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 : **Réseaux et Systèmes**

Présenté par :

COULIBALY Moussa

THEME :

Traçabilité des produits alimentaires grâce à la blockchain

Soutenu le : 03 juillet 2022

Devant le jury composé de :

Adnane Laredj	Dr	Université de Mostaganem	Président
Miroud Mustapha	Dr	Université de Mostaganem	Examinateur
Bessaoud Karim	Dr	Université de Mostaganem	Encadreur
Abid Meriem	Dr	Université de Mostaganem	Encadreur

Année Universitaire 2021-2022

Résumé

Ce document présente l'application de la blockchain dans la mise en place de la traçabilité alimentaire. La traçabilité est le suivi des aliments, elle consiste à garder des traces qui aident à retrouver les produits et les causes des problèmes de non conformité, à faciliter la gestion de la production mais elle sert aussi de témoin pour les consommateurs qui veulent être rassurés sur l'authenticité et la fiabilité liées à leurs consommations. La blockchain est quand a elle un registre transactionnel distribué et décentralisé dont l'intégrité et la disponibilités des informations qu'elle contient est garantit.

La dégradation de l'opinion publique sur l'agroalimentaire prouve que le domaine n'est pas très satisfaisant du fait que ce ne sont pas les crises alimentaires qui ont manqués des années 1980 jusqu'au temps actuel, parmi lesquelles ont peut citer : la crise de la vache, le scandale des lasagnes de cheval, les grippes porcine, etc. Les consommateurs par conséquence demandent plus de preuve et de transparence envers les entreprises de production dans un cadre de maintient de la sécurité de consommations, ce qui pousse ces entreprises dans l'obligation de prouve la qualité de leurs productions, et ce qui sure c'est que la performance de ces systèmes reste toujours a discutés suite au problèmes de leurs mises en places de leurs maintenances, et de leurs impertinences.

Ce travail est dans le cadre de cette observation en proposant une solution pour les deux parties. Un système de traçabilité mise en place grâce à la blockchain qui permettrait une réelle transparence de la traçabilité aux consommateurs et de faire face à ces difficultés rencontrés par les entreprises de productions.

Mots clés : *Blockchain, signature numérique, transaction, traçabilité, supplychain, chaine de production, chaine logistique, contrat intelligent, consommateur, producteur, prestataire de service logistique.*

Abstract

This document presents the application of blockchain in the implementation of food traceability. Traceability is the monitoring of food, it consists in keeping traces which help to find the products and the causes of non-conformity problems, to facilitate the management of production but it also serves as a witness for consumers who want to be reassured about the authenticity and reliability linked to their consumption. The blockchain is a distributed and decentralized transactional register whose integrity and availability of the information it contains is guaranteed.

The deterioration of public opinion on the food industry proves that the field is not very satisfactory because it is not the food crises that have been lacking from the 1980s to the present time, among which we can cite : the cow crisis, horse lasagna scandal, swine flu, etc. Consumers therefore demand more proof and transparency towards production companies in a framework of maintaining consumer safety, which pushes these companies into the obligation to prove the quality of their productions, and what is sure is that the performance of these systems is still discussed following the problems of their implementation of their maintenance, and their impertinence.

This work is within the framework of this observation by proposing a solution for both parties. A traceability system set up thanks to the blockchain which would allow real transparency of traceability to consumers and to deal with these difficulties encountered by production companies.

Keywords : *Blockchain, digital signature, transaction, traceability, supplychain, production chain, supply chain, smart contract, consumer, producer, logistics service provider.*

Table des figures

Table des matières

Introduction général

Problématique

Des années 1980 à nos jours, les maladies d'origine alimentaire ont été connus massivement. En 2015, elles touchent plus de 91 millions de personnes uniquement en Afrique, et provoque le décès du tiers de ce chiffre. Les consommateurs du monde entier sont alertés pour leurs sécurités. Pourquoi après toutes ses années, la traçabilité n'est elle toujours pas efficace ? Une réponse est que les consommateurs sont censés faire confiance au lieu d'avoir leurs mains dans la surveillance de ce qu'ils consomment d'une part, et du fait que les entreprises qui gèrent cette surveillance, n'arrivent pas totalement à assurer d'autre part en raison des difficultés croisées dans le domaine, qui sont entre autre, la gestions des données récoltées, la non généralisation des flux d'informations dans la chaine d'approvisionnement et un manque de réglementation.

La blockchain est un registre de transaction disponible qu'en écriture, fonctionnant sur un réseau décentralisé et distribué. Cet registre à la sécurité infaillible se repose principalement sur des concepts cryptographiques et des protocoles connus pour tenir une chaine de bloc de transaction copiées sur l'ensemble des nœuds d'un réseau, dont ces nœuds suivent tous un mécanisme de consensus pour maintenir l'intégrité de cette chaine de bloc.

Guide du document

Le but de notre travail est de proposer une solution aux problèmes croisés dans la traçabilité alimentaire avec la technologie blockchain. Ce travail est divisé en 4 chapitre : en premier nous allons étudié la blockchain et son fonctionnement. Dans le chapitre 2, nous allons présenté la traçabilité et les problèmes rencontrés dans cet domaine. Dans le chapitre 3, nous allons présenté des systèmes de traçabilités pour nous situés. Par la suite nous allons définir notre système en fonction des avantages et inconvénient repérés dans ces systèmes. Dans le dernier chapitre nous allons mettre en œuvre notre système, en réalisant un DApp sur la blockchain ethereum.

Chapitre 1

Blockchain

1.1 Introduction

En 2008 la première technologie de blockchain est publiée par Satoshi Nakamoto, dans laquelle l'auteur affirme proposer une solution pour ≪permettre des paiements en ligne directs sans passer par une institution financière≫ . La technologie est utilisée dans le cadre financière, médicale ,traçabilité, et partout ou il peut y avoir une nécessite de tenir un registre.Cette popularité est due à sa prise en charge de plusieurs critères de sécurité comme son intégrité sans faille, sa disponibilité continue, etc. Dans ce chapitre nous voir ce qu'est la blockchain. Nous commencerons par énumérer ses dépendances puis nous présenterons son fonctionnement ainsi que sa structure. Pour finir, nous présenterons ses critères de sécurités, son extension et ces différents type.

La blockchain est sert une technologie récente, mais son fonctionnement est complément basé sur l'utilisation d'un ensemble d'algorithme et de concept facile qui date. Avant de la présentée nous allons commencé par ces notions qui sont nécessaires pour mieux comprendre une blockchain.

1.2 Rappel sur les concepts de cryptographie utilisés dans la blockchain

Il est évident de comprendre ces concepts enfin de les saisir le fonctionnement de la blockchain. Avant d'aller loin nous présentons ces concepts.

1.2.1 La cryptographie asymétrique

Pour s'échanger des messages avec la cryptographie symétrique, Alice et Bob doivent se mettre d'accord sur une clé, qui permettrait de chiffrer et de déchiffre les messages entre ces deux acteurs. Le problème est que ça va leur prendre beaucoup d'effort pour s'échanger cette clé en toute discrétion et continuer de la garder secrète, si ça ne concerne bien sûr que ces deux acteurs. Sinon il va falloir aussi que Bob garde secrète chaque clé qui le lie à chaque autre acteur qui échange avec lui, idem pour Alice.

Un alternative pour facilité leur tâche est de recourir à la cryptographique asymétrique *Fig 1.1* . Contrairement à la première, elle exige pour chacun de ces acteurs (Alice et bob) deux clés, *une clé privée* et *une clé publique* qui est générée à partir de la clé privée. Ils s'échangent les

clés publiques, et avec n'importe quelle autre entité d'ailleurs qui aura envie de leurs envoyer un message. Cette dernière n'a pas à reste secrète, car elle ne sert qu'a chiffrer un message, donc un attaquant qui intercepte un message chiffrer destiné à Alice doit avoir sa clé privée pour lire le contenu, et évidement une clé publique ne permet pas de remonter à la clé privée dont elle a été dérivée.

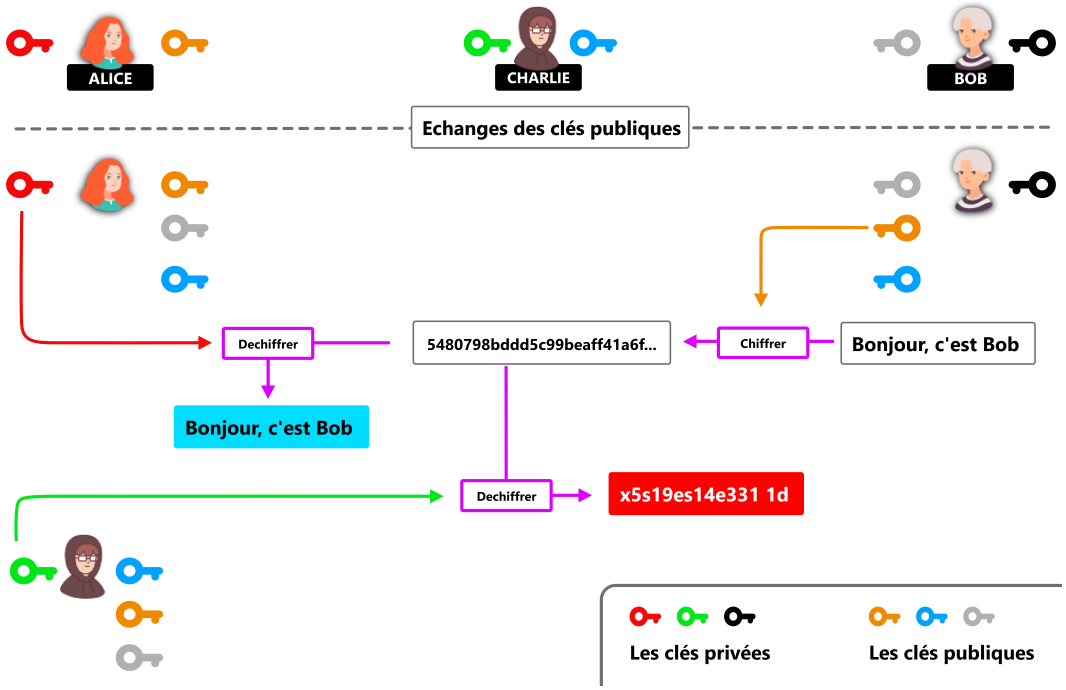


FIGURE 1.1 – Illustration de la cryptographie asymétrique

Cette clé privée d'Alice, est maintenant sa seule responsabilité, elle doit être connue que par elle, et sert à déchiffrer tout message chiffré avec la clé publique dérivée d'elle, c'est à dire la clé publique d'Alice *(vous pouvez voir dans la figure, que la clé privée d'Alice est la clé rouge derrière elle, dont elle s'est servie pour déchiffrer le message adressé à elle par Bob grâce à la clé orange qui est sa clé publique)*.

1.2.2 Une fonction de hachage

Une fonction de hachage, est une fonction cryptographique qui prend une donnée numérique pour fournir en sortie une chaine de caractère appelée *hash* ou *empreinte numérique* ou *condensé*, comme dans la *figure 1.2*. L'empreinte numérique du mot **bonjour** est 2CB4B1431B84EC15D35E D83BB927E27E8967D75F4BCD9CC4B25C8D879AE23E18, et celui de **Bonjour** est 9172E8EE C99F144F72ECA9A568759580EDADB2CFD154857F07E657569493BC44, en utilisant le SHA-256 *(type de fonction de hachage)*.

La chaine change littéralement au moindre changement dans l'entrée comme la lettre **b** dans **b***onjour* et **B***onjour*. Mais peut importe le type, le contenu ou la taille de la donnée en entrée, le résultat est toujours une chaine de caractère de taille fixe, cette taille dépend de la fonction

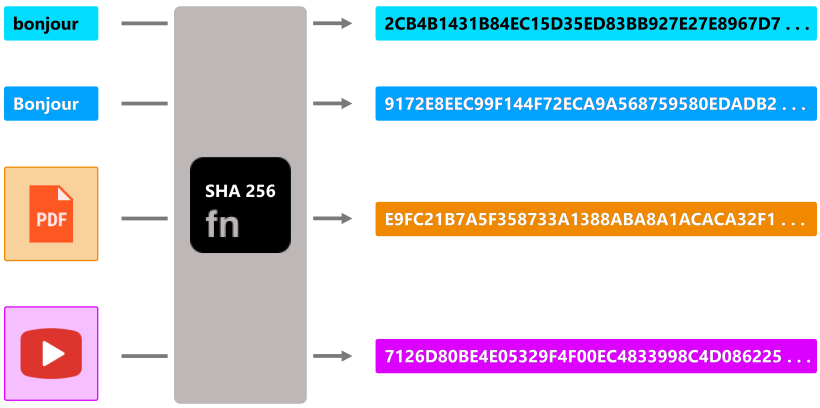


FIGURE 1.2 – Illustration d'une fonction de hachage

de hachage utilisée.

La collision : n'importe quelle chaine de caractère ou de fichier pourrait être l'entrée d'une fonction de hachage, et devrait correspondre à une sortie qui se trouve dans un ensemble borné, soit 2 à la puissance 256 pour SHA-256. Alors il y a au moins 2 entrées possibles qui tombent sur le même empreinte numérique, *(c'est la collision)*. Plus l'ensemble d'arrivé a une petite taille, plus le risque de collision est grand. Si une collision est connue dans une fonction de hachage, elle est considérée comme non sure. Il est déconseillé d'utiliser une fonction de hachage non sure.

Sécurité d'une fonction de hachage : une particularité des fonctions de hachage est qu'elles sont irréversibles , c'est-à-dire qu'elles ne permettent pas avec un empreinte donné de retrouver une entrée correspondante. Par cryptanalyse, on pourrait utiliser aléatoirement des entrées jusqu'à avoir une qui fournit le même empreinte à la sortie, mais cet astuce ne promet pas un résultat immédiat.

1.2.3 Signature numérique

Maintenant qu'on a vu ce qu'est un condensé ou hash, revenons dans la cryptographie asymétrique. Nous avions dit que Alice était la seule a accédé à sa clé privée, avec laquelle elle déchiffrait les messages qui lui étaient destinés, c'est a dire les messages chiffrés avec sa clé publique. Dans ce cas elle peut être sure que le message ne serait pas lu par une autre personne qu'elle, tant qu'elle garde bien sa clé privée, mais ce dont elle ne peut pas être sure, c'est de la provenance du message *tout le monde lui envoie un message de la même façon.* C'est là qu'intervient la signature numérique *(schématisée par la figure 1.3)*, qui est tout simplement la version numérique de la signature manuscrite qui est un moyen d'assurer le consentement et la non répudiation des documents.

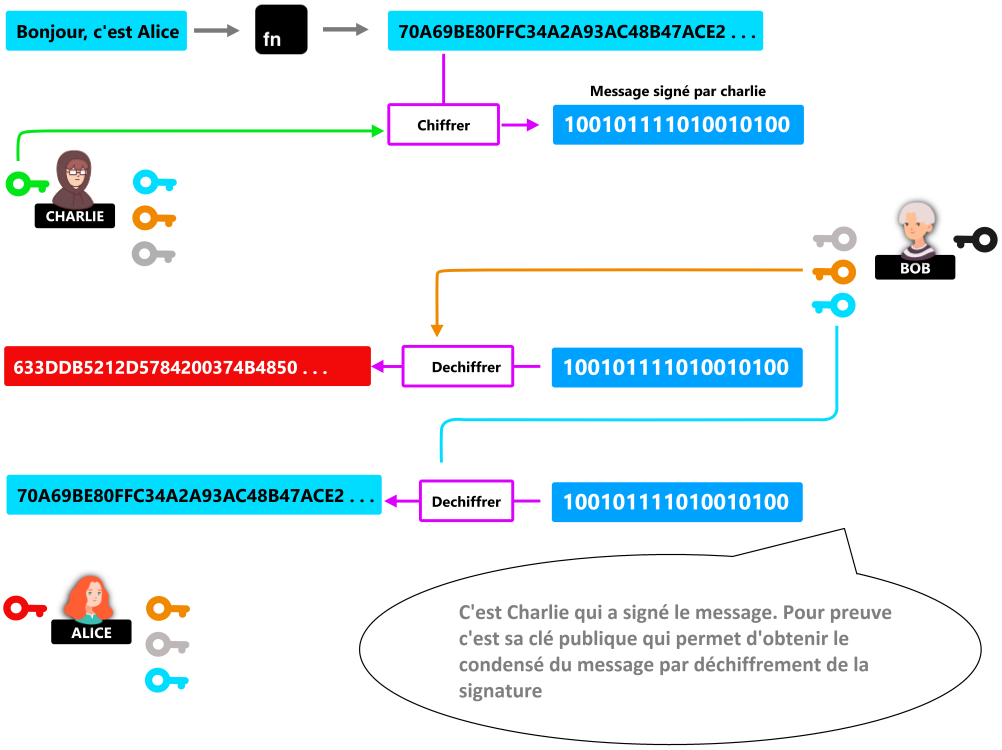


FIGURE 1.3 – Illustration de la signature numérique

Dans la signature numérique, c'est le processus inverse de la cryptographie asymétrique qui est utilisé. Pour que Charlie signe un message ou même un document, il suffit de deux étapes :

a- Il condense le message ou le document.
b- Il chiffre le condensé avec sa clé privée dont il est le seul connaisseur.

Pour déterminer si le message est bien d'Alice ou pas, il suffit de déchiffrer la signature avec la clé publique d'Alice pour voir si ça donne le même condensé que celui du message. *Dans l'exemple c'est Charlie qui a signé le message.*

1.2.4 Arbre de Merkle

C'est un arbre binaire complet, son objectif est de lier tous les éléments d'une liste en un seul empreinte numérique [5]. Le principe de la formation de cet arbre, est toujours de former des couples avec les items, puis de condenser chaque couple pour former une nouvelle liste qui recommencera le même processus jusqu'à avoir un seul condensé qui sera la racine, voir *figure 1.4*. Si la liste a une taille impaire, le dernier item est dupliqué *cas de l'item C*.

Grâce à cette racine, toute modification dans la liste de départ sera conséquente, par le changement du condensé de ce point et par conséquence tous les condensés liés à ce point de changement

jusqu'à la valeur de la racine.

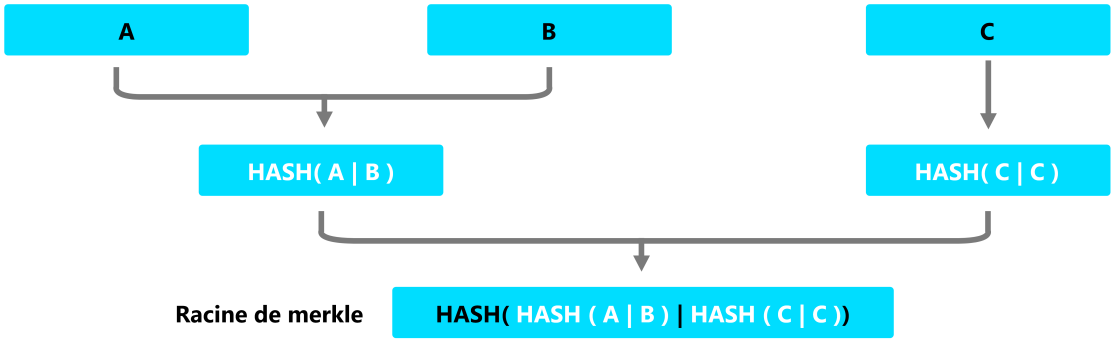


FIGURE 1.4 – Processus de formation d'un arbre de Merkle

1.3 Fonctionnement

Dans un système de transaction centralisé, il y a deux rôles principales, un tiers de confiance pour surveiller et acheminer les transactions, et des clients qui s'échangent des données via cet intermédiaire. L'ennui avec ce genre de système est que ce tiers pose problème, au moment où il est possible de supprimer ou d'ajouter des informations non voulues. Comme rien ne garantie qu'elle peut être complètement fiable, c'est à dire être corrompue volontaire ou pas, il n'est donc pas la meilleure approche en sois pour l'échange de donnée.

La blockchain propose plutôt de se baser sur la preuve au lieu de la confiance. Le but est de permettre à deux parties volontaires de réaliser entre elles des transactions sans le besoin d'un tiers de confiance. La suppression d'intermédiaire entre les partie prenante, fait que toute partie prenante doit jouer le rôle d'intermédiaire en plus d'être client. Cela nécessite un système décentralisé et distribué, dans lequel les parties prenantes ou nœuds sont identifiées grâce au principe de la cryptographie asymétrique. Chaque nœud a une clé privée pour signer ses transactions et un clé publique utilisée pour lui adresser des transactions.

1.3.1 Transactions

Dans une transaction blockchain, il est question d'entrée et de sortie. Les entrées sont les transactions dont on est récepteur et les sortie sont les transactions dont on est le destinataire. Chaque nœud envoie une valeur au suivant en signant la transaction précédente qu'il va destiner à la clé publique du nouveau propriétaire [1]. Pour vérifier la fiabilité d'une transaction il suffit de vérifier sa signature avec la clé publique du destinataire.

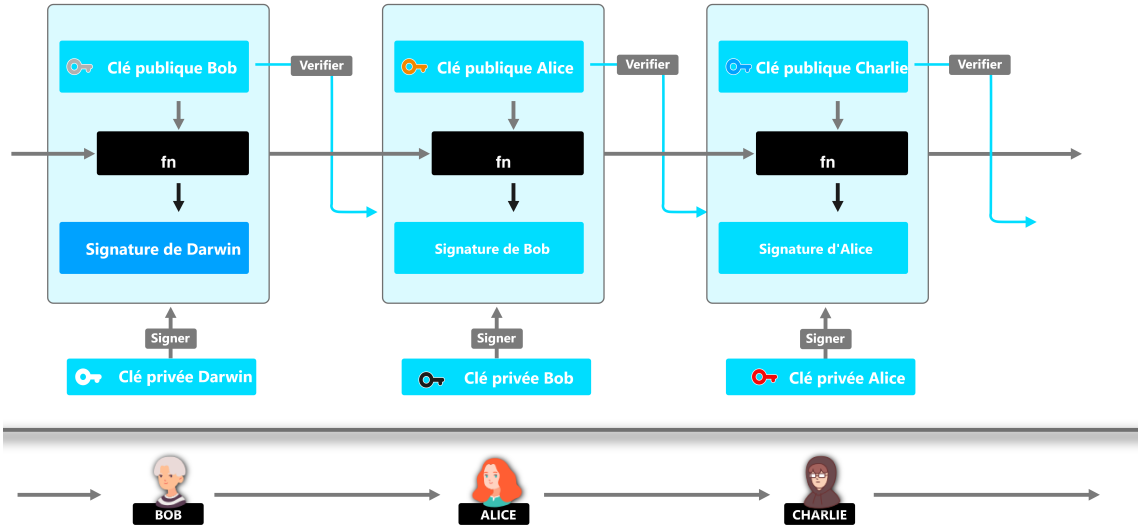


FIGURE 1.5 – Illustration des transactions des valeurs dans la blockchain

1.3.2 Minage

Les mineurs collectionnent les transactions afin d'en faire des blocs. Supposons que la transaction de Bob vers Alice *dans la figure 1.5* fait partie de la liste d'un mineur X. À partir de cette sa liste, il prