MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et d'Informatique

Département de Mathématiques et informatique

Filière : Informatique

MEMOIRE DE FIN D'ETUDES

Pour l'Obtention du Diplôme de Master en Informatique

Option : **Ingénierie des Systèmes d'Information**

Présenté par :

GUANI Amina

HAMMOU Hadja

THEME :

La Blockchain et son utilisation dans les chaînes d'approvisionnement

Soutenu le : 19/06/2021

Devant le jury composé de :

HAMAMI Dalila	MCB	Université de Mostaganem	Président
BESSAOUD Karim	MCB	Université de Mostaganem	Examinateur
MIROUD Mohammed El Mustapha	MAA	Université de Mostaganem	Encadrant

Année Universitaire 2020-2021

Résumé

L'objectif de notre projet de fin d'étude était de concevoir et d'implémenter une application décentralisée qui résout les failles de sécurité des applications centralisées, et supprime les tiers de confiance. C'est pourquoi nous avons utilisé le concept de blockchain et nous l'avons appliqué à l'expédition des produits par des transporteurs d'une entreprise, afin de démontrer l'intérêt d'utiliser cette technologie dont le premier avantage réside dans sa facilité de traçabilité.

Au cours de ce projet de fin d'études de master en informatique, nous avons effectué une étude approfondie de la blockchain, des smart contrat ainsi que de la plateforme Ethereum. Nous avons proposé une solution à la problématique de la traçabilité des produits expédiés tout au long de la chaîne d'approvisionnement, en temps réel tout en supprimant l'administration par autorité centrale, ainsi que les documents papiers. Nous avons proposé une solution basée sur la technologie de la blockchain en utilisant les smart contracts afin de développer une application décentralisée d'expédition des produits.

Mots-clés :

Blockchain, supply chain, chaîne d'approvisionnement, Bitcoin, cryptographie, cryptomonnaies, consensus, Etherum, Smart contracts, Solidity.

Abstract

The objective of this work was to study the blockchain and crypto currency technologies mechanics. We have first explained Bitcoin, blockchain and cryptocurrencies mechanics. Next, we studied the supply chain management problems, and how it can be solved using blockchain technology. Finally, we introduced and implemented our own blockchain solution for handling traceability problems on the supply chain.

Keywords :

Blockchain, supply chain, chaîne d'approvisionnement, Bitcoin, cryptographie, cryptomonnaies, consensus, Etherum, Smart contracts, Solidity.

Dédicaces

Nous dédions ce projet

A nos Parents

Pour tous les sacrifices consentis. Pour tous les encouragements qu'ils ont su nous insuffler aux moments difficiles. Qu'ils trouvent dans ce mémoire, le témoignage de nos vives gratitudes et de notre grande reconnaissance, pour l'énergie qu'ils ont su implanter en nous à tous les instants de nos études.

A tous nos amis

Que ce travail vous soit le témoignage de notre profonde affection.

A notre encadreur Mr MIROUD Mohammed El Mustapha

Pour sa générosité et ses précieuses directives qu'il n'a cessé de nous prodiguer.

A toute nos famille « GUANI » et « HAMMOU », a nos frères et sœurs

A tous ceux que nous aimons.

A tous nos amis, nos camarades, et à ceux qui sont en train de lire ces lignes. Pour leur appui moral et leurs conseils.

Remerciement

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour achever ce travail.

Nous adressons nos sincères remerciements à notre encadrant, « Mr MIROUD Mohammed El Mustapha », pour sa patience, sa disponibilité, son encouragement et surtout ses conseils et ses critiques qui ont guidé nos réflexions et répondu à nos questions durant ce travail.

Nous désirons aussi remercier tous les enseignants de la faculté des sciences exactes et de l'informatique de l'université de Mostaganem, pour leur générosité et la grande patience dont ils ont su faire preuve, malgré leurs charges académiques et professionnelles.

Un grand merci à nos très chers parents, qui ont toujours été là pour nous. Nous remercions nos frères, sœurs et toutes les personnes que nous aimons, pour leurs encouragements.

Nous voudrions aussi exprimer notre reconnaissance envers les amis et camarades de promotion qui nous ont apporté leur soutien moral et intellectuel tout au long de notre démarche.

Afin de n'oublier personne, nos vifs remerciements s'adressent à tous ceux qui nous ont aidés à la réalisation de ce modeste mémoire.

Liste des figures

Figure 1-Structure de données représentant un jeton dans la cryptomonnaie GoofyCoin 4
Figure 2-Structure représentant une transaction de transfert de jeton depuis Goofy vers Alice 5
Figure 3-Structure représentant une transaction pour payer Bob 6
Figure 4-Attaque à double dépense 7
Figure 5-ScroogeCoin Blockchain 8
Figure 6-Détection de modification dans la blockchain de Scrooge 9
Figure 7-Transaction Bitcoin 17
Figure 8-Structure d'un bloc Bitcoin 17
Figure 9-Transaction Coinbase 18
Figure 10-Diagramme de Contexte 34
Figure 11-Diagramme de cas d'utilisation global 35
Figure 12-Diagramme de séquence d'Authentification 40
Figure 13-Diagramme de séquence pour ajouter produit/transporteur 41
Figure 14-Diagramme de séquence pour l'affectation du transporteur à un produit 42
Figure 15-Diagramme de classe 43
Figure 16-La fenêtre « Page d'Accueil » 46
Figure 17-La fenêtre d'interface « Authentification » 47
Figure 18-L'interface « accueil Expéditeur » 48
Figure 19-Interface d'Ajout des transporteurs 49
Figure 20-fenêtre d'interface d'Ajout des produits 50
Figure 21-Fenêtre d'interface d'affectation d'un transporteur à un produit 51
Figure 22-Accueil Transporteur/Client 51
Figure 23-Fenêtre liste des produits 52
Figure 24-Fenêtre liste des transporteurs 52
Figure 25-L'état du transport de produits 53
Figure 26-les blocs de Ganache 54

Liste des tableaux

Tableau 1-Description du cas "Authentification" 36
Tableau 2-Description du cas "Ajouter un Transporteur / Ajouter un Produit " 37
Tableau 3-Description du cas "Affecter un Transporteur à un Produit " 38
Tableau 4-Description du cas "Consulter l'état de transport de produits " 39
Tableau 5-Description du cas « Consulter liste des transports / produits » 39

Table des matières

Introduction Générale 1

Chapitre 1 Introduction aux crypto monnaies et à la blockchain 3

1.1 Introduction 3

1.2 Introduction à Bitcoin et aux cryptomonnaies 3

1.2.1 L'utilisation des clés publiques en tant qu'identité dans le réseau bitcoin 3

1.2.2 Exemple simple de crypto monnaie 4

1.2.2.1 GoofyCoin 4

1.2.2.2 ScroogeCoin 8

1.3 Comment Bitcoin parvient à la décentralisation 11

1.3.1 Décentralisation contre centralisation 11

1.3.1.1 Aspects de la décentralisation dans Bitcoin 12

1.3.1.2 Aspects de Bitcoin qui sont décentralisé 12

1.3.1.3 Aspects de Bitcoin qui sont centralisés 12

1.3.2 Consensus distribué 13

1.3.2.1 Définition d'un protocole de consensus 13

1.3.2.2 Comment le consensus fonctionne dans Bitcoin 14

1.3.3 Consensus sans identité 14

1.3.4 Incitations et preuve de travail 15

1.3.4.1 Les incitations 15

1.3.4.2 Preuve de travail (proof of work) PoW 16

1.4 Scripts Bitcoin 16

1.5 Types de blockchain 18

1.5.1 Blockchain publique 19

1.5.2 Blockchain privée 19

1.5.3 Blockchain de consortium 19

1.5.4 Blockchain hybride 20
1.6 Conclusion 20
Chapitre 2 Blockchain et supply chain 21
2.1 Introduction 21
2.2 Supply Chain “ Chaîne d’approvisionnement ” 21
2.3 Défis actuels de la supply chain : 22
2.4 Comment la blockchain peut apporter des solutions aux problèmes rencontrés dans le domaine de la supply chain 23
2.5 Application de la blockchain dans Les chaînes d’approvisionnement « Supply Chain » 23
2.5.1 Applications de la blockchain dans la chaîne d'approvisionnement alimentaire 24
2.5.1.1 Partage d'informations pour la traçabilité et la transparence 25
2.5.1.2 Améliorer la qualité et éviter les rappels 26
2.5.1.3 Cas réel d'utilisation de la chaîne alimentaire 26
2.5.2 Applications de la blockchain dans la chaîne d'approvisionnement des soins de santé 27
2.5.3 Applications de la blockchain et opportunités futures dans les transports 28
2.5.3.1 Monétisation des données 28
2.5.3.2 Traitement efficace des réclamations d'assurance 28
2.5.3.3 Suivi de l'historique des performances de la flotte et des véhicules 29
2.5.3.4 Normes de données communes 29
2.5.4 Applications de la blockchain dans l'approvisionnement au détail 29
2.5.4.1 Visibilité de bout en bout de la chaîne d'approvisionnement 30
2.5.4.2 Anti-contrefaçon 30
2.6 Conclusion 30
Chapitre 3 Conception de l’application 32
3.1 Introduction 32
3.2 Problématique traitée au cours de notre projet 32

3.3 Le scénario descriptif pour notre système 33
3.4 Méthodes d'analyse et de conception 34
3.4.1 Spécification et analyse des besoins 34
3.4.2 Expression des besoins 35
3.4.2.1 Diagramme de cas d'utilisation 36
3.4.2.2 Diagramme de séquence 41
3.4.2.3 Diagramme de classe 43
3.5 Conclusion 44
Chapitre 4 Réalisation de l'application 45
4.1 Introduction 45
4.2 Outils et environnements de développement 45
4.2.1 Truffle 45
4.2.2 Ganache 45
4.2.3 Metamask 46
4.2.4 Bibliothèque web3 46
4.2.5 Bootstrap 46
4.2.6 Visual Studio Code 46
4.2.7 Solidity 46
4.2.8 JavaScript 47
4.3 Présentation des interfaces de développement 47
4.3.1 La fenêtre d'interface « Page d'Accueil » 47
4.3.2 Les fenêtres d'interfaces « Pour l'Expéditeur » 48
4.3.2.1 La fenêtre « Authentification » 48
4.3.2.2 La fenêtre « Page d'accueil expéditeur» 48
4.3.3 Les fenêtres d'interfaces « Pour Transporteur/Client » 52
4.3.3.1 La fenêtre « Page d'accueil transporteur/client» 52
4.4 Discussion de notre solution 54

4.5 Conclusion 57

Conclusion Générale 58

Bibliographies 60

Introduction Générale

La blockchain est une technologie très récente qui s'est rapidement popularisée ces dernières années dans le monde. Et ceci est dû principalement à la très célèbre crypto-monnaie **bitcoin** [1], créé par un inconnu ayant pour pseudonyme « Satoshi Nakamoto » en 2008, et qui a tout changé.

La technologie blockchain consiste en une chaîne de blocs de données, reliés entre eux par des techniques cryptographiques garantissant que les données stockées ne peuvent être ni altérées ni trafiquées à moins que l'ensemble de réseau ne donne son accord.

Par conséquent, les systèmes blockchain fournissent une architecture sécurisée et fiable pour la transmission d'informations. Bien qu'elle soit souvent utilisée pour l'enregistrement de transactions de crypto-monnaies, la technologie blockchain peut s'avérer extrêmement utile pour sécuriser tous types de données numériques et son application au réseau de la chaîne logistique peut présenter de nombreux avantages.

Ce rapport de projet de fin d'études se concentre sur l'étude de la blockchain, ses mécanismes, ainsi que ses applications dans le domaine de la supply-chain (la chaine d'approvisionnement). Nous estimons que bien comprendre les mécaniques utilisées par Bitcoin, est essentiel avant de pouvoir comprendre comment la blockchain peut être utilisée dans différents domaines. C'est pour cette raison que nous avons choisi de consacrer tout une partie de ce document à l'étude de Bitcoin.

Nous avons divisé notre rapport en quatre chapitres : Lors du premier chapitre, nous avons présenté les cryptomonnaies au travers d'exemples. Par la suite, nous expliquons la vraie innovation dans Bitcoin : comment **est-ce qu'il parvient à la décentralisation**. La fin du chapitre est consacrée quant à elle à une description des transactions dans la blockchain, ainsi qu'à introduire le langage **« script »**.

Le deuxième chapitre est consacré aux supply chain. Nous expliquons la notion de la chaîne d'approvisionnement qui est le thème traité dans notre projet de fin d'étude, et dans lequel la Blockchain pourrait avoir un impact potentiel important. La fin du chapitre est

consacrée à quelques exemples des applications de la blockchain dans les chaînes d'approvisionnement.

Le troisième chapitre est dédié dans un premier temps à la présentation de la problématique traitée par notre application : « **Gérer une partie de la chaîne de production d'un produit »,** plus précisément, la dernière étape avant que le produit n'atteigne sa désignation finale. Nous présenterons donc d'abord les fonctionnalités de notre solution. Ensuite, nous présenterons les étapes de sa conception et sa modélisation.

Le quatrième chapitre sera quant à lui consacré à la réalisation de notre application. Nous présenterons notamment l'environnement de développement ainsi que les outils et langages de programmation que nous avons utilisés.

Chapitre 1

Introduction aux crypto monnaies et à la blockchain

1.1 Introduction

Aujourd'hui notre manière d'interagir a évolué, et la technologie de la Blockchain nous a conduits à repenser complètement la gestion d'une transaction et de sa vérification. Cette nouvelle technologie sur laquelle repose Bitcoin et d'autres crypto-monnaies, permet de fiabiliser les transactions et devrait ainsi offrir de multiples applications dans différents domaines. Nous allons consacrer ce premier chapitre à l'étude de la blockchain bitcoin et de son principe de fonctionnement. Nous allons dans un premier temps donner deux exemples de cryptomonnaies afin d'en saisir le sens et de comprendre le rôle important que peut posséder une autorité centrale dans un système centralisé. Par la suite nous expliquerons comment la blockchain arrive à garder un système fonctionnel en supprimant l'autorité de confiance et en la remplaçant par un protocole de consensus. Enfin nous finirons par décrire comment une transaction est écrite dans la blockchain et à l'aide de quel langage.

1.2 Introduction à Bitcoin et aux cryptomonnaies

1.2.1 L'utilisation des clés publiques en tant qu'identité dans le réseau bitcoin

Dans un schéma de signature électronique de document, étant donné qu'une personne peut signer n'importe quel message à l'aide de sa clé publique, et qu'elle n'a pas besoin de révéler sa clé privée pour que nous puissions être sûrs que c'est bien elle qui a signé son message, nous pouvons utiliser ce principe pour communiquer de façon pseudo-anonyme sur internet. Cela peut se faire en utilisant les clés publiques comme identité numérique en lieu et place de l'utilisation de notre identité réelle (une description détaillée de la signature électronique peut être trouvée dans [2]). Ce principe est utilisé dans Bitcoin pour garantir un certain degré d'anonymat dans le réseau :

- **Les individus dans Bitcoin sont identifiés seulement grâce à leurs adresses publiques.**
- Envoyer des bitcoins à quelqu'un **équivaut à envoyer des bitcoins vers l'adresse publique de cette personne.**

- Bitcoin, utilise **ECDSA** (Elliptic Curve Digital Signature Algorithm) [3], comme algorithme de signature numérique.

1.2.2 Exemple simple de crypto monnaie

Les auteurs de [4] donne un exemple assez simples de cryptomonnaies, et des différents problèmes qu'ils risquent de rencontrer. Nous allons dans la section qui suit, tenter de résumer cela, afin d'avoir une idée d'en quoi une cryptomonnaie peut consister.

1.2.2.1 GoofyCoin

C'est la cryptomonnaie la plus simple que nous puissions imaginer.

Il n'y a que deux règles très simples dans Goofycoin :

1ére règle : Une entité centrale nommée Goofy, peut créer de nouveaux coin (elle peut créer de la monnaie) à chaque fois qu'elle le désire. Cette monnaie nouvellement créée appartiendra à Goofy.

- Pour créer de la monnaie, Goofy génère un identifiant de jeton **UniqueCoinID** qu'il n'a jamais généré auparavant et construit un string Creat_Coin **[UniqueCoinID]**.
- Ensuite, Goofy génère la signature électronique de ce string à l'aide de sa clé privée.

- **Le String + La signature électronique de Goofy = Une pièce (un jeton)**.

Tout le monde peut vérifier que le jeton contient bien la signature de Goofy et que c'est bien un jeton valide qui a bien été généré par Goofy. La figure 1 ci-dessous représente un jeton dans GoofyCoin.

