Seconds: 0
   > contract address:    0x4D88Caf54625a68D537f820C4384364FDd33B0a8
   > block number:        14
   > block timestamp:     1600181167
   > account:             0xFBc9E8bED47ad67D9b25B200ca9e4188e986ed91
   > balance:             99.82102284
   > gas used:            1263838 (0x1348de)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.02527676 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.02527676 ETH
```

Figure IV-16 déploie de contrat intelligente de médicament dans le réseau Blckchain.

- Dès que le Contrat Intelligent est déployé un nouveau Block est créé au sein du réseau Blockchain.

- Ce contrat sera distribuer vers tous les nœuds de réseau Blockchain et elle sera enregistrer dans le livre distribuer.
- **IFPS** il va gérer automatiquement les données et le cordonnée du contrat dans le réseau des nœuds de Blockchain

IV.2 Inspection et vérification des résultats obtenue :

Après d'avoir vérifié qu'un nouveau Block est créé. On retourne vers la plateforme DApp web pour s'assurer que les données des médicaments sont-elles bien enregistrées et qu'elles vont s'afficher proprement.

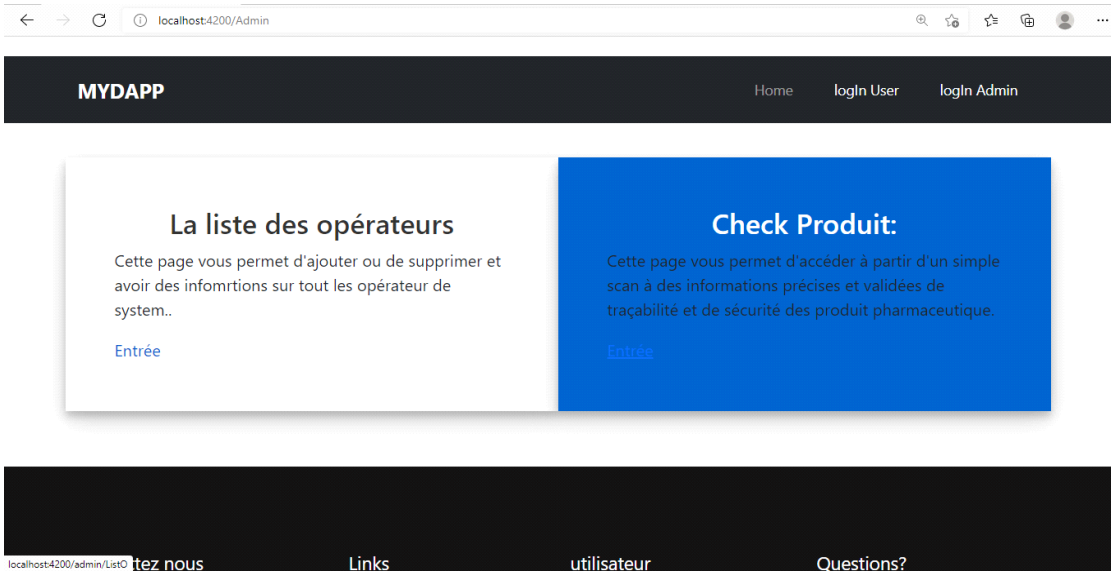


Figure IV-17 L'administrateur peut accéder à des informations précises sue la traçabilité de produit pharmaceutique

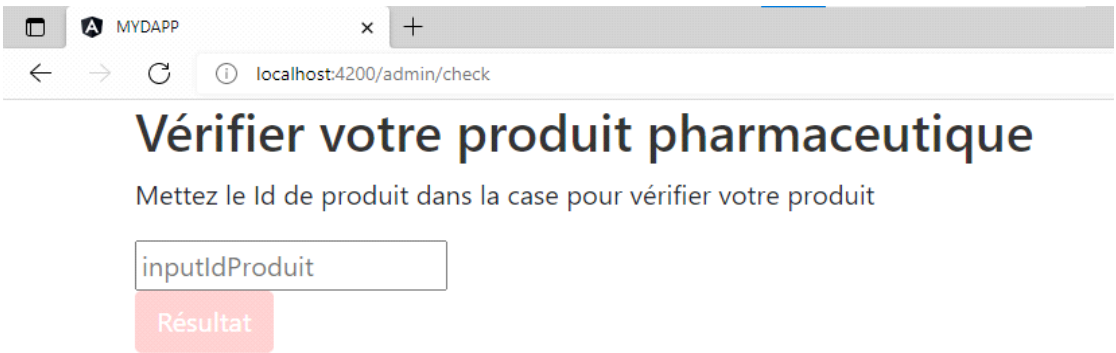


Figure IV-18 insérer l'identifient du produit pour chercher le produit pharmaceutique spécifique.

- Cette interface s'affichera pour l'Admin et aussi pour les utilisateurs de la DApp.

0

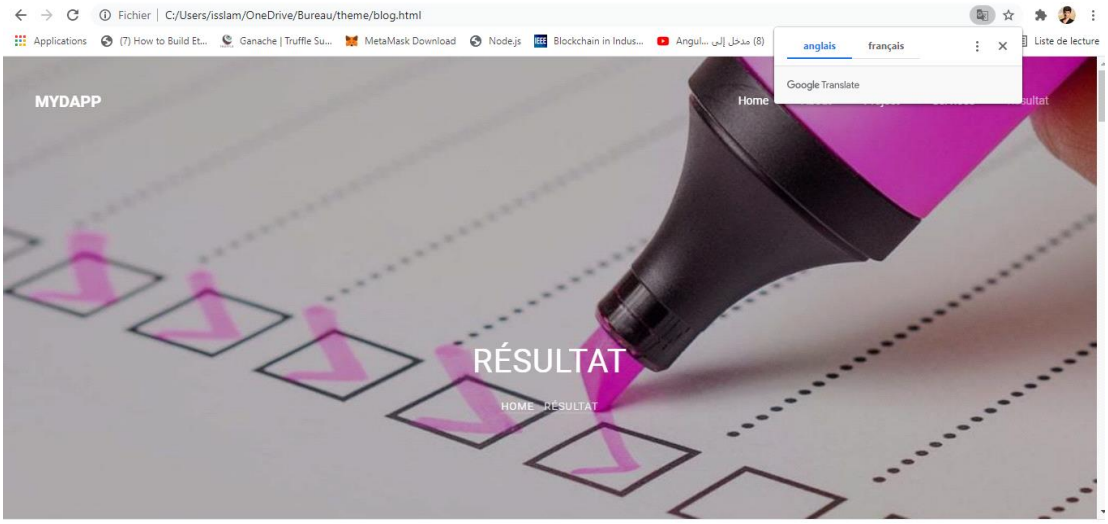


Figure IV-19 l'accès vers le résultat de recherche

- Quand l'identifient et saisie dans la case de recherche l'Admin ou l'utilisateur vont être orienté vers le résultat de recherche.

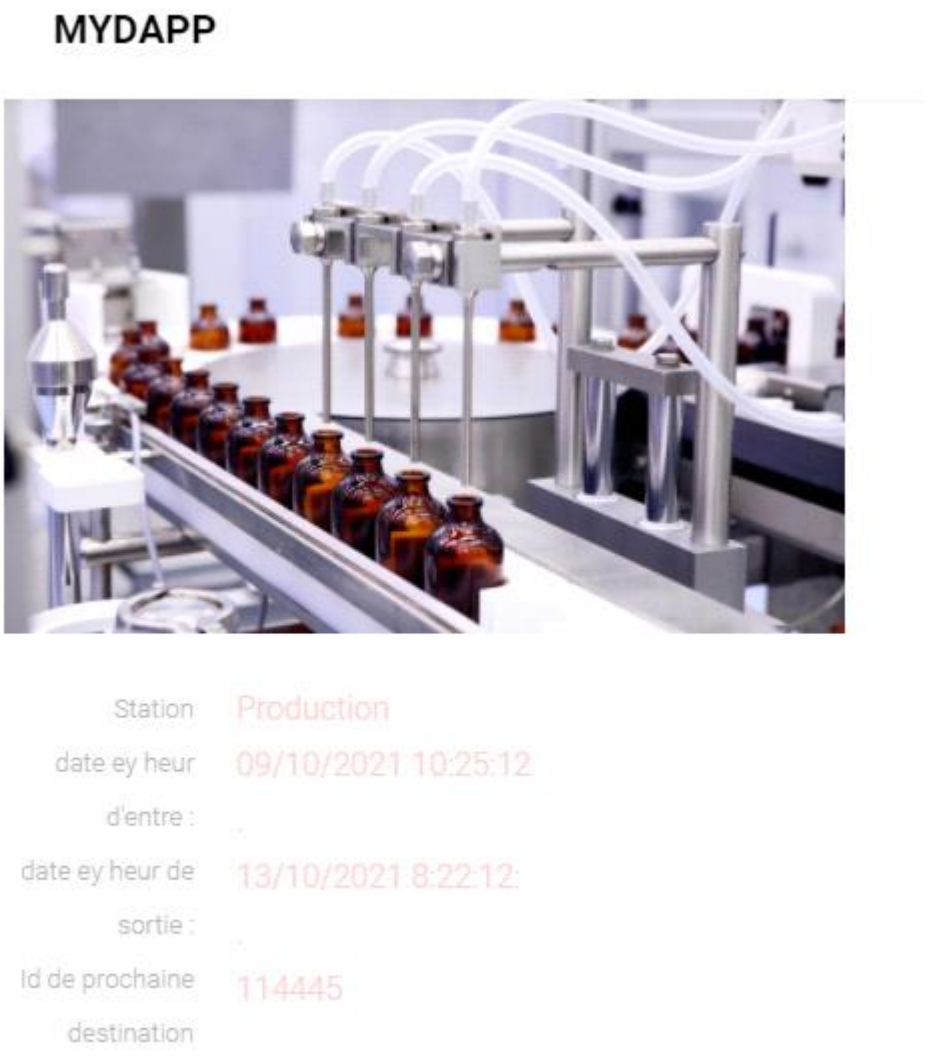


Figure IV-20 Exemple n°1 de résultat de recherche obtenu

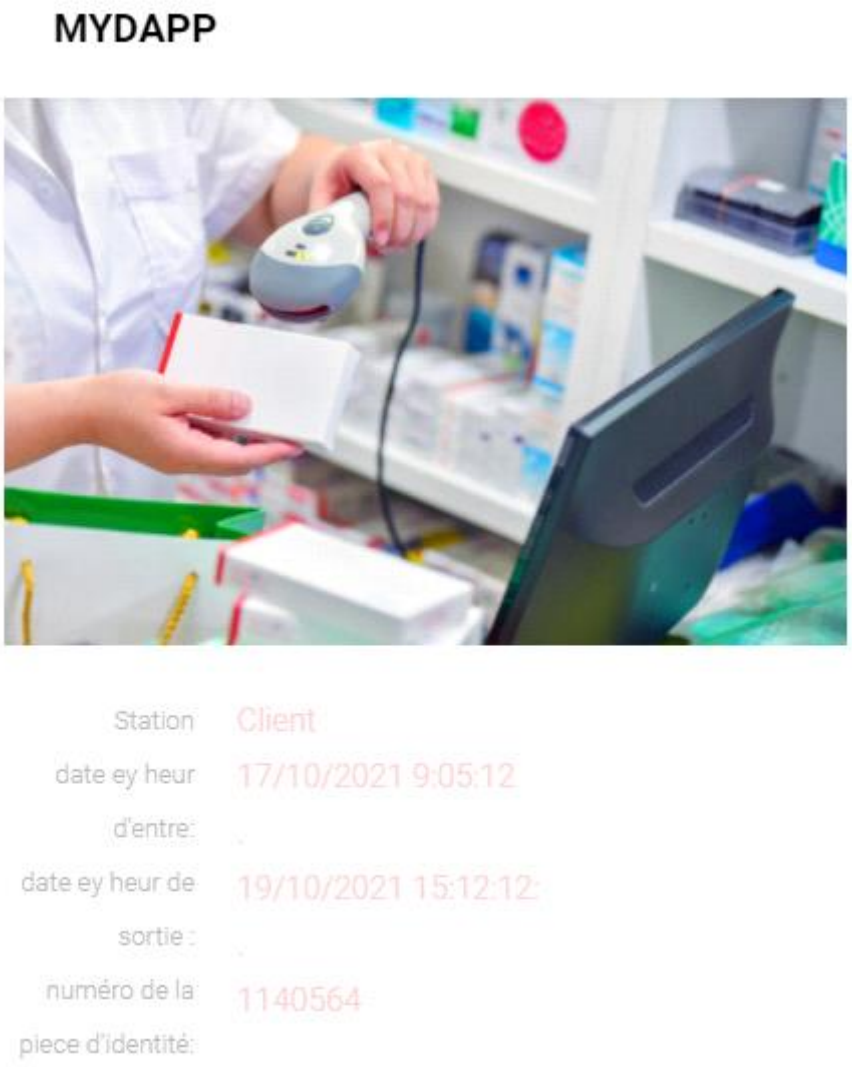


Figure IV-21 un exemple n°2 de résultat de recherche obtenu

IV.3 Analyse des résultats obtenue :

Après toutes ces démarches, Nous avons pu créer notre propre Blockchain pour la traçabilité et la transparence du produit pharmaceutique. Cette démarche a fonctionné proprement à l'aide de Hyperledger Fabric, elle a réduit les couts de transaction d'Ethereum entre les nœuds.

Avec cette Dapp on a la possibilité de créé on Application (Android/ Ios) pour rendre l'accès vers les informations des produits pharmaceutique plus rapide et plus facile, en scannant le codes de réponse rapide (QR code) qui se trouve sur la boite à l'aide d'une caméra d'un smartphone.

IV.4 Conclusion :

Nous avons développé et évalué une solution basée sur la blockchain pour la chaîne logistique de produits pharmaceutique afin de suivre et de tracer les médicaments de manière décentralisée. Plus précisément, notre solution proposée d'exploiter les fondamentaux cryptographiques sous-jacents à la technologie blockchain. Nous pouvons alors obtenir des journaux d'événements infalsifiables au sein de la chaîne logistique. nous avons utilisé des contrats intelligents au sein de la blockchain Ethereum pour réaliser un enregistrement automatisé des événements qui sont accessibles à toutes les parties prenantes participantes.

Conclusion générale

La blockchain est une nouvelle entrante dans l'écosystème technologique. Au début, elle était conçue pour des transactions d’argent pair à pair avec un objectif économique, après, elle est devenue une base de données décentralisée distribué dans tous les réseaux. Ce qu’elle a permet à la technologie Blockchain d’entrer dans des différents domaines et surtout dans le domaine industriel à l’aide de ses caractéristiques.

Cette technologie a permet de rendre la chaine logistique plus transparente pour mieux protéger et sécuriser des différents produits comme on l’a vue avec les produits pharmaceutiques.

Bien que de nombreuses fonctionnalités aient été implémentées et discutées dans notre travail, certains aspects restent encore en suspens. Par exemple, la prévention du clonage des codes de réponse rapide (QR) et le suivi en direct avec des appareils compatibles IoT sont laissés aux perspectives futures de ce projet. L'intégration du code Quick Response (QR) avec la blockchain peut être très pratique et utile pour que les choses se passent plus facilement.

D'autres DLT (Distributed Ledger Technology) comme IOTA peuvent être utiles pour la chaîne logistique avec davantage d'appareils compatibles IoT pour rendre le processus fluide et plus rapide. Un autre avantage principal d'un système comme celui-ci pourrait se trouver dans chaque secteur de la chaîne logistique, à l'exception de la pharmacie.

Essayer de combiner Combinées, l'intelligence artificielle et la blockchain conduiront à une révolution à la fois technique et économique, notamment en termes de chaîne logistique.

Les Références :

[1] Rhonda R Lummus and Robert J Vokurka. Defining Supply Chain Management: a HistoricalPerspective and Practical Guidelines. Industrial Management & Data Systems, 99(1):11 – 17, 2014.

[2] Ram P HarrisonGaneshan and Terry. Introduction to Supply Chain Management. Supply Chain ManagementAn International Journal, 47(July):3–4, 1995. ISSN 1745493X. doi:10.1111/j.1745-493X.2011.03231.x. URLhttp://lcm.csa.iisc.ernet.in/scm/supply_chain_intro.html.ISSN 10983015. doi:10.1108/02635579910243851. Citerdans pp. 1 and 2.

[3] Ronald H. Ballou. The Evolution and Future of Logistics and Supply Chain Management. EuropeanBusiness Review, 19(4):332–348, 2007. ISSN 0955-534X. doi: 10.1108/09555340710760152.

[4] Mamun Habib. Supply chain management (scm): Theory and evolution. In Mamun Habib, editor, Supply Chain Management, chapter 1. IntechOpen, Rijeka, 2011. doi: 10.5772/24573. URLhttps://doi.org/10.5772/24573. Citerdans p. 2.

URL : http://www.emeraldinsight.com/doi/10.1108/09555340710760152. citer dans p. 2.

[5] Alan Punter. Supply Chain Failures - A Study of the Nature, Causes and Complexity of SupplyChain Disruptions. Airmic Technical, pages 1–52, 2013Citer dans p. 3.

[6] Michael Prokle. Theory and Practice of Supply Chain Synchronization. Doctoral Dissertations, 2017.

[7] Kari Korpela, Jukka Hallikas, and Tomi Dahlberg. Digital Supply Chain Transformation towardBlockchain Integration. pages 4182–4191, 2017. doi: 10.24251/HICSS.2017.506. URL http://hdl.handle.net/10125/41666.

[8] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Www.Bitcoin.Org,page 9, 2008.ISSN 09254560. doi: 10.1007/s10838-008-9062-0. URLhttps://bitcoin.org/bitcoin.pdf.

[9] Stuart Haber and W Scott Stornetta. How to time-stamp a digital document. Journal of Cryptology,3(2):99–111, jan 1991. ISSN 1432-1378. doi: 10.1007/BF00196791. URL https://doi.org/10.1007/BF00196791. Citer dans p. 4.

[10] Dave Bayer, Stuart Haber, and W. Scott Stornetta. Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences II, pages 329–334, 1992. doi: 10.1007/978-1-4613-9323-8_24. URLhttp://link.springer.com/10.1007/978-1-4613-9323-8{_}24. Citerdans p. 4.

[11] Filiz Isik. Complexity in Supply Chains: A New Approach to Quantitative Measurement of theSupply-Chain-Complexity. Supply Chain Management, pages 417—-432, 2011. Citerdans p. 4.

[12] Richard Wilding. The Supply Chain Complexity Triangle: Uncertainty Generation in the SupplyChain. International Journal of Physical Distribution & Logistics Management, 28(8):599–616, 1998. ISSN0960-0035. doi: 10.1108/09600039810247524. URL http://www.emeraldinsight.com/doi/10.1108/09600039810247524. Citerdans p. 5.

[13] : Blockchain, une révolution à venir pour le secteur de l'industrie ? https://www.1life.fr/blog/blockchain-industrie/

[14] La Blockchain : la garantie d'une traçabilité transparente https://www.bearingpoint.com/fr-fr/blogs/blog-digital-strategy/la-blockchain-la-garantie-dune-tra%C3%A7abilit%C3%A9-transparente/#_ftn1

[15] liver: Blockchain and Supply Chain Logistics.Chapitre 3

[16] Fourth Industrial Revolution https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

[17] What is Industry 4.0—the Industrial Internet of Things (IIoT)? https://www.epicor.com/en/resource-center/articles/what-is-industry-4-0/

[18] Applying Blockchain in Industry 4.0 Application https://ieeexplore.ieee.org/abstract/document/8666558 figure 10
https://www.apave.com/industrie-40-reussir-son-projet-et-maitriser-tous-les-risques

[19]articl Blockchain-enabled technology: the emerging technology set to reshape and decentralise many industries

https://www.inderscienceonline.com/doi/abs/10.1504/IJADS.2019.102642
[20] M. Mainelli and C. von Gunten, Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance, London, U.K, Dec. 2014, [online] Available: http://archive.longfinance.net/images/Chain_Of_A_Lifetime_December2014.pdf.

[21] Blockchain in Industries
https://ieeexplore.ieee.org/abstract/document/8662573

[22] R. H. Lasseter and P. Paigi, "Microgrid: A conceptual solution", Proc. IEEE 35th Annu. Power Electron. Specialists Conf. (PESC), vol. 6, pp. 4285-4290, Jun. 2004.

[23] A. Cohn, T. West and C. Parker, "Smart after all: Blockchain smart contracts parametric insurance and smart energy grids", Georgetown Law Technol. Rev., vol. 1, no. 2, pp. 273-304, 2017.

[24] E. Münsing, J. Mather and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks", Proc. IEEE Conf. Control Technol. Appl. (CCTA), pp. 2164-2171, Aug. 2017.

[25] . A. Cohn, T. West and C. Parker, "Smart after all: Blockchain smart contracts parametric insurance and smart energy grids", Georgetown Law Technol. Rev., vol. 1, no. 2, pp. 273-304, 2017.

[26] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid", Appl. Energy, vol. 210, pp. 870-880, Jan. 2018.

[27] E. R. Sanseverino, M. L. Di Silvestre, P. Gallo, G. Zizzo and M. Ippolito, "The blockchain in microgrids for transacting energy and attributing losses", Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), pp. 925-930, Jun. 2017.

[28] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures blockchain and anonymous messaging streams", IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 840-852, Sep./Oct. 2018.

[29] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids", Sensors, vol. 18, no. 1, pp. 162, 2018. http://www.agro-media.fr/actualite/carrefour, illustration BearingPoint -Figure 12 Chris Martin, How Blockchain Is Threatening to Kill the Traditional Utility, Ljubljana Slovenia Juin 2018. CIRED

[30] Médicaments contrefaits : La police saisie plus de 650000 comprimés, journal Sante news, source : http://www.santenews-dz.com/medicaments-contrefaits-police-saisie-plus-de-650000-comprimes/