Figure 1-Structure de données représentant un jeton dans la cryptomonnaie GoofyCoin

2ème règle : Toute personne possédant un coin peut transférer la propriété de ce coin à quelqu'un d'autre. Mais ce transfert ne consiste pas seulement à transférer cette structure de données au bénéficiaire (au destinataire), le transfert s'effectue en utilisant des opérations cryptographiques.

Supposons que Goofy veuille transférer un coin à Alice. Pour se faire, il va créer un nouveau communiqué (une déclaration, **Goofy va générer une transaction**) qui dit :

« Versez **ceci** à Alice »

- Où « **ceci** » est un pointeur de hachage vers le coin en question.

Et comme nous l'avons mentionné plus haut, nous allons supposer que les identités des utilisateurs sont les clés publiques des utilisateurs du système. Donc Alice est représentée par sa clé publique dans le système.

Enfin, Goofy signe le string représentant la déclaration : Étant donné que c'est lui le propriétaire original du jeton, il doit signer n'importe quelle transaction qui va dépenser ce jeton. Une fois cette structure de donnée représentant la déclaration de Goofy signée, Alice devient la nouvelle propriétaire du jeton. Elle peut le prouver à tout le monde, puisqu'elle peut leur montrer la structure de données avec une signature valide de Goofy. En plus, cette transaction pointe vers un coin valide qui a vraiment appartenu à Goofy. Donc la validité et la propriété des jetons sont évidentes dans le système. La figure 2 ci-dessous illustre nos propos.

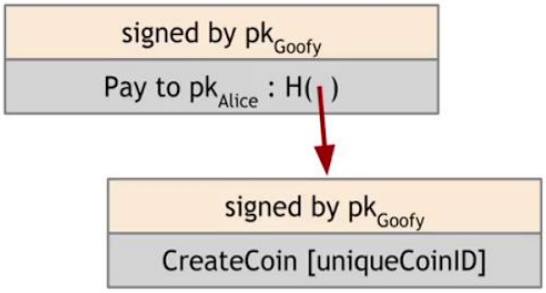

Figure 2-Structure représentant une transaction de transfert de jeton depuis Goofy vers Alice

Une fois qu'Alice est entrée en possession du jeton, elle pourra le dépenser à son tour. Pour se faire, elle va effectuer la déclaration suivante :

« Payer **ceci** à la clé publique de Bob ».

- où « **ceci »** est un pointeur de hachage vers le jeton qui lui appartient.

Alice devra bien sûr signer cette déclaration. Toute personne à qui l'on va présenter ce jeton pourra vérifier que Bob est vraiment son propriétaire, elle pourra suivre la chaîne de pointeur (hach pointer, ou pointeur de hachage) jusqu'à la création du jeton (voir la figure 3 ci-dessous). Elle pourra également vérifier qu'à chaque étape, le vrai propriétaire du jeton a vraiment signé la déclaration qui a transmis le jeton à la personne suivante.

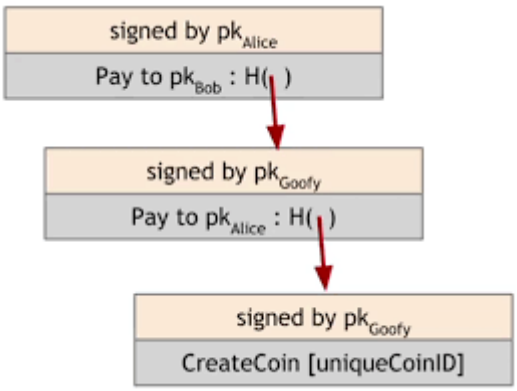

Figure 3-Structure représentant une transaction pour payer Bob

Pour résumer, les règles de GoofyCoin sont :

- Goofy peut créer de nouveau jeton, simplement en signant une déclaration qui stipule qu'il créer un nouveau jeton avec un identifiant unique.
- Tout individu possédant un jeton, peut le transmettre à un autre individu simplement en signant la transaction suivante : « Passer ceci à X » où X est l'adresse publique du bénéficiaire de la transaction et où ceci est un pointeur de hachage vers le jeton.
- Tout individu peut vérifier la validité d'un jeton en suivant la chaîne de pointeurs de hachage jusqu'à la création de celui-ci, en vérifiant toutes les signatures au passage.

Cependant, il y a un problème de sécurité fondamental avec les GoofyCoin:

Supposons qu'Alice transmette un jeton à Bob en signant la transaction, mais en omettant de le dire aux autres personnes qui utilisent cette monnaie. Elle pourra alors tenter une autre transaction dans laquelle elle va payer le même jeton à Chuck. En apparence, ceci va sembler être une transaction parfaitement valide. Chuck et Bob auront tous les deux des prétentions valides sur ce jeton.

Ceci est appelé **"a double spendingattack" "Une attaque par double dépense"** (voir la figure 4). Alice est en train de dépenser la même pièce deux fois et nous savons que la monnaie n'est pas censée fonctionner de la sorte.

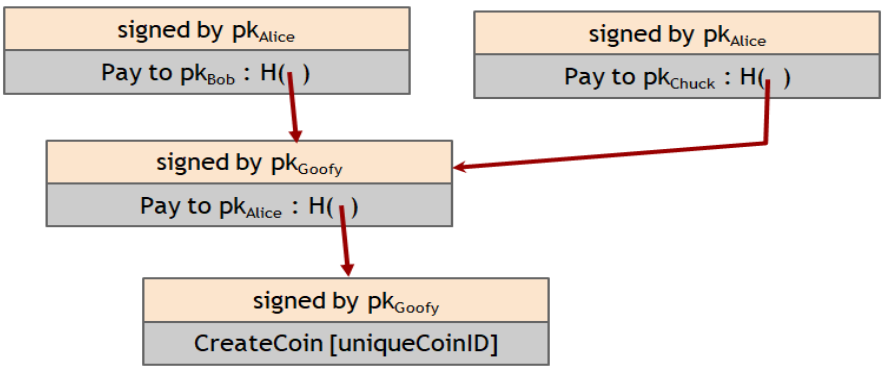

Figure 4-Attaque à double dépense

Discussion de la Figure ci-dessus : Chuck et Bob ont tous les deux des prétentions valides sur le jeton qu'Alice leur a transmis, puisqu'ils peuvent tous les deux prouver l'existence d'une chaîne de signatures valides, entre la transaction lors de laquelle ils ont reçu le jeton, et la toute première transaction dans laquelle le jeton a été créé par Goofy.

Les attaques de double dépense sont l'un des principaux problèmes que doit résoudre une cryptomonnaie. Goofycoin n'arrive cependant pas à résoudre le problème, et par

conséquent, cette crypto monnaie n'est pas sécurisée. Le mécanisme de transfert de jeton que nous venons de présenter ici pour Goofycoin est en fait le même que celui utilisé par bitcoin. Cependant, étant donné qu'il n'est pas sécurisé, Goofycoin ne peut pas être considéré comme une crypto monnaie utilisable. Nous allons dans la section suivante présenter une méthode pour empêcher ce genre d'attaque.

1.2.2.2 ScroogeCoin

Pour résoudre le problème de double dépense cité plus haut, nous allons présenter une deuxième crypto monnaie appelée ScroogeCoin. Elle est similaire à GoofyCoin dans certains points et diffère quelque peu dans d'autres.

La 1er idée de base de cette crypto monnaie, est qu'une entité nommée Scrooge, publie un registre appelé « **append-only »** qui va contenir l'historique de toutes les transactions effectuées. Ce registre sera public et visible par tous les utilisateurs de la crypto monnaie.

Append-only : Cette propriété veut dire que toute information écrite sur ce registre, sera enregistrée de façon définitive. Cela veut dire que l'on ne pourra pas la supprimer.

- Si cette propriété est réalisée, alors nous pourrons nous défendre contre la double dépense d'un Jeton, **en requérant que toute transaction ne peut être validée qu'après avoir été inscrite sur le registre**.
- Ceci va nous permettre de vérifier qu'un Jeton n'a pas été dépensé lors d'une transaction précédente, et **que son propriétaire légitime est bien celui qui tente de le dépenser.**
- Pour implémenter ce registre (append-only), Scrooge peut construire une blockchain, qu'il signera numériquement.

Cette blockchain consiste en une série de blocs de données, chacun contenant une transaction. Chaque bloc contiendra :

1. L'identifiant de la transaction.
2. Le contenu de la transaction.
3. Et enfin un hash pointer vers le bloc précédent (consulter la figure 5).

Scrooge signera numériquement l'empreinte finale du dernier bloc, ce qui aura pour effet de lier toutes les données dans la structure, **et il publiera également la signature en même temps que la blockchain.**

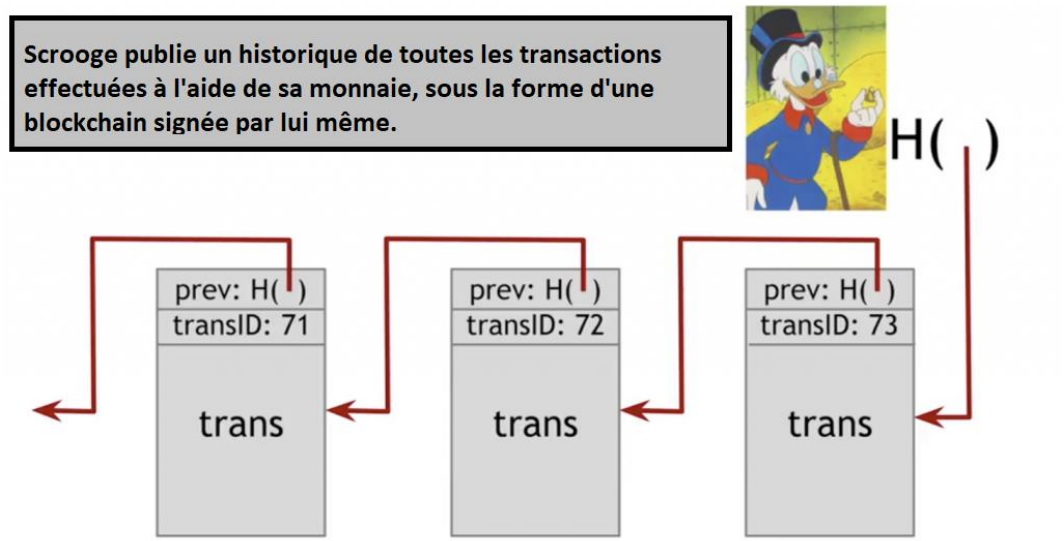

Figure 5-ScroogeCoin Blockchain

Dans le système de ScroogeCoin, une transaction ne compte que si elle est contenue dans la blockchain et qu'elle a été signée par Scrooge. Ceci va impliquer que tout le monde pourra vérifier qu'une transaction a été approuvée par lui, en vérifiant la signature dans le bloc dans lequel la transaction a été insérée. Scrooge quant à lui, devra vérifier que la transaction n'est pas en train de dépenser un jeton qui aurait déjà été dépensé, avant d'inscrire la transaction.

Nous pourrions nous poser la question suivante : Pourquoi avons-nous besoin d'une blockchain, alors que toutes les transactions ont déjà été signées par Scrooge ?

- Ceci en fait, garantit la propriété d'append-only dont nous avons fait mention au début de la section.
- Si Scrooge tente de supprimer ou d'ajouter une transaction ou d'en modifier une déjà existante, ceci va affecter toutes les autres transactions suivant celle-ci, grâce à la blockchain. Et tant que quelqu'un surveille le dernier hash publié par Scrooge, tout changement devient évident et facilement détectable (voir la figure 6).

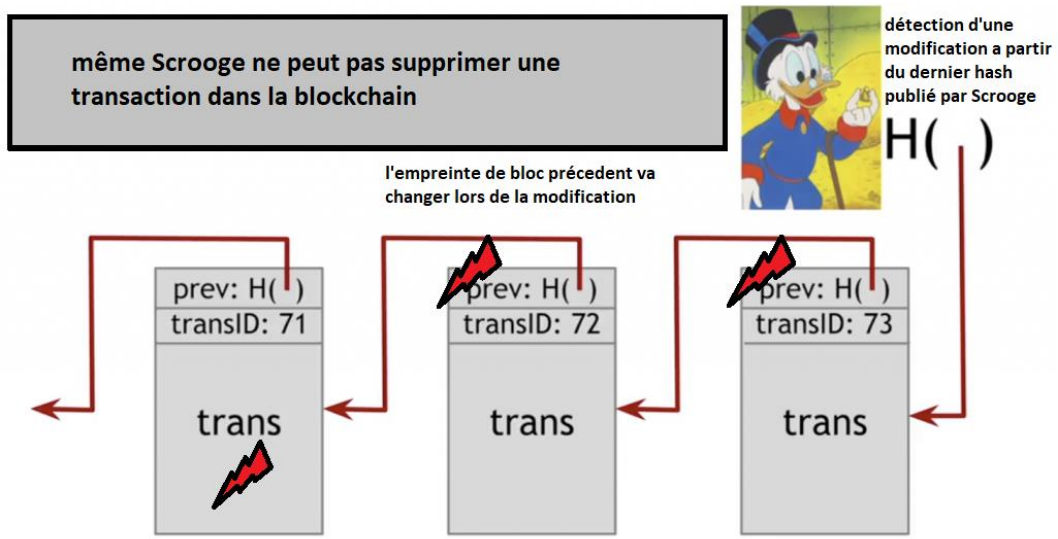

Figure 6-Détection de modification dans la blockchain de Scrooge

- Dans un système où Scrooge signerait chaque bloc individuellement, nous aurions besoin de garder une trace de chaque signature de Scrooge jamais signée. Utiliser la blockchain rend la surveillance de l'historique des transactions beaucoup plus facile à mettre en œuvre.

La raison pour laquelle nous avons pris le temps d'expliquer quelque peu ScroogeCoin, c'est que son fonctionnement est **très similaire au fonctionnement de la crypto monnaie bitcoin.** Comprendre les principes expliqués dans cette section, équivaudrait à comprendre le principe de fonctionnement de bitcoin.

Nous arrivons à présent au problème central et principal avec le système ScroogeCoin : Ce système va fonctionner dans le sens où, les utilisateurs peuvent voir quel jeton est valide, et la double dépense n'est pas possible parce que tout le monde pourra regarder dans la blockchain, et voir toutes les transactions et vérifier que chaque jeton est consommé une seule fois.

Le problème dans le système, c'est Scrooge, il possède un immense pouvoir dans le système. Il ne peut certes pas créer de fausses transactions, parce qu'il ne peut pas falsifier les signatures des autres. Cependant, il peut :

1. Arrêter d'approuver les transactions de certaines personnes, les priver du service et rendre leurs jetons inutilisables (Scrooge va leur dénier le service).

2. Il peut refuser de publier des transactions, sauf si des frais de transaction lui sont payés pour chaque transaction.

3. Bien entendu, Scrooge peut créer autant de jetons pour lui-même qu'il le désire.

4. Enfin, Scrooge peut en avoir assez de tout cela, et arrêter de mettre à jour la blockchain. Et arrêter par conséquent tout le système.

Le problème dans ce système c'est la **centralisation.** Malgré le fait que Scrooge soit satisfait par lui, les utilisateurs pourraient ne peut pas l'être.

Même si un système comme ScroogeCoin paraît irréaliste, une grande partie des premières recherches sur des cryptomonnaies supposaient qu'il y aurait une sorte d'autorité de confiance. Cependant, toutes les cryptomonnaies utilisant une autorité centrale n'ont pas réussi à prendre leur envol en pratique. Il y a plusieurs raisons à cela, mais rétrospectivement, il semblerait qu'il soit difficile pour les gens d'accepter une crypto monnaie avec une autorité centrale. Par conséquent, le challenge technique le plus important que nous devons relever pour améliorer ScroogeCoin, créer un système fonctionnel et qui puisse marcher, est le suivant : **peut-on supprimer Scrooge du système ?** Peut-on se débarrasser de cette figure d'autorité ? Peut-on avoir une crypto monnaie qui opère de la même façon que ScroogeCoin dans la plupart des aspects mais qui ne possède aucune autorité centrale de confiance ?

Si nous pouvons résoudre ces problèmes, alors, nous pourrons construire une crypto monnaie semblable à ScroogeCoin mais sans autorité centrale : **Ce serait un système comme le Bitcoin**[4]**.**

1.3 Comment Bitcoin parvient à la décentralisation

1.3.1 Décentralisation contre centralisation

La décentralisation est un concept important pour Bitcoin, mais aucun système n'est purement centralisé ou décentralisé. Par exemple, le concept d'email est censé être décentralisé de par son protocole SMTP qui est open source. N'importe qui peut implémenter son propre serveur email. Mais dans la réalité, la plupart des utilisateurs se tournent vers des fournisseurs de services privés, dont une petite poignée domine le marché.

La même analogie peut être appliquée avec le Bitcoin. Satoshi Nakamoto a pensé le protocole comme étant décentralisé, mais en réalité il contient des aspects qui sont décentralisés et d'autres qui ne le sont pas.

1.3.1.1 Aspects de la décentralisation dans Bitcoin

Lorsque nous parlons de la décentralisation dans bitcoin, nous parlons de cinq aspects :

1. Qui est ce qui entretient le registre ?
2. Qui est ce qui a autorité pour dire quelles sont les transactions valides ?
3. Qui est ce qui peut créer de nouveaux bitcoins ?
4. Comment déterminer comment les règles du système changent ?
5. Comment est-ce que les bitcoins acquièrent un taux de change ?

Dans ce document, nous n'allons traiter que les trois premiers aspects de la décentralisation. La référence [4] contient de plus amples détails sur les aspects 4 et 5. Elle contient également, d'autres recommandations de lecture sur le sujet.

La réponse aux trois premières questions peut être fournie avec un seul terme : **le Minage** (un bref descriptif du minage est fourni un peu plus loin dans le document).

Comme nous venons de le mentionner, aucun système n'est décentralisé à 100%. Bitcoin ne déroge pas à cette règle. Certains de ses aspects le sont, mais d'autres non.

1.3.1.2 Aspects de Bitcoin qui sont décentralisé

Le réseau P2P est presque décentralisé à 100%, étant donné que c'est un réseau P2P et ouvert à tous. En d'autres termes, n'importe qui peut installer un logiciel client Bitcoin et rejoindre le réseau (La barrière d'entrée est assez faible).

1.3.1.3 Aspects de Bitcoin qui sont centralisés

- **Le minage :** il est ouvert à n'importe qui, mais demande un investissement très important. Ce qui a mené à une concentration de pouvoir au sein d'un ensemble restreint de mineurs.
- **La mise à jour du logiciel client :** Bitcoin est censée être open source, et chacun est censé pouvoir implémenter sa propre version du logiciel client, et rejoindre le réseau. Cependant, la plupart du temps, la communauté d'utilisateurs installe simplement la version core du logiciel, elle fait confiance aux développeurs de cette version, ce qui implique que ces derniers possèdent un assez grand pouvoir.

1.3.2 Consensus distribué

Pour réaliser la décentralisation dans Bitcoin, Nous devons supprimer l'autorité centrale dans une crypto-monnaie (supprimer Scrooge, ou Goofy). Pour se faire, nous pouvons par exemple partager une copie de registre de transactions dans chaque nœud du réseau P2P. De plus, lorsque l'on désire ajouter une nouvelle transaction, il faudra l'ajouter dans toutes les copies des utilisateurs pour qu'elle soit considérée comme valide. Les problèmes qui se posent alors sont:

1. Comment savoir quelles sont les transactions valides à ajouter dans le registre ?

2. Comment les nœuds du réseau vont-ils décider d'ajouter le prochain bloc dans la chaîne de blocs ?

3. Comment les nœuds vont-ils arriver à se mettre d'accord sur le prochain bloc à ajouter à la blockchain, et dans lequel toutes les transactions sont valides ? Cette dernière question est dénommée sous le terme d'un **problème de consensus**.

Le problème de consensus distribué est étudié depuis très longtemps dans la littérature de l'informatique, pour avoir des systèmes fiables dans le cadre de base de données distribuées. Les protocoles de consensus distribués ont différentes applications telles que : les DNS (Le DNS permet d'associer un nom compréhensible, à une adresse IP) [5].

Une seconde application des protocoles de consensus que l'on peut citer, consiste en les **AltCoin.** Les AltCoin désignent toute monnaie numérique qui s'inspire de Bitcoin **« alternative à Bitcoin »**. Les AltCoin peuvent proposer des fonctionnements inspirés de celui du Bitcoin avec quelques variations, par exemple avec de nouvelles règles de consensus, mais elles peuvent aussi proposer un fonctionnement totalement différent en repartant de zéro [6].

1.3.2.1 Définition d'un protocole de consensus

Nous avons « n » nœuds dont chacun à une valeur d'input, quelques-uns sont malicieux ou contiennent des erreurs. Le protocole de consensus possède deux propriétés :

1. Il doit se terminer avec tous les nœuds qui se sont mis d'accord sur une même valeur d'output.

2. La valeur de consensus doit être générée par un nœud honnête.

1.3.2.2 Comment le consensus fonctionne dans Bitcoin

Les n nœuds du réseau vont proposer leurs propres blocs de transactions, puis ils vont effectuer un certain protocole de consensus qui doit nous donner comme sortie : un bloc valide proposé par un nœud valide, qui va être ajouté à la blockchain.

Remarque :

Le protocole de consensus dans Bitcoin fonctionne mieux que les protocoles traditionnellement modélisés pour une utilisation dans des bases de données distribuées, parce qu'il effectue certaines choses différemment par rapport aux protocoles traditionnels :

- Il introduit la notion de motivation (Possible uniquement parce que c'est une monnaie).
- Il accepte le hasard.

1.3.3 Consensus sans identité

Traditionnellement, la notion d'identité dans les protocoles de consensus est très importante pour leurs exécutions. Cependant, le réseau bitcoin ne fournit pas d'identité aux nœuds. Ceci est dû au fait qu'il soit difficile, dans un système P2P sans autorité centrale qui gère le réseau, de fournir des identités aux nœuds du réseau.
Une deuxième raison pour l'absence d'identité dans la blockchain Bitcoin est le fait que son concepteur, Satoshi Nakamoto, avait voulu que ça soit une caractéristique intrinsèque au système. Cette caractéristique est désignée sous le terme de **pseudo anonymat**.

Mode opératoire du protocole de consensus dans Bitcoin

1. Les nouvelles transactions sont diffusées sur tous les nœuds.
2. Chaque nœud collecte les nouvelles transactions dans un bloc.
3. À chaque tour, un nœud**, « choisi aléatoirement »**, parvient à diffuser son bloc.
4. Les autres nœuds n'acceptent le bloc, que si toutes les transactions qu'il contient sont valides (pas de doubles dépenses, signatures valides).

Les nœuds expriment implicitement leur acceptation du bloc, en incluant son hachage dans le bloc suivant qu'ils créent.

1.3.4 Incitations et preuve de travail

1.3.4.1 Les incitations

Lors de cette section, nous allons répondre à la question suivante : Comment **inciter** les nœuds du réseau à agir de façon honnête ? Comment les **motiver** à agir de la sorte ? Ceci est un problème difficile. On ne peut pas pénaliser les nœuds qui agissent de façon appropriée (diffuse des blocs qui contiennent une transaction de double dépense par exemple), car il n'y a pas de notion d'identité dans le réseau bitcoin. Une autre formulation de ce problème serait : Pouvons-nous récompenser les nœuds qui ont créé des blocs valides ?

La réponse est **oui**. Bitcoin a introduit la notion de motivation et d'incitation pour les nœuds. Il existe principalement deux types de motivations :

Motivation n°1 : les récompenses par bloc (bloc reward)

Le créateur du bloc est autorisé à y inclure une transaction spéciale nommée **coinbase**. Cette transaction consiste en la création d'un certain montant de bitcoin. Bien sûr, le bénéficiaire de cette transaction sera très probablement le créateur du bloc.

La valeur de bitcoin créé pour chaque nouveau bloc est fixe : actuellement elle est de 6.25 bitcoins. Elle est divisée par deux tous les 4 ans à peu près.

Le créateur du bloc ne peut « collecter » la récompense que si le bloc se retrouve sur une branche consensuelle à long terme. Donc s'il y inclut des transactions invalides ou de double dépense, il court le risque que son bloc soit rejeté par les autres nœuds du réseau, et par conséquent, qu'il ne finisse pas dans la chaîne de consensus, ce qui implique bien sûr qu'il ne pourra pas récupérer ses gains.

Motivation 2 : Les frais de transaction

Le créateur d'une transaction peut choisir de mettre une valeur d'output inférieure à la valeur d'input de la transaction. La différence entre les deux sera considérée comme des frais de transaction qui iront au créateur du bloc, comme un pourboire pour la peine qu'il s'est donné pour miner le bloc.

1.3.4.2 Preuve de travail (proof of work) PoW

Nous avons mentionné plus haut dans le document, qu'un nœud est sélectionné aléatoirement pour proposer un bloc lors du processus de consensus. En réalité cette sélection s'effectue à l'aide d'une sorte de course effectuée par l'ensemble des nœuds du réseau. Le nœud prétendant avoir gagné la course, devra fournir ce que l'on désigne par : **une preuve de travail.**

Principe de la preuve de travail : Sélectionner des nœuds proportionnellement à une ressource que personne ne peut monopoliser (nous l'escomptons tout du moins).

La sélection du nœud, peut être en proportion de la puissance de calcul de chaque nœud: « **Preuve de travail »**, ceci veut dire que plus un nœud possède de puissance de calcul, plus il aura de chance d'être sélectionné.

- La **preuve d'enjeu** est une alternative à la preuve de travail, elle consiste en la sélection d'un nœud en proportion de la propriété « **preuve d'enjeu »**. Elle est utilisée par certaines cryptomonnaies alternatives.

1.4 Scripts Bitcoin

Les transactions dans Bitcoin sont formulées dans une langage de script. Une transaction valide est une transaction dont le script s'est exécuté avec succès. Bitcoin utilise un langage de script nommé tout simplement **« script ».** C'est un langage de programmation très simple, utilisé pour traiter et générer les transactions. Le langage se lit de gauche à droite. Il est basé sur des structures linéaires : **des piles**. Les piles traitent les instructions et les données dans l'ordre LIFO (dernier entré - premier sorti). Les instructions dans la pile sont exécutées consécutivement l'une après l'autre. Ce langage n'est pas « Turing complet » car sa fonctionnalité est limitée et il ne peut pas boucler (il ne contient pas d'instruction de boucle).

Une transaction bitcoin de paiement, contient deux scripts : le **scriptSig** et le **scriptPubKey.**

- **Le scriptSig est le script de déverrouillage** qui contient une signature numérique qui garantit que c'est bien le propriétaire légitime des bitcoins qui désire les dépenser. Dans les premières versions du logiciel Bitcoin, des vérifications de signature ont été incluses. Par conséquent, le système n'accepte

les transactions que si les signatures et leur vérification sont conformes à une série de règles établies qui garantissent un bon comportement sur le réseau.

- **Le scriptPubKey, est le script de verrouillage, qui contient un hachage de clé publique, également appelé adresse Bitcoin.** Le propriétaire légitime des bitcoins devra en quelque sorte déverrouiller ce script pour pouvoir les dépenser (il devra l'exécuter avec succès). La figure 7 ci-dessous représente une transaction bitcoin réelle rédigée sous la forme d'un script.

Figure 7-Transaction Bitcoin

La structure des blocs

La figure 8 ci-dessous illustre la structure d'un bloc dans la blockchain bitcoin.

Chaque bloc contient le pointeur de hachage vers le bloc précédent, mais également un ensemble de transactions rassemblées sous la forme d'un arbre de Merkle.

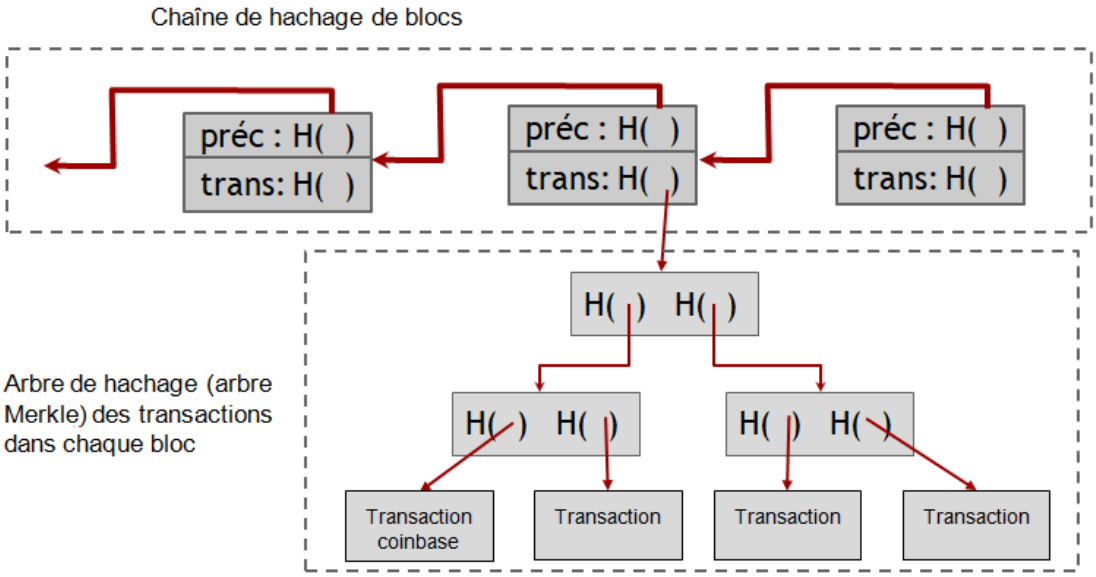

Figure 8-Structure d'un bloc Bitcoin

- Chaque bloc contient une transaction spéciale qui s'appelle la transaction **CoinBase** illustrée dans la figure 9 ci-dessous.

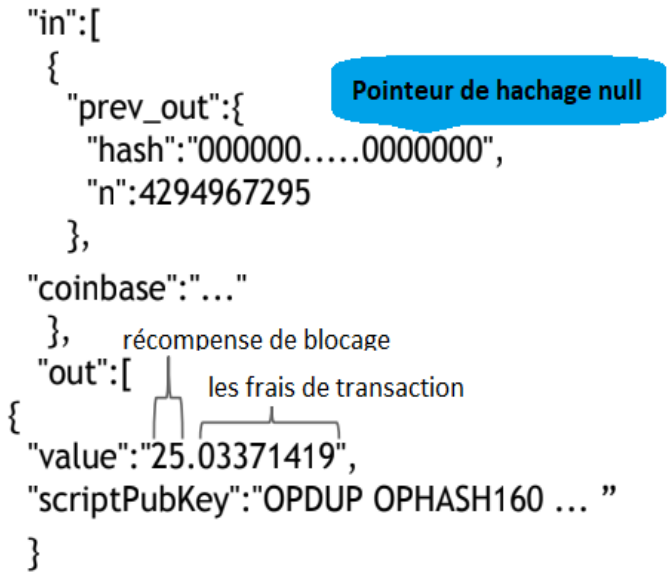

Figure 9-Transaction Coinbase

1.5 Types de blockchain

Après avoir donné un bref descriptif du principe de fonctionnement de la blockchain, qui est la blockchain originale, nous allons à présent donné les différents types apparus par la suite. En effet, toutes les blockchain ne sont pas identiques. Elles peuvent être divisés en quatre

systèmes de blockchain différents : blockchain publique, blockchain privée, blockchain de consortium et blockchain hybride. Chaque type répond à certains objectifs et exigences[7].

1.5.1 Blockchain publique

Connue également sous le nom de blockchain sans autorisation. En général, elle est ouverte et décentralisée mais cependant lente en termes de publication de transactions. Tout le monde peut participer, lire et écrire des données sur le réseau sans vérification d'autorisation. Tout le monde a également accès en toute transparence aux données stockées. Comme exemples de blockchain publiques nous avons : Bitcoin, Ethereum, Lisk, Litecoin[7].

1.5.2 Blockchain privée

Ce type de blockchain est également connue sous le nom de blockchain autorisée. Il se réfère à un système fermé et partiellement ou complètement centralisé. Ce type utilise un « grand livre privé » distribué et limite les participations grâce à une autorité centrale - propriétaire de la blockchain et surtout une organisation unique et hautement fiable, qui a le pouvoir de contrôler et de consolider le réseau et de donner des autorisations à certains nœuds, afin d'afficher, lire, écrire ou valider des transactions. Cette blockchain est très efficace car la vérification est effectuée par le propriétaire du réseau et est privée car le propriétaire contrôle qui peut quoi faire dans le réseau. Néanmoins, il est difficile d'aligner de nombreuses organisations sur une même blockchain privée. Les exemples de ce type de chaînes de blocs sont : Hyperledger Fabric, Hyperledger Sawtooth, Ripple, MultiChain[7].

1.5.3 Blockchain de consortium

Également connue sous le nom de blockchain fédérée, elle désigne un système partiellement décentralisé et « semi-privé ». Le réseau est contrôlé par un groupe d'organisations, mais fonctionne dans différentes organisations. Il n'y a pas de consolidation du pouvoir de contrôle. Les participants ont besoin d'autorisations pour afficher, lire, écrire et vérifier les transactions. C'est efficace, car dès nœuds relativement plus petits vérifient les transactions. La blockchain de consortium est sécurisée et contribue à protéger la confidentialité. Plus d'une organisation peut agir en tant que nœud et avoir accès pour échanger des informations et faire du minage. Comme exemples nous citons : Quorum, R3 Corda[7].

1.5.4 Blockchain hybride

Fait référence à une combinaison de la blockchain privée et publique. La blockchain hybride est contrôlée par un consortium d'entreprises ou d'entités gouvernementales qui peuvent à la fois donner accès au public pour afficher ou ajouter des données et restreindre l'accès à ses membres[8] . Ce type utilise à la fois un grand livre ouvert et un grand livre privé. Il utilise les fonctionnalités des deux types de blockchains, c'est-à-dire que l'on peut avoir un système privé basé sur des autorisations ainsi qu'un système public sans autorisation. Par conséquent, ce système maximise les avantages d'une solution combinée de blockchain publique et privée. Les entreprises peuvent sécuriser les transactions en arrière-plan avec leurs partenaires commerciaux sur un grand livre privé, tout en partageant également des informations sur les produits avec les clients sur un grand livre ouvert. Cela permet également la flexibilité d'inviter plus de participants. Comme exemple, nous allons citer : Dragonchain, XinFin, Balance[7].

1.6 Conclusion

Nous avons au cours de ce chapitre, donné deux exemples simples de crypto monnaies, afin de saisir la notion d'autorité de confiance et de son pouvoir sur tout système centralisé. Par la suite, nous avons décrit comment Bitcoin est arrivé à supprimer cette figure d'autorité du système, tout en garantissant que la double dépense ne soit pas possible. La décentralisation est la plus grande innovation de Bitcoin, elle a été possible grâce à un protocole de consensus utilisant un savant mélange de cryptographie et d'incitation. Après avoir présenté le protocole de consensus et la notion de preuve de travail, nous avons donné un exemple de transaction écrite ne langage script. Enfin nous avons cité les principaux types de blockchains. Lors du prochain chapitre, nous allons donner des exemples d'utilisation de la blockchain dans un tout autre domaine que celui du paiement : celui des chaînes d'approvisionnement ou supply chain.

Chapitre 2

Blockchain et supply chain

2.1 Introduction

Au cours du chapitre précédent, nous avons brièvement présenté les principe de fonctionnement de la blockchain. En plus du domaine du paiement, plusieurs autre utilisations peuvent être envisagées avec cette technologie, et dans de nombreux domaines : le vote électronique, les assurances, l'immobilier, la santé, la supply Chain avec ces différents secteurs…etc.

Lors de ce deuxième chapitre, Nous allons d'abord définir la supply chain ainsi que les défis auxquels elle doit faire face. Par la suite nous allons citer quelques-unes des applications de la blockchain dans ce domaine.

2.2 Supply Chain " Chaîne d'approvisionnement "

La technologie blockchain peut être utilisée non seulement dans le domaine du paiement par internet, mais également dans de nombreux autres tels que le vote, l'immobilier, la santé, et enfin les supply chain. Dans le souci d'être les plus concis possible, nous n'allons pas détailler les domaines d'application qui ne font pas partie de notre thème, une description assez détaillée du potentiel de la blockchain peut être trouvée dans [9]. Nous allons dans la partie qui suit étudier plus en détail ses applications dans le secteur des chaînes d'approvisionnement. En effet, C'est un sujet qui touche énormément la société de consommation dans laquelle nous vivons aujourd'hui, car il y a beaucoup de consommations et donc beaucoup de productions dans le monde. Mais avant cela, donnons une définition de la supply chain.

Définition de la supply chain ou chaîne d'approvisionnement

Définition 1 : C'est la coordination de toutes les activités industrielles ou logistique pour faire en sorte que l'utilisateur final puisse consommer le produit final. Nous parlons alors d'un besoin de consommation.

Définition 2 : C'est un flux des produits et de l'information le long des processus logistiques à partir de l'achat des matières premières jusqu' à la livraison des produits finis au consommateur. La chaîne d'approvisionnement inclut tous les fournisseurs de service et les clients.

Définition 3 : La supply Chain consiste en la coordination ou l'enchaînement de toutes les activités industrielles ou logistiques pour une production destinée à la consommation finale (inscrire chaque étape de processus de fabrication d'un produit depuis sa production jusqu'à son lieu de vente).

Elle met en relation de nombreux acteurs : fournisseurs, transporteurs, fabricants, distributeurs, détaillants …etc[10].

2.3 Défis actuels de la supply chain :

La plupart des dysfonctionnements de la supply chain sont les surcoûts du partitionnement des services au sein de l'organisation, l'insuffisance de coopération entre les clients et les fournisseurs et le manque de performance du système d'information. C'est à ces nouveaux enjeux que doit répondre la gestion SCM (supply chain management).

La supply chain ne fonctionne jamais très bien en pratique et quand elle fonctionne mal, les producteurs ou les distributeurs courent le risque de perdre des ventes parce qu'un produit n'est plus disponible dans les étagères par exemple, ce qui va pousser les consommateurs à passer chez les concurrents.

Le modèle actuel rend difficile le maintien d'une chaîne logistique cohérente et efficace, ce qui a un impact négatif non seulement sur la rentabilité des entreprises mais également sur le prix de détail final.

A l'heure actuelle, le système de gestion de la S-Chain souffre d'un manque d'efficacité et rencontrent des difficultés lorsque l'on tente d'intégrer toutes les parties concernées (les produits et les matériaux, ainsi que l'argent et les données). Certains des problèmes les plus importants des supply chain peuvent être résolus grâce à l'utilisation de la technologie de la Blockchain qui offre de nouvelles méthodes d'enregistrement, de transmission et de partage des données.

2.4 Comment la blockchain peut apporter des solutions aux problèmes rencontrés dans le domaine de la supply chain

Les technologies de la blockchain ont capturé l'imagination des universitaires, des gestionnaires et des pratiquants du monde entier. Il est largement admis par ces acteurs que la blockchain n'est pas un mot à la mode, mais une technologie hautement perturbatrice qui remodèle déjà les organisations et leurs modèles commerciaux de chaîne d'approvisionnement. Malgré l'avancée significative de ces dernières années, les applications blockchain concernant les opérations et la gestion de la chaîne d'approvisionnement (OSCM - Opération and supply chain management) sont encore à leurs débuts. Nous savons peu de choses sur le rôle de la blockchain en termes de traçabilité des opérations, ainsi que dans des domaines tels que le commerce électronique, l'agriculture, les services publics, ...etc [9].
À cet effet, nous nous intéressons plus précisément à la façon dont la blockchain s'intègre et impacte les nouveaux modèles commerciaux, transforme les relations et améliore les performances. Les trois points qui suivent représentent quelques-uns des avantages que cette technologie peut apporter :

- La blockchain peut être utilisée pour tracer les articles des fournisseurs afin de s'assurer que les produits sont authentiques, décrits avec précision et transportés correctement et en toute sécurité.
- Elle peut apporter la transparence à la chaîne d'approvisionnement, en permettant au consommateur de constater dans quelles conditions sa nourriture a été cultivée.
- À l'aide de la blockchain, nous pourrions suivre chaque ingrédient dans notre alimentation depuis son origine, afin que nous puissions, par exemple, comprendre si la bouteille d'huile d'olive que nous venons d'acheter est à 100% d'huile d'olive, ou si elle est mélangée avec d'autres types d'huile [11].

2.5 Application de la blockchain dans Les chaînes d'approvisionnement « Supply Chain »

Les secteurs concernés par la supply chain par rapport à la blockchain sont multiples : **luxe** (diamants, sac …), **industrie pharmaceutique** (enregistrer chaque étape de la chaîne de fabrication et de distribution d'un médicament), **immobilier et bâtiment** (enjeux de maintenance), **industries lourdes** (pièces détachées).

Les supply Chain actuelles font face à des problèmes pour assurer la traçabilité totale des produits, ainsi qu'à des manques de flexibilité et de rapidité. Ceci engendre de nombreux coûts externes. La technologie Blockchain ouvre le champ à un suivi bien plus fiable des produits, sans qu'un individu ou une entité ne puisse modifier ou supprimer l'information. De plus, elle permet aux acteurs de détecter en temps réel où et quand la faute/fraude a été commise. Au cours de cette section, nous allons présenter quelques-uns des domaines de l'industrie concernés.

2.5.1 Applications de la blockchain dans la chaîne d'approvisionnement alimentaire

La chaîne d'approvisionnement alimentaire est confrontée à des défis sans précédent, concernant la santé du consommateur, la sécurité et la sûreté alimentaires, le changement climatique et le bien-être animal. Pour relever ces défis, assurer la transparence et la traçabilité dans la chaîne d'approvisionnement alimentaire devient un enjeu de plus en plus important, afin de réduire les pertes et gaspillages 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. La montée en puissance des initiatives basées sur la blockchain trouve une utilité pour assurer la traçabilité en apportant plus de transparence et d'efficacité à la chaîne d'approvisionnement agricole et alimentaire.

Les chaînes d'approvisionnement alimentaire sont devenues mondiales et complexes avec de multiples fournisseurs de matières premières et d'ingrédients répartis dans le monde[12]. Cela rend difficile le suivi du flux des matières premières et des produits de la ferme à la fourchette et d'assurer la traçabilité tout au long de la chaîne. Les rappels d'aliments sont également devenus assez courants, plusieurs produits étant rappelés quotidiennement en raison de problèmes de qualité et de santé. Cela a également donné lieu à des cas très médiatisés comme le rappel du beurre d'arachide aux États-Unis, le scandale de la viande de cheval au Royaume-Uni et l'adultération (contrefaçon) du lait en poudre pour bébé en Chine. Les produits alimentaires en poudre, les épices et les produits de grande valeur comme l'huile d'olive sont particulièrement sensibles à l'altération. Les consommateurs veulent devenir plus conscients de la qualité des aliments qu'ils consomment et aimeraient avoir les informations de traçabilité avant d'acheter le produit. Les détaillants doivent assurer cette traçabilité et également suivre l'état des produits transportés.

Des technologies telles que la RFID (radio frequency identification) ou des capteurs sans fil peuvent être utilisées pour suivre respectivement l'emplacement et l'état du produit. La blockchain peut intégrer et gérer chaque processus et transaction tout au long de la chaîne d'approvisionnement agricole en temps réel. Chaque transaction traitée dans le registre distribué peut contenir des détails de transaction et des attributs spécifiques pour le produit, qui peuvent être ajoutés par les membres de la chaîne d'approvisionnement. Les entreprises peuvent saisir des informations de traçabilité tout en gardant cachées les informations propriétaires ou concurrentielles importantes. Les membres de la chaîne d'approvisionnement peuvent identifier et examiner le mouvement du produit à chaque étape : de la ferme, aux conditions et détails de transport et de stockage, à mesure que le produit est acheminé vers le détaillant et le consommateur[13]. Ainsi, la blockchain peut permettre aux détaillants de partager les informations de provenance avec les clients.

Toutes les parties prenantes impliquées dans la chaîne d'approvisionnement alimentaire (agriculteurs, distributeurs, conditionneurs, transformateurs, épiciers, restaurants, commerçants) sont motivées par le besoin de démontrer à leurs clients la qualité supérieure de leurs processus et produits. Mais cela s'est avéré être une tâche très difficile en raison des multiples parties prenantes impliquées et de leur dispersion géographique. Les cas d'utilisation de la blockchain dans la chaîne d'approvisionnement alimentaire vont au-delà de la sécurité alimentaire. Elle ajoute également de la valeur au marché actuel en créant un registre distribué dans le réseau et en équilibrant le prix du marché. Certains de ces cas sont donnés ci-dessous, mais ils ne sont pas limités[7].

2.5.1.1 Partage d'informations pour la traçabilité et la transparence

Les informations sur un produit final doivent être aussi complètes, fiables et facilement accessibles que possible. Le QR code peut permettre le partage de telles informations. Par exemple, il peut donner 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.

Nous donnons comme exemple une entreprise chinoise, “ZhongAn Online” qui a lancé un programme d'élevage basé sur la blockchain, appelé «GoGo Chicken», afin de permettre aux clients de suivre les poulets d'élevage biologique, qu'ils ont pré-achetés en utilisant la technologie de reconnaissance faciale et également pour surveiller la santé et les mouvements des volailles grâce à des bracelets de suivi GPS attachés aux jambes. Toutes les informations sont enregistrées de manière immuable sur le registre de la blockchain et les clients peuvent suivre leurs mouvements, comment ils grandissent, et ce qu'ils mangent [7].

2.5.1.2 Améliorer la qualité et éviter les rappels

Les rappels de produits sont de plus en plus préoccupants pour les fabricants et les détaillants de produits alimentaires. Le non-respect des bonnes pratiques de fabrication (BPF) étant la principale raison de ces rappels [14]. Le manque de capture et de surveillance en temps réel des données de processus rend difficile le suivi des lots de production individuels. Le suivi précis des produits de qualité inférieure et l'identification des transactions ultérieures des produits peuvent aider à réduire les retouches et les rappels [15]. Capturer les données de processus à l'aide de la RFID ou de capteurs, et créer des systèmes d'alertes associés à la blockchain garantira l'absence de falsification des données et aidera à la surveillance en temps réel. Cela aidera à améliorer la qualité des produits, des processus de production, le stockage et le transport et évitera les rappels coûteux de produits alimentaires.

Parmi les difficultés rencontrées dans ce genre d’application, nous pouvons citer le suivi des fruits et légumes vendus en vrac provenant de différentes fermes, la résistance des agriculteurs à partager trop d'informations et la création d'entrées de données complètes à partir de différents nœuds le long d'une longue chaîne de valeur [7].

2.5.1.3 Cas réel d'utilisation de la chaîne alimentaire

Le détaillant français Carrefour a lancé des informations sur la blockchain pour 20 articles, dont le poulet, les œufs, le lait cru, les oranges, le porc et le fromage, et en ajoutera à l'avenir en mettant l'accent sur les domaines où les consommateurs veulent être rassurés, comme les bébés et les produits biologiques. Les clients peuvent scanner un code-barres QR sur un pamplemousse avec leur téléphone et connaître la date de récolte, le lieu de culture, le propriétaire de la parcelle, quand elle a été emballée, combien de temps il a fallu pour transporter en Europe et des conseils sur la préparation [15]. L'utilisation de la Blockchain

pour partager des informations sur les produits avec les clients a permis d'accélérer les ventes de pamplemousse et de poulet pour Carrefour. Le partage de ces informations avec les clients permet également à Carrefour de gagner la confiance des clients. Jusqu'à présent, l'initiative s'est avérée très populaire en Chine, où il est déjà courant pour les acheteurs de scanner les codes QR, suivie de l'Italie et de la France. Carrefour ne se concentre pas sur ce projet que sur ses propres marques, il a également travaillé avec Nestlé pour donner aux consommateurs un accès aux données de la blockchain pour sa purée de pommes de terre Mousline, leur permettant de voir qu'elle est uniquement fabriquée à partir de pommes de terre françaises[7].

2.5.2 Applications de la blockchain dans la chaîne d'approvisionnement des soins de santé

La chaîne d'approvisionnement pharmaceutique (PSC) comprend des fabricants de médicaments, des fournisseurs / grossistes de services logistiques, des prestataires de soins et des points de vente au détail.

Après l'emballage, les médicaments sont distribués par les fabricants à différents prestataires de services logistiques tiers (3PL), grossistes et autres distributeurs qui acheminent ensuite les médicaments vers les hôpitaux, les pharmacies et d'autres détaillants. À ce stade, les distributeurs doivent gérer les flux inversés de médicaments vers les fabricants en raison des retours et des rappels de produits dangereux, de sorte que les fabricants sont en mesure de traiter les médicaments retournés de manière appropriée.

L'accumulation de médicaments périmés peut potentiellement contaminer l'environnement et cela deviendra un danger pour l’être humain. Le médicament doit donc être identifié, et correctement éliminé au lieu d'être réutilisé ou recyclé. Cependant, les médicaments invendus ou indésirables, qui conservent encore leur efficacité, peuvent être redistribués, revendus ou donnés à des marchés subsidiaires dans les pays en développement, ou aux personnes qui n'ont pas les moyens d'acheter de nouveaux médicaments.

Arriver à développer une excellente chaîne d'approvisionnement qui assure une bonne coordination, des processus fiables et une visibilité, représente un défi de taille pour les fabricants. Cependant, récemment, des chercheurs étudient le potentiel de l'utilisation de blockchains pour suivre et tracer les transactions.

2.5.3 Applications de la blockchain et opportunités futures dans les transports

La technologie blockchain a le potentiel de révolutionner le transport, car elle peut redéfinir et repenser l'ensemble du système de gestion des transports, en permettant des opérations commerciales plus efficaces, augmentant ainsi les marges bénéficiaires. Les plates-formes compatibles avec la blockchain facilitent la coordination des documents d'expédition / d'emballage sur un grand livre distribué partagé dans l'écosystème de la chaîne d'approvisionnement du transport, rendant la saisie manuelle des données, ainsi que les formalités papier presque inutiles, et réduisant également la contrefaçon des documents. Les approbations et le dédouanement peuvent être plus rapides et plus efficaces et les délais de traitement des importations / exportations des marchandises peuvent être accélérés aux points de contrôle douanier en utilisant des contrats intelligents.

La blockchain offre des applications prometteuses dans les chaînes d'approvisionnement du transport. Certains d'entre eux sont donnés ci-dessous :

2.5.3.1 Monétisation des données

Continental et Hewlett Packard Enterprise ont lancé une plateforme de monétisation de données basée sur la blockchain dans le cadre d'un partenariat stratégique au profit de la chaîne d'approvisionnement du transport [16]. La plate-forme permet à de nouveaux services numériques d'améliorer la sécurité et la commodité du conducteur en permettant de partager les données collectées à partir des capteurs IoT (fournissant des services d'assistance au conducteur tels que les avertissements de circulation en temps réel, la localisation des parkings disponibles, etc.) sur un véhicule sur la route avec d'autres véhicules connectés. En attendant, la plateforme aide les constructeurs automobiles à monétiser leurs données et à différencier leurs marques. Bien que cette plate-forme en soit à ses débuts, une application similaire peut être considérée comme étant utilisée dans les plates-formes de flotte de camions [7].

2.5.3.2 Traitement efficace des réclamations d'assurance

Un avantage majeur de l'utilisation de la technologie blockchain pour le suivi du fret, est le traitement plus rapide des réclamations d'assurance, dans les cas où le fret a été perdu ou endommagé. Considérant que les données de suivi sur les blockchains sont fiables et traçables jusqu'à l'origine de la perte, les compagnies d'assurance peuvent traiter les causes de l'incident, le transporteur impliqué, le type de fret et la validité des réclamations plus

rapidement et plus facilement. Un exemple récent d'application est la première plateforme mondiale d'assurance maritime sur blockchain appelée Insurwave, elle exploite la technologie blockchain, la plate-forme d'analyse Microsoft Azure tout en utilisant les normes de données ACORD. Insurwave peut prendre en charge un demi-million de transactions et gérer le risque d'expédition pour plus de 1000 navires commerciaux, en connectant toutes les parties prenantes du processus d'assurance, y compris les tiers, les clients, les assureurs ainsi que les courtiers [7].

2.5.3.3 Suivi de l'historique des performances de la flotte et des véhicules

La technologie Blockchain offre à toutes les parties de la chaîne de transport une visibilité sécurisée, universelle et à la demande sur le mouvement des marchandises. Les parties peuvent suivre les performances de leurs unités de transport (camions, semi-remorques, remorques, conteneurs maritimes) en termes de taux de chargement, tels que les kilomètres de chargement complet. L'historique des performances et de la maintenance des unités de livraison conduit à un modèle de tarification et d'efficacité plus fiable.

2.5.3.4 Normes de données communes

En 2017, la Blockchain in Transport Alliance, appelée BiTA [11] a été créée pour rassembler les principales sociétés de technologie et de transport afin de développer et d'adopter un cadre commun et des normes de fret universelles pour les applications blockchain. BiTA compte plus de 500 membres du monde entier couvrant les secteurs du transport et de la logistique, des biens de consommation et de la technologie. BiTA cherche à favoriser l'adoption à l'échelle de l'industrie, de la technologie de la blockchain dans la logistique et le transport, pour standardiser la méthode de suivi des marchandises : comme l'enregistrement des demandes de propositions et de transactions, le paiement du carburant et la révision des prix, sans avoir besoin d'un processeur, de solutions de paiement et de règlement.

2.5.4 Applications de la blockchain dans l'approvisionnement au détail

La technologie Blockchain fournit une solution évolutive et immédiate pour le suivi et l'authentification des commandes. La surveillance des processus peut garantir que les produits parviennent aux consommateurs finaux en toute sécurité et intacts.

La plupart des projets de blockchain actuels dans l'espace de la chaîne d'approvisionnement de détail, utilisent des registres privés et sont basés sur une blockchain privée, de consortium ou même hybride.

En particulier, les grands détaillants créent des consortiums de chaînes de blocs avec des fournisseurs, des prestataires de services logistiques et d'autres partenaires de la chaîne d'approvisionnement, pour créer leurs propres plates-formes de chaînes de blocs à partir de zéro, qui ne sont pas accessibles à partir du réseau de chaînes de blocs. Les détaillants adoptent également ces plates-formes blockchain en utilisant des balises intelligentes (NFC / RFID / QR Code) pour assurer la visibilité ainsi que la traçabilité de l'ensemble de la gestion du cycle de vie des produits de détail.
Certaines des applications blockchain dans la chaîne d'approvisionnement au détail sont indiquées ci-dessous :

2.5.4.1 Visibilité de bout en bout de la chaîne d'approvisionnement

La résolution de la visibilité devient une condition préalable essentielle pour chaque partie du commerce de détail. IBM est l'une des entreprises technologiques à agir avec les détaillants pour développer des solutions blockchain pour résoudre la visibilité de la chaîne d'approvisionnement dans le cadre du programme IBM Food Trust.

2.5.4.2 Anti-contrefaçon

La blockchain peut répondre à ce défi : le système de grand livre crypté permet aux détaillants de créer ce que l'on appelle un « passeport numérique » pour les marchandises, afin de démontrer le mouvement des marchandises tout au long de l'acheminement, des producteurs, à la chaîne d'approvisionnement jusqu'aux magasins. La société de distribution américaine, Walmart, a testé des pilotes blockchain exécutés sur Hyperledger Fabric [17] avec la collaboration du programme IBM Food Trust et a bien progressé avec les cas d'utilisation de la blockchain pour détecter facilement la fraude ou les produits contaminés et identifier la source potentielle de maladies d'origine alimentaire.
Chaque partie de la blockchain représente une entité qui gère le produit en cours de stockage. Le produit de vente au détail infecté est détecté facilement et plus rapidement dans le magasin de détail, et la source du produit de vente au détail est également identifiée rapidement et de manière fiable.

2.6 Conclusion

Au cours de ce chapitre, nous avons pu constater quelques applications de la blockchain en matière de chaînes d'approvisionnement, et avons donné quelques exemples de cas réels

d’utilisation par des entreprises à travers le monde. Nous allons au cours du chapitre suivant, donner la conception de l’application que nous avons développée dans le cadre de notre projet de fin d’étude, et qui consiste en un système de mutualisation de transport.

Chapitre 3

Conception de l’application

3.1 Introduction

Après avoir au cours des deux chapitres précédents donné un descriptif de la technologie blockchain ainsi que de ce qu’elle peut apporter comme avantages pour les différents types de supply chain, le chapitre qui suit est consacré aux étapes fondamentales de la conception de notre système d’expédition des produits. Pour la modélisation et la conception de notre application, nous avons choisis de modéliser avec le formalisme UML qui s'exprime par l'utilisation des diagrammes, ainsi que le processus UP (Unified Process ou le Processus unifié) comme démarche d’analyse.

3.2 Problématique traitée au cours de notre projet

Aujourd’hui, le cycle de transport de marchandises routier fonctionne sur une multitude d’échanges d’informations et de documents papiers à partir de la prise de commande jusqu’à la livraison.

Ce cycle est ralenti par la complexité et le volume de document papier à traiter, la communication des informations des documents se fait d’un point à l’autre sans vision globale des partie prenantes : transporteurs, expéditeur, autorité de contrôle et les clients. Ce circuit rend l’information difficilement accessible et peu fiable.

De ce fait, la technologie blockchain permet de créer un maillage global composé d’un registre partagé, archivé et sécurisé, dont l’intégralité des données sera garantie et accessible immédiatement à toutes les parties prenantes. Concrètement, le circuit des marchandises sera suivi par l’expéditeur, les transporteurs et les clients en temps réel, étape par étape, afin qu’ils puissent mieux se synchroniser.

Comme nous l'avons mentionné lors des chapitres précédents, la blockchain est une solution au problème de la sécurité et de la confidentialité des données, car la blockchain permet de décentraliser le stockage des données et ainsi d'augmenter le niveau de sécurité. Dans notre projet nous allons utiliser la blockchain pour son avantage en termes de facilité de traçabilité. En effet, grâce à elle, il est possible de suivre le parcours du transport de produit tout au long de la chaîne et en temps réel.

Notre application concerne la dernière phase avant que le consommateur final (client) ne reçoive son produit commandé. Plus précisément l'expédition des produits par des transporteurs. Nous avons pour but de garantir la traçabilité des produits. Le client et le transporteur pourront consulter l'état du transport du produit, par exemple : que le produit X est transporté par le transporteur Y et est destiné au client Z. Enfin, pour réaliser cette application nous allons utiliser un contrat intelligent qui va s'exécuter lorsque certaines conditions seront rencontrées. Nous avons trois (3) types d'utilisateurs dans notre système : l'expéditeur, les transporteurs et les clients. Seul l'expéditeur possède un compte lui permettant d'ajouter de nouveaux transporteurs ou produits. De plus, il associe à chaque produit un transporteur valide (libre). Quant aux transporteurs et aux clients, ils vont juste consulter l'état du transport du produit.

3.3 Le scénario descriptif pour notre système

Dans cette section, nous allons décrire notre système au travers d'un scénario d'utilisation. Avant de commencer nous pouvons imaginer que l'expéditeur et les transporteurs travaillent dans une entreprise de transport de produits, ou dans un magasin de vente en ligne par exemple. Dans notre système, nous allons traiter seulement la partie relative à l'expédition. Nous ne sommes pas concernés par les étapes antérieures (par exemple l'étape de la commande d'un produit par un client). En premier lieu, nous avons l'expéditeur qui joue le rôle d'un administrateur dans le système. Lorsqu'un nouveau transporteur est recruté dans l'entreprise, l'expéditeur l'ajoute à la blockchain (lui crée un compte), à l'aide d'un formulaire qui contient ses données. Ensuite, lorsqu'un client commande un produit, l'expéditeur va ajouter le produit au système, mais à condition qu'il n'existe pas déjà. Après coups, l'expéditeur va envoyer le produit au client, en affectant un transporteur a un produit. L'expéditeur devra prendre certains critères en compte avant d'affecter un produit à un transporteur. Il devra commencer par les produits urgents, et choisir le transporteur selon les conditions suivantes :

- Le transporteur doit être libre.
- Le transporteur doit satisfaire plusieurs conditions, par exemple le poids du produit transporté ne dépassant pas le poids maximal transporté par le transporteur.

Pour que l'expéditeur puisse choisir un transporteur qui convient, il devra consulter la liste des transporteurs et décider. Quand un transporteur est affecté à un produit, son statut change et devient occupé.

Le but de notre système est de réaliser la traçabilité des produits lors de leur acheminement. Les transporteurs peuvent consulter quel produit ils peuvent transporter et a qui est ce qu'il est destiné. Les clients quant à eux, peuvent savoir où en est leur commande et qui est ce qui la prend en charge.

3.4 Méthodes d'analyse et de conception

Après avoir dans la section précédente décrit notre application et donné un scénario d'utilisation, nous allons dans celle qui suit, la concevoir et la modéliser.

3.4.1 Spécification et analyse des besoins

Notre application devra satisfaire les besoins fonctionnels du système et les besoins non fonctionnels qui amélioreront sa qualité logicielle.

- **Les besoins fonctionnels**

Cette application doit couvrir principalement les besoins fonctionnels suivants :

- Ajout des Transporteurs
- Ajout des Produits
- Affecter un transporteur à un produit
- Affichage de la liste de Transporteurs/Produits et l'état des produits

- **Les besoins non fonctionnels**

A part les besoins fondamentaux, notre système doit répondre aux critères suivants :

- **Authentification :** Cette opération permet à l'expéditeur d'introduire son mot de passe afin d'accéder au système, cela permet d'assurer la sécurité.

- **Utilisabilité :** Le système doit offrir à l'utilisateur une interface simple et facile à utiliser.
- **Disponibilité :** Le système doit garantir l'accès à l'utilisateur aux résultats finals.
- Garantir l'intégrité et la cohérence des données à chaque mise à jour et à chaque insertion.

➢ **L'identification des acteurs**

Dans notre système, nous avons identifié trois (3) acteurs comme illustré dans la figure 10 ci-dessous :

- L'expéditeur désigne la personne chargée d'affecter des produits à des transporteurs pour la livraison au client.
- Le Transporteur : désigne la personne qui transporte un produit en utilisant un moyen de transport.
- Le Client : c'est le destinataire final de produit.

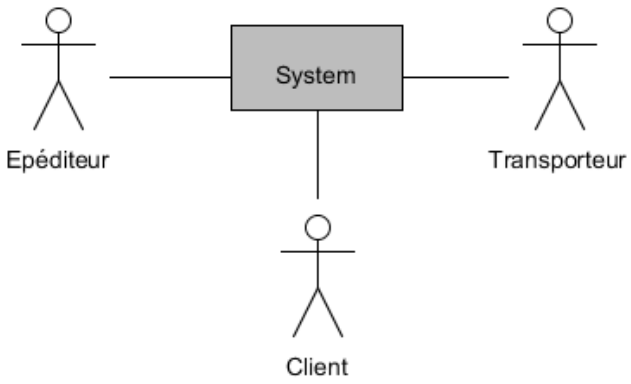

Figure 10-Diagramme de Contexte

3.4.2 Expression des besoins

Nous allons à présent présenter quelques diagrammes de modélisation, que nous avons jugé importants pour la compréhension du fonctionnement de notre système.

- Le diagramme de **cas d'utilisation** pour exprimer les besoins des utilisateurs.
- Le diagramme de **séquence** pour la vue des processus du système.
- Le diagramme de **classe** pour la vue logique du système.

3.4.2.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation est utilisé pour donner une vision globale du comportement fonctionnel du système. Il permet de structurer les besoins des utilisateurs et les objectifs du système. La figure 11 suivante montre le diagramme de cas d'utilisation global de notre application.

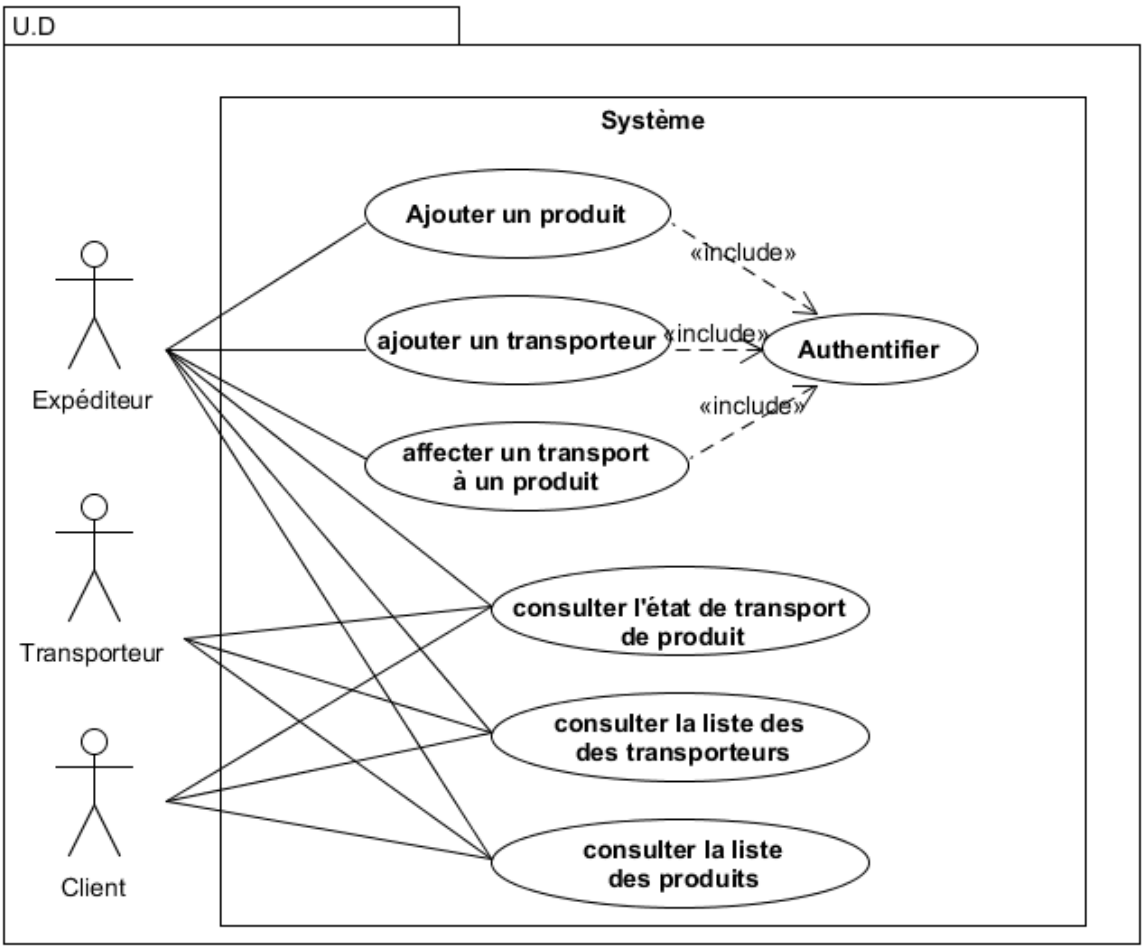

Figure 11-Diagramme de cas d'utilisation global

Dans la partie qui suit, nous allons donner une série de tableaux pour décrire les différents cas d'utilisation de notre application :

- **Description du cas « Authentifier »**

Tableau 1-Description du cas "Authentification"

Nom	**Authentifier**
Acteur	Expéditeur
Description du cas	Permettre à l'expéditeur de s'authentifier pour pouvoir accéder à son compte dans l'application.
Données d'entrées	Nom d'utilisateur, mot de passe
Scénario	**Nominale :** 1. L'utilisateur accède à l'application 2. Le système demande à l'utilisateur de choisir entre : Expéditeur ou Transporteur/Client 3. L'expéditeur saisit son nom d'utilisateur et mot de passe 4. Le système vérifie la saisie des données 5. Le système vérifie l'existence de l'utilisateur 6. Le système renvoie l'utilisateur à son compte **Erreur :** Erreur de saisie, utilisateur inexistant : le système affiche un message d'erreur.
Sortie	Expéditeur authentifié

- **Description du cas « Ajouter un Transporteur / Ajouter un Produit »**

Tableau 2-Description du cas "Ajouter un Transporteur / Ajouter un Produit "

Nom	**Authentifier**
Acteur	Expéditeur
Description du cas	● Permettre à l'expéditeur d'ajouter le Transporteur dans la liste des Transporteurs ● Permettre à l'expéditeur d'ajouter le Produit dans la liste des Produits
Données d'entrées	Transporteur/ Produit
Scénario	**Nominal** : 1. L'expéditeur saisit les informations sur le transporteur/le produit et valide l'opération de l'ajout 2. Le système vérifie la saisie des données 3. Le système vérifie l'existence du Transporteur/Produit 4. Le système ajoute le Transporteur/Produit à la Blockchain 5. Le système affiche un message de validation **Erreur :** Erreur de saisie, Transporteur/Produit déjà ajouter : le système affiche un message d'erreur
Sortie	Transporteur/Produit ajouté avec succès

- **Description du cas « Affecter un Transporteur à un Produit »**

Tableau 3-Description du cas "Affecter un Transporteur à un Produit "

Nom	**Authentifier**
Acteur	Expéditeur
Description de cas	Permettre à l'expéditeur d'affecter à chaque produit un Transporteur libre pour le transporter à sa destination.
Données d'entrées	Une liste des Transporteurs
Scénario	**Nominal** : 1. Le système affiche une liste des transporteurs 2. L'expéditeur choisi un transporteur parmi la liste selon les conditions de transport du produit 3. L'expéditeur valide son choix 4. Le système affiche un message de validation **Erreur :** Transporteur occupé : le système affiche un message d'erreur
Sortie	Transporteur affecter à un Produit

- **Description du cas « Consulter l'état de transport de produits »**

Tableau 4-Description du cas "Consulter l'état de transport de produits "

Nom	**Authentifier**
Acteur	Transporteur/Client /Expéditeur
Description du cas	● Permettre à Transporteur/Client/Expéditeur de consulter l'état de transport du produit
Données d'entrées	Un Transporteur affecté à un Produit
Scénario	**Nominal** : Le système affiche l'état de transport.
Sortie	Etat du transport consulté par Transporteur/Client/Expéditeur

- **Description du cas « Consulter liste des transports / produits »**

Tableau 5-Description du cas « Consulter liste des transports / produits »

Nom	**Authentifier**
Acteur	Transporteur/Client /Expéditeur
Description de cas	● Permettre à Transporteur/Client/Expéditeur de consulter liste des transporteurs / produits
Données d'entrées	L'existence des transporteurs / produits

Scénario	**Nominal** : Le système affiche la liste des transporteurs / produits.
Sortie	La liste des transporteurs/produits consulter par Transporteur/Client/Expéditeur

3.4.2.2 Diagramme de séquence

Les diagrammes de séquences sont la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique dans la formulation UML.

- **Diagramme de séquence d'Authentification**

La figure 12 ci-dessous représente le Diagramme de séquence d'Authentification

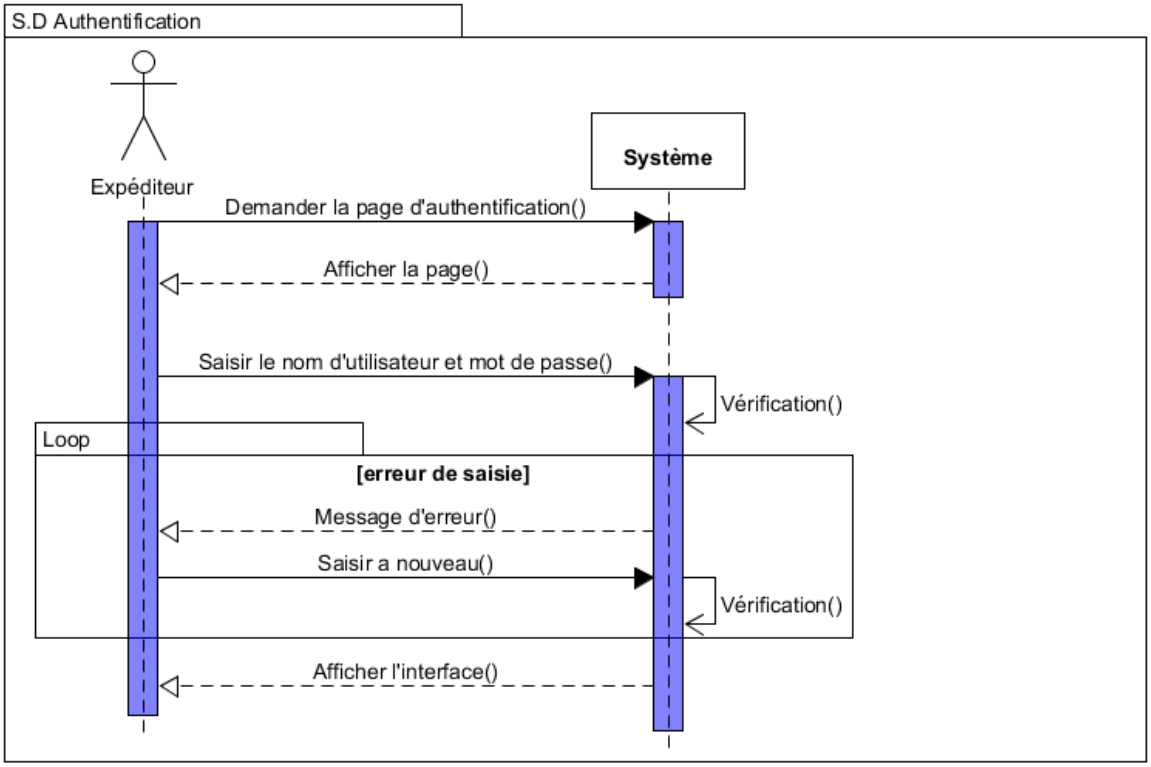

Figure 12-Diagramme de séquence d'Authentification

➢ **Diagramme de séquence pour ajouter produit/transporteur**

La figure 13 ci-dessous représente le diagramme de séquence pour ajouter produit/transporteur

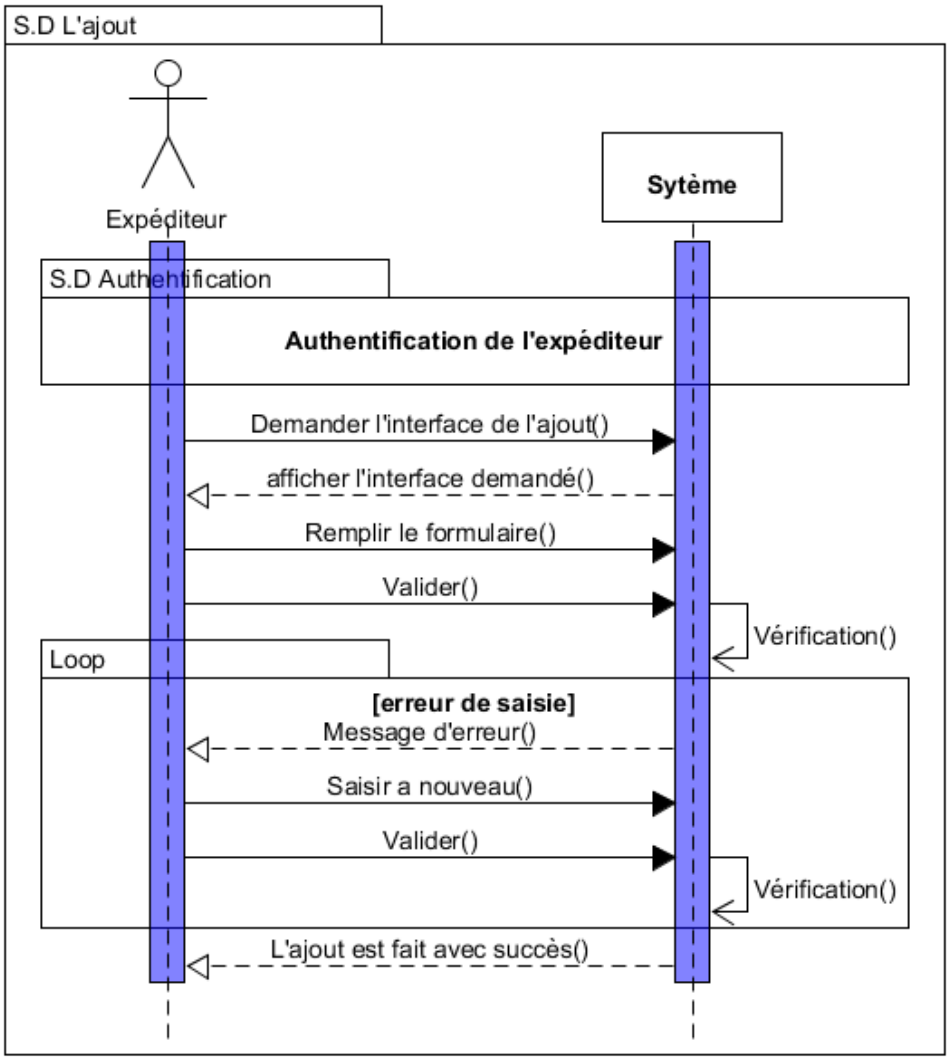

Figure 13-Diagramme de séquence pour ajouter produit/transporteur

➢ **Diagramme de séquence pour l'affectation du transporteur à un produit**

La figure 14 ci-dessous représente le diagramme de séquence pour l'affectation du transporteur à un produit

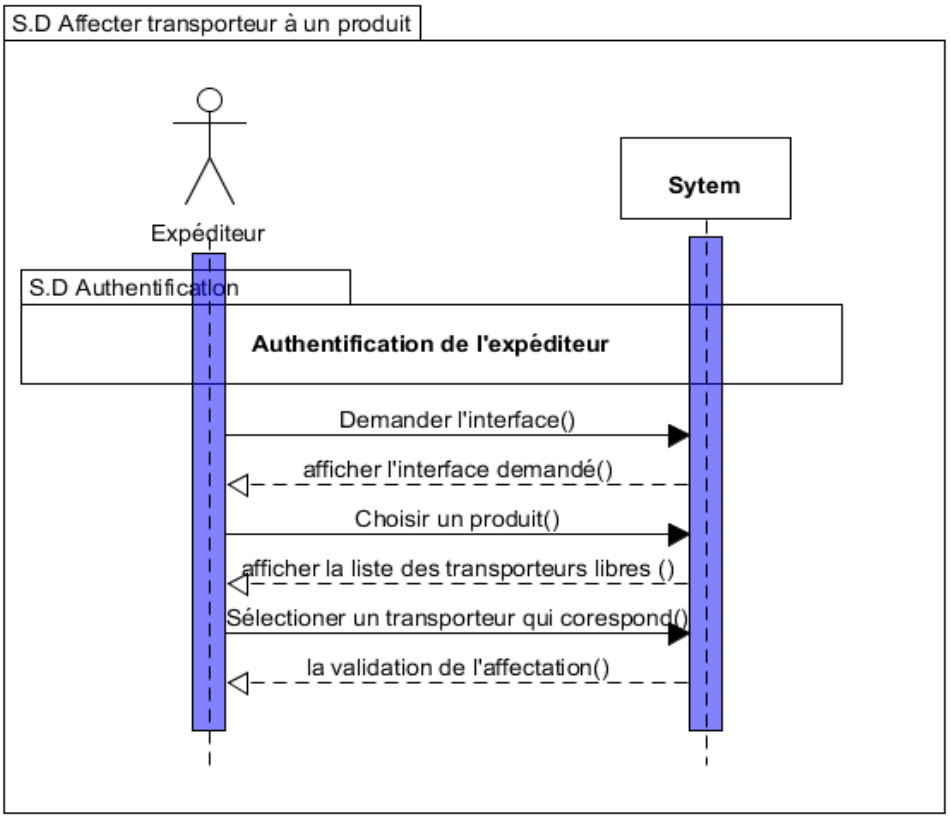

Figure 14-Diagramme de séquence pour l'affectation du transporteur à un produit

3.4.2.3 Diagramme de classe

Un diagramme de classes fournit une vue globale d'un système en présentant ses classes, interfaces et collaborations, ainsi que les relations entre elles. Les diagrammes de classes sont statiques : ils affichent ce qui interagit mais pas ce qui se passe pendant l'interaction. La figure 15 ci-dessous représente le diagramme de classe de notre application.

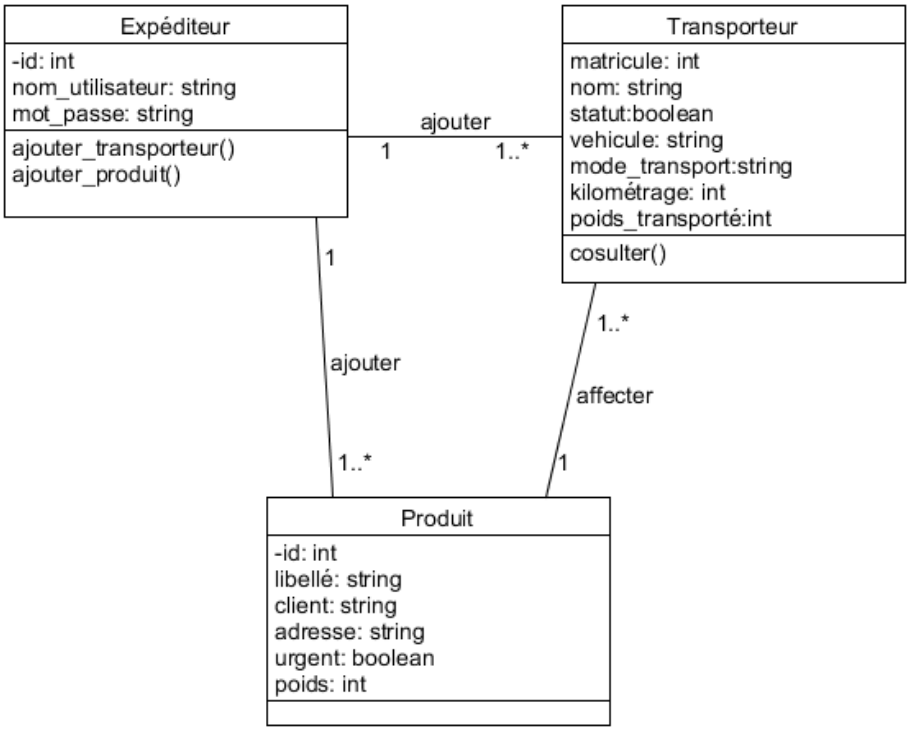

Figure 15-Diagramme de classe

3.5 Conclusion

Après avoir mis le projet dans son cadre et après avoir mis en place une démarche de développement, nous avons pu concevoir une application pour l'expédition de produit par des transporteurs en nous basant sur les diagrammes du formalisme UML, à savoir : le diagramme de cas d'utilisation, le diagramme de séquences et le diagramme de classes. Le produit obtenu est un modèle graphique prêt à être codé.

Nous pouvons maintenant étudier en détail les outils et les langages utilisés durant la phase de construction. Cette partie fera l'objet du prochain chapitre.

Chapitre 4

Réalisation de l’application

4.1 Introduction

Après la partie conception réalisée lors du troisième chapitre, celui-ci est consacré à la réalisation et à la mise en œuvre de notre application d’expédition des produits par des transporteurs. Nous allons présenter les outils de développement adoptés, à savoir : la Blockchain Ganache, les langages de programmation Solidity et JavaScript, le Framework Bootstrap ainsi que l'environnement de développement Visual-Studio-Code et MetaMask. Enfin nous allons montrer les principales interfaces de l'application, et discuter de la solution que nous avons implémentée.

4.2 Outils et environnements de développement

Dans cette section, nous allons présenter les outils informatiques que nous avons utilisés lors du développement de notre application.

4.2.1 Truffle

C’est un framework permettant de créer, tester et déployer des applications sur le réseau Ethereum, Nous pouvons créer différents smart contrats en utilisant un Atom, là où on va coder (éditeur de texte). Truffle fonctionne sur invite de commande.

4.2.2 Ganache

Ganache est une blockchain personnelle pour le développement rapide d'applications distribuées Ethereum et Corda. Nous pouvons utiliser Ganache tout au long du cycle de développement ; afin de développer, déployer et tester nos dapps (applications décentralisées) dans un environnement sûr et déterministe.

Ganache est disponible en deux versions : une interface utilisateur et une interface de ligne de commande. Ganache UI est une application de bureau prenant en charge les technologies

Ethereum et Corda. L'outil de ligne de commande, ganache-cli (anciennement appelé TestRPC), est disponible pour le développement Ethereum. Toutes les versions de Ganache sont disponibles pour Windows, Mac et Linux.

4.2.3 Metamask

C'est une application web, qui permet l'interaction d'applications web avec la blockchain Ethereum sans exécuter un nœud Ethereum complet. Metamask nous permet d'avoir un compte rendu de nos adresses, et va injecter web3 qui est un framework javascript qui nous permet d'interagir avec la blockchain.

Un utilisateur doit avoir un nœud connecté, il s'agit d'une extension de navigateur chrome.

4.2.4 Bibliothèque web3

Pour développer une application web qui pourra interagir avec la blockchain Ethereum, nous devons utiliser une bibliothèque JavaScript appelée web3.js. Celle-ci permet d'entrer l'adresse d'un Smart Contrat et d'appeler les fonctions qu'il contient, en passant éventuellement les paramètres nécessaires.

L'avantage d'utiliser la bibliothèque Web3 est que vous avez un contrôle total non seulement sur votre clé privée, mais également sur chaque interaction que vous effectuez avec Ethereum.

4.2.5 Bootstrap

Bootstrap est un Framework développé par l'équipe du réseau social Twitter. Proposé en open source (sous licence MIT), ce Framework utilise les langages HTML, CSS et JavaScript, et fournit aux développeurs des outils pour créer un site facilement.

4.2.6 Visual Studio Code

Visual Studio Code est un éditeur de code source léger mais puissant, qui est disponible pour Windows, macOS et Linux. Il est livré avec un support intégré pour JavaScript, TypeScript et Node.js et dispose d'un riche écosystème d'extensions pour d'autres langages (tels que C ++, C #, Java, Python, PHP, Go) et des environnements d'exécution (tels que .NET et Unity)[18].

4.2.7 Solidity

C'est le langage de programmation de la plateforme d'applications décentralisées la plus connue (et la plus utilisée) : Ethereum, qui s'approche du javaScript.

Solidity permet de coder des smart contracts. Cependant, Solidity va plus loin que le langage utilisé sur Bitcoin (script) et permet de réaliser des transactions plus complexes, car il présente une différence majeure [19].

4.2.8 JavaScript

JavaScript est un langage de programmation qui permet d'implémenter des mécanismes complexes sur une page web. À chaque fois qu'une page web fait plus que simplement afficher du contenu statique — afficher du contenu mis à jour à des temps déterminés, des cartes interactives, des animations 2D/3D, des menus vidéo défilants, etc... ,JavaScript a de bonnes chances d'être impliqué.

4.3 Présentation des interfaces de développement

Lors de cette section, nous présenterons les différentes interfaces graphiques de notre application.

4.3.1 La fenêtre d'interface « Page d'Accueil »

La fenêtre représentée dans la figure 16 ci-dessous représente la page d'accueil principale de notre application. Elle permet aux utilisateurs (Expéditeur et Transporteur/Client) de se diriger vers la page d'accueil correspondant à chacun d'entre eux.

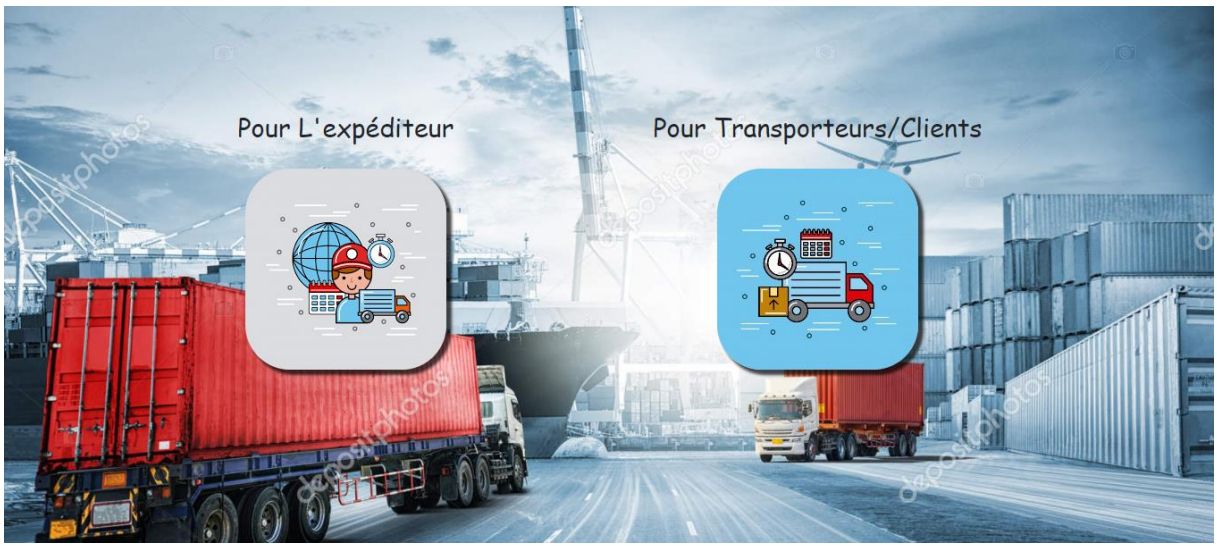

Figure 16-La fenêtre « Page d'Accueil »

4.3.2 Les fenêtres d'interfaces « Pour l'Expéditeur »

4.3.2.1 La fenêtre « Authentification »

Seul l'expéditeur doit s'identifier pour accéder à sa page d'accueil. La figure 17 ci-dessous représente la fenêtre d'authentification de l'expéditeur.

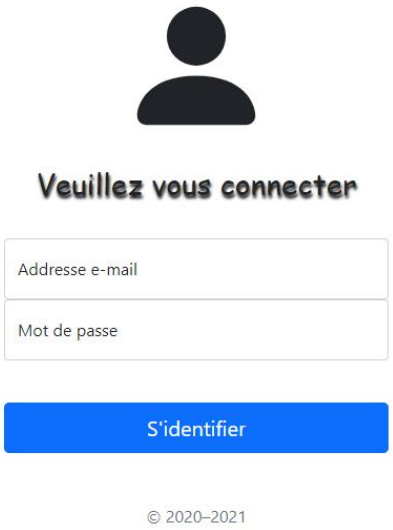

Figure 17-La fenêtre d'interface « Authentification »

4.3.2.2 La fenêtre « Page d'accueil expéditeur»

La fenêtre d'interface « Accueil Expéditeur » se compose de trois boutons (fonctionnalités) : Ajouter transporteur, Ajouter produit et Affecter un transporteur pour chaque client. Elle est représentée par la figure 18 ci-dessous.

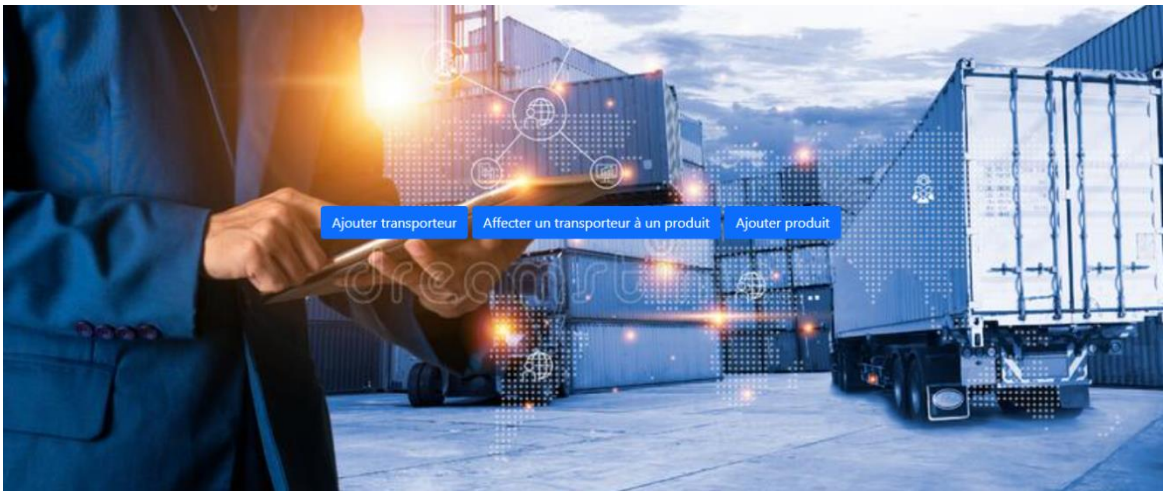

Figure 18-L'interface « accueil Expéditeur »

a- « Ajouter transporteur »

En cliquant sur le bouton **« Ajouter transporteur »** (voir figure 18)**,** une autre interface s'affiche (fenêtre d'interface d'Ajout des transporteurs) et cela permet à l'expéditeur d'inscrire les nouveaux Transporteurs. La figure 19 ci-dessous illustre la fenêtre ajout des transporteurs.

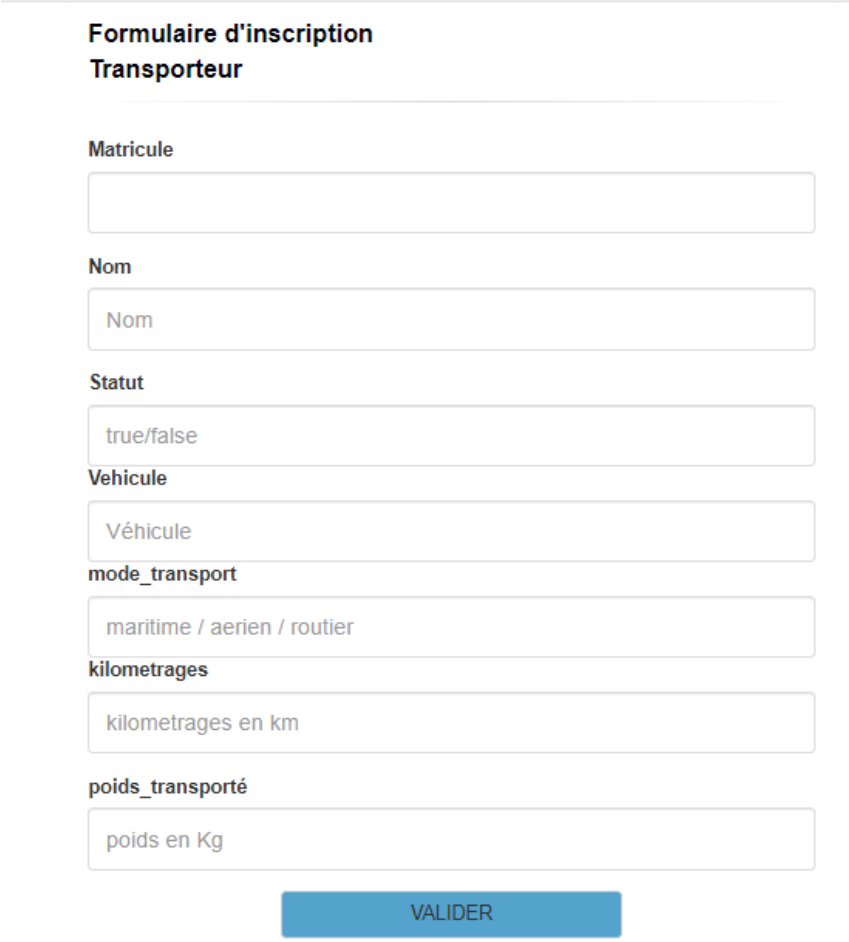

Figure 19-Interface d'Ajout des transporteurs

b- « Ajouter produit »

En cliquant sur ce bouton (voir figure 18), une autre fenêtre s'affiche (fenêtre d'interface d'Ajout des produits illustrée dans la figure 20 ci-dessous) et cela permet à l'expéditeur d'inscrire les nouveaux Produits.

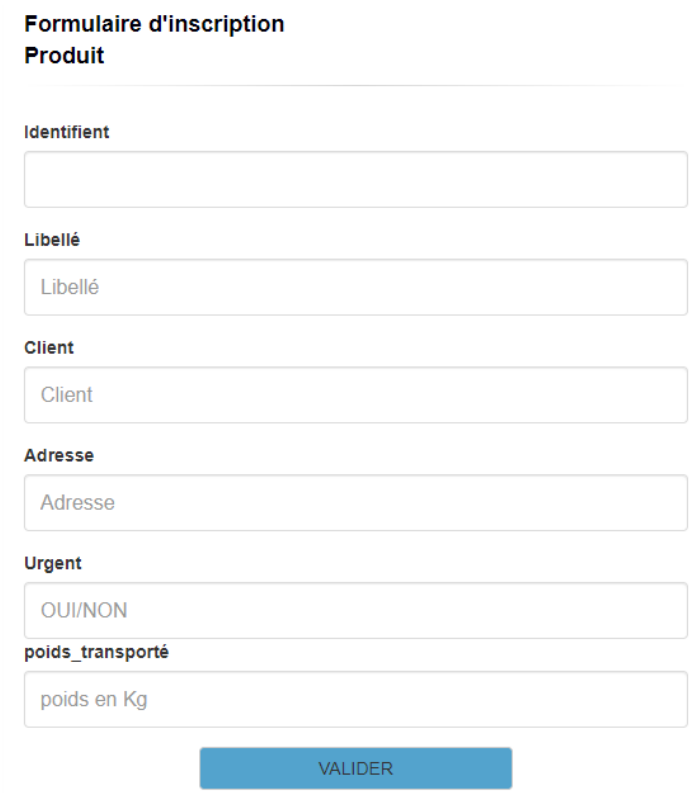

Figure 20-fenêtre d'interface d'Ajout des produits

c- « Affecter un transporteur pour chaque produit »

Une fois que l'expéditeur reçoit des produits pour les faire transporter (livraison), il doit sélectionner un transporteur parmi la liste des transporteurs libres qui convient au transport du produit, en parallèle lors de validation du choix le statut de transporteur va être changé à « false ». Cette fenêtre est illustrée par la figure 21 ci-dessous. (Le bouton Affecter un transporteur pour chaque produit se trouve dans la fenêtre représentée dans la figure 18).

Figure 21-Fenêtre d'interface d'affectation d'un transporteur à un produit

4.3.3 Les fenêtres d'interfaces « Pour Transporteur/Client »

4.3.3.1 La fenêtre « Page d'accueil transporteur/client»

La fenêtre « Accueil Transporteur/Client » se compose de trois boutons (fonctionnalités) : Consulter liste des transporteurs, Consulter liste des Produit et Consulter l'état du transport de produit (figure 22).

Figure 22-Accueil Transporteur/Client

a- Consulter la liste des produits

La fenêtre illustrée dans la figure 23 s'affiche en cliquant sur le bouton « **Consulter la liste des produits »** (bouton contenu dans la fenêtre illustrée par la figure 22) :

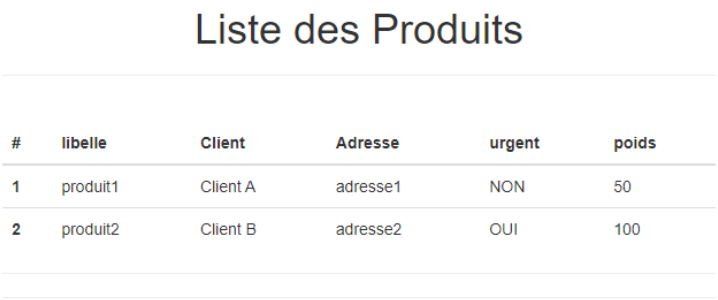

Figure 23-Fenêtre liste des produits

b- Consulter la liste des transporteurs

En cliquant sur le bouton **« Consulter la liste des transporteurs »** (contenue dans la fenêtre illustrée par la figure 22)**,** une interface s'affiche (fenêtre d'interface de la liste des transporteurs). La figure 24 ci-dessous l'illustre.

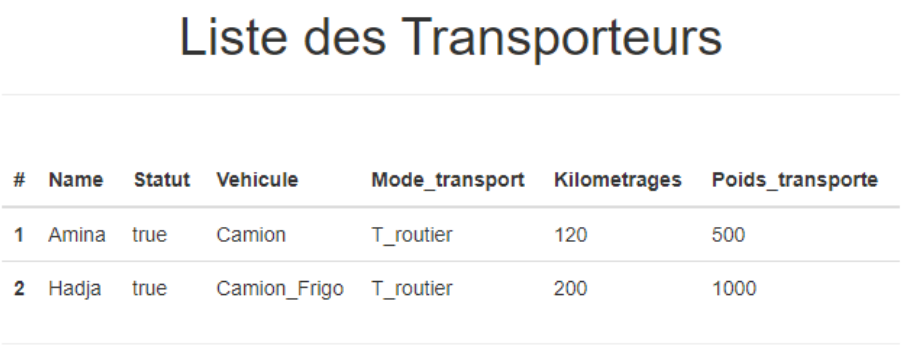

Figure 24-Fenêtre liste des transporteurs

c- Consulter l'état de produit transporté

En cliquant sur le bouton « **Consulter l'état de produit transporté »** (contenue dans la fenêtre illustrée par la figure 22)**,** une interface s'affiche (fenêtre d'interface de l'état du produit transporté) dans laquelle le client et le transporteur peuvent suivre quel est le produit à transporter, par qui et à qui est-il destiné, ce qui représente le but de notre application. La figure 25 ci-dessous l'illustre.

Figure 25-L'état du transport de produits

4.4 Discussion de notre solution

La partie qui va suivre a été consacrée pour répondre aux différentes questions qui ont été ou peuvent être posées lors du développement ou de l'examen de notre application « L'expédition des produits via la blockchain ».

Question 1 : Comment est garanti la traçabilité transparente dans notre application blockchain ?

Vous pouvez voir la gestion de la traçabilité en vérifiant l'ensemble des blocs dans ganache, où vous trouvez que chaque transporteur et/ou produit créé par l'expéditeur est défini par un bloc daté et non altéré.

Voici ci-dessous dans la figure 26 une partie de cet ensemble :

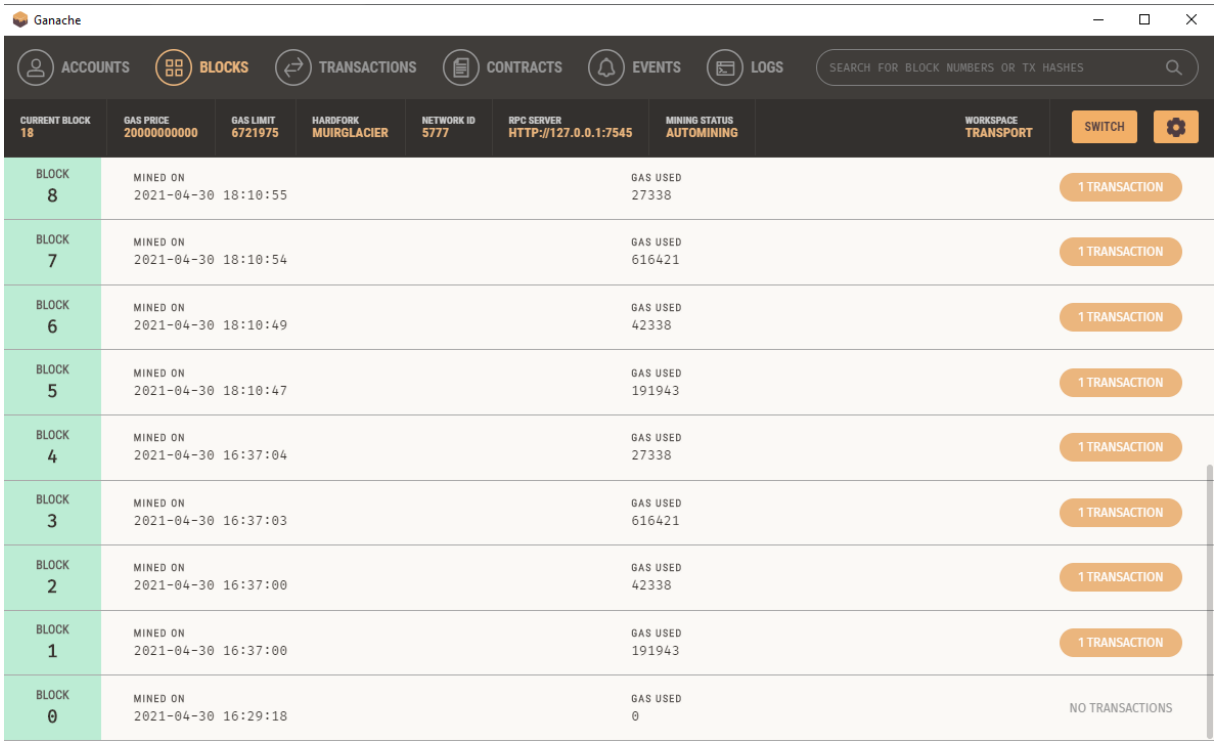

Figure 26-les blocs de Ganache

La blockchain est l'outil qui permettra de révolutionner la traçabilité du transport de produit : elle garantit de façon quasi immédiate une traçabilité à moindre coût. En effet, c'est une sorte de base de données sans contrôle d'une autorité supérieure et dont la sécurité est garantie par des techniques de cryptographie numérique. La base de données est alimentée par l'expéditeur qui rentre lui-même les informations qu'ils souhaitent stocker (liste des transporteurs et liste des produits). Chaque bloc de données est daté et connecté à celui produit avant lui dans la même chaîne. Avant de passer à celui d'après, le contenu de chaque bloc doit être contrôlé par l'expéditeur et validé. Une fois ajouté, un bloc de données ne peut être ni modifié ni supprimé. L'ensemble crée donc une chaîne de données datées et inaltérables. C'est en ayant recours à cet outil qu'il est désormais possible de sécuriser les transactions, de déterminer par qui le produit est transporté et à qui est destiné en quelques secondes mais surtout de garantir la fiabilité des informations communiquées.

Question 2 : Quelles sont les contraintes pour utiliser notre application dans un environnement réel ?

Pour utiliser notre application dans un environnement réel, il est nécessaire de se procurer des ethers afin de couvrir les frais de déploiement du contrat intelligent, ainsi que l'opération de l'expédition des produits (frais de transaction).

Question 3 : Quelles sont les limites de notre application ?

L'une des principales limites de notre application est le fait que la blockchain est en local. Nous sommes donc obligés d'utiliser le même ordinateur (la même machine) pour pouvoir expédier les produits.

De plus, comme nous venons de le mentionner dans le paragraphe précédent, il faut des ethers pour déployer nos contrats intelligents et les frais de transactions. Ce qui constitue un certain coup financier pour l'utilisation de cette application. Cependant, toutes les applications utilisant une blockchain Ethereum (même dans les autres domaines d'application) auront ces mêmes contraintes en plus de celle d'avoir des mineurs près à miner afin de valider leurs transactions. Ce qui, de notre point de vue, ne constitue pas une limite, mais un coût que les concepteurs devront prendre en compte avant l'adoption d'une telle application et le comparer avec le bénéfice qu'ils pourront tirer en utilisant une application blockchain. Ils décideront par la suite si c'est intéressant pour eux financièrement d'utiliser une telle application.

Question 4 : Que faudrait-il pour que la blockchain ne soit plus installée en local mais de façon distribuée ?

Pour que la blockchain ne soit plus installée en local, il suffit de changer le serveur local (Ganache dans notre cas) avec un autre proposé par MetaMask par exemple : Ropsten, Kova, etc.

Question 5 : Une blockchain a besoin de mineurs pour qu'elle puisse valider ses transactions et fonctionner normalement. Il faut donc une méthode pour inciter des mineurs à miner dans une blockchain comme la nôtre. Comment proposez-vous de les inciter à miner ?

Afin d'inciter les mineurs à miner, nous pouvons par exemple :

Attribuer au mineur un certain pourcentage sur chaque transaction validée. Le minage constitue l'un des principaux problèmes pour l'adoption d'applications basées sur la blockchain. En effet le matériel nécessaire ainsi que le coût énergétique élevé risquent de rebuter les mineurs potentiels s'ils ne trouvent pas d'intérêts financiers dans l'opération.

Question 6 : Quelles seraient les améliorations futures pour notre application ?

Comme perspectives futures pour notre application, nous proposons :

- D'ajouter un serveur mail afin de notifier les transporteurs et le client (une fois que l'expéditeur affecte un transporteur à un produit, le transporteur reçoit une notification qu'un produit lui a été attribué, de même une notification au client que son produit est transporté).
- L'envoie d'un lien unique après l'inscription de l'expéditeur par l'administrateur afin d'initialiser son mot de passe.

- D’ajouter un deuxième facteur d’authentification pour l’expéditeur. Ceci permettra d’ajouter plus de sécurité dans l’application.
- Enfin bien sûr, l’élargissement de notre application pour qu’elle puisse prendre en charge d’autres types d'expédition de produits plus complexes.

4.5 Conclusion

Nous avons présenté dans ce chapitre le côté implémentation de notre projet en spécifiant les différents outils utilisés, les langages et l’environnement de développement de notre application ainsi que ses fenêtres d’interface. Nous avons ensuite discuté de notre application et apporté des réponses à des questions qui pourraient être posées.

Conclusion Générale

La blockchain est une technologie qui crée des opportunités spécifiques aux yeux de différents acteurs. Certains la perçoivent comme un outil capable de désintermédier la confiance avec la création d'applications décentralisées, leur permettant d'interagir les uns avec les autres et d'échanger de la valeur sans aucun intermédiaire de confiance. D'autres la voient comme un outil de libération ou comme un moyen de promouvoir la collaboration entre différents acteurs, grâce à des mécanismes de coordination et de consensus distribués. Quelles qu'en soient les raisons, tous sont d'accord sur un même point : la blockchain est une technologie de rupture, susceptible de transformer l'ordre économique, social et politique de notre société. Cette technologie est née avec le bitcoin, qui reste aujourd'hui l'application majeure et l'exemple le plus remarquable de sa mise en œuvre. Il est cependant apparu qu'à côté de la réussite de cette blockchain particulière, bien des variantes sont possibles, certaines plus complexes, plus puissantes (Ethereum), certaines plus simples (les blockchains privées). C'est un volumineux ensemble de méthodes et d'applications qui est en train de naître et que les spécialistes de ce domaine sont en train de perfectionner en s'inspirant de près ou de loin de la construction inattendue de Satoshi Nakamoto. Il ne fait aucun doute que le rôle de cette nouvelle technologie sera déterminant dans le monde des réseaux, où les outils permettant de créer des échanges sécurisés d'informations, de valeurs et de confiance seront des clés du progrès.

A l'issue de ce projet, nous avons pu étudier et comprendre le principe de fonctionnement d'une blockchain, nous sommes également parvenus à concevoir et à implémenter une application de chaîne d'approvisionnement basée sur la Blockchain. Le but de l'utilisation de cette technologie est de garantir la traçabilité, la sécurité et la fiabilité.

Ce rapport décrit notre idée de la façon dont la technologie de la chaîne de blocs pourrait être utilisée pour mettre en œuvre un système d'expédition des produits sécurisé dans une entreprise de transport de produits.

Pour la réalisation de l'application nous avons choisi de modéliser avec le formalisme UML qui nous a permis d'identifier les différents acteurs, les possibilités du système et les

besoins des utilisateurs à l'aide des diagrammes détaillés. Nous avons par la suite utilisé la plateforme de développement Ethereum basée sur les contrats intelligents pour sa réalisation.

L'application que nous avons réalisée permet aux transporteurs de consulter quel produit ils peuvent transporter et à qui est ce qu'il est destiné. Les clients quant à eux, peuvent savoir où en est leur commande et par qui le produit est transporté. Le but de notre système est de réaliser la traçabilité des produits, lors de leur acheminement.

Comme possible améliorations de notre application, nous pourrions donner au client la possibilité de consulter en temps réel l'emplacement GPS de sa commande, proposer une application mobile pour le client ou le transporteur, ou enfin automatiser l'affectation des transporteurs.

Pour conclure, ce projet nous a permis d'apprendre encore plus et de développer nos connaissances et d'acquérir une expérience dans le domaine de la blockchain, et comment créer une application décentralisée (dapp) sur la blockchain ethereum à l'aide des contrats intelligents.

Bibliographies

[1] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », p. 9.

[2] J. Katz and Y. Lindell, Introduction to Modern Cryptography, Second Edition-, 2 édition. Boca Raton: Chapman and Hall/CRC, 2014.

[3] « National Institute of Standards and Technology | NIST ». https://www.nist.gov/.

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[5] P. Albitz and C. Liu, *DNS et BIND*. O'Reilly Media, Inc., 2002.

[6] L. Perlman, « A Model Crypto-Asset Regulatory Framework », Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3370679, mai 2019. doi: 10.2139/ssrn.3370679.

[7] N. Subramanian, A. Chaudhuri, and Y. Kayıkcı, *Blockchain and Supply Chain Logistics: Evolutionary Case Studies*. Springer Nature, 2020.

[8] N. Subramanian, A. Chaudhuri, and Y. Kayikci, « Basics of Blockchain », in *Blockchain and Supply Chain Logistics: Evolutionary Case Studies*, N. Subramanian, A. Chaudhuri, et Y. Kayıkcı, Éd. Cham: Springer International Publishing, 2020, p. 11-19. doi: 10.1007/978-3-030-47531-4_2.

[9] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Portfolio / Penguin, 2016.

[10] I. Heckmann, T. Comes, and S. Nickel, « A critical review on supply chain risk – Definition, measure and modeling », *Omega*, vol. 52, p. 119-132, avr. 2015, doi: 10.1016/j.omega.2014.10.004.

[11] A. Jabbari and P. Kaminsky, « Blockchain and Supply Chain Management », p. 13.

[12] B. G. Smith, « Developing sustainable food supply chains », *Philos. Trans. R. Soc. B Biol. Sci.*, vol. 363, n° 1492, p. 849-861, févr. 2008, doi: 10.1098/rstb.2007.2187.

[13] J. Schmidhuber, « Emerging Opportunities for the Application of Blockchain in the Agri-food Industry », août 2018.

[14] S. Kumar and E. M. Budin, « Prevention and management of product recalls in the processed food industry: a case study based on an exporter's perspective », *Technovation*, vol. 26, n° 5, p. 739-750, mai 2006, doi: 10.1016/j.technovation.2005.05.006.

[15] « Blockchain technology and its relationships to sustainable supply chain management: International Journal of Production Research: Vol 57, No 7 ».

[16] N. Subramanian, A. Chaudhuri, and Y. Kayıkcı, « Blockchain Applications and Future Opportunities in Transportation », in *Blockchain and Supply Chain Logistics: Evolutionary Case Studies*, N. Subramanian, A. Chaudhuri, et Y. Kayıkcı, Éd. Cham: Springer International Publishing, 2020, p. 39-48. doi: 10.1007/978-3-030-47531-4_5.

[17] « Hyperledger – Open Source Blockchain Technologies ». https://www.hyperledger.org/ (consulté le juin 07, 2021).

[18] « Documentation for Visual Studio Code ». https://code.visualstudio.com/docs.

[19] Solidity : Caractéristiques du langage d'Ethereum • BitConseil », *BitConseil*, août 22, 2019. https://bitconseil.fr/solidity-langage-ethereum/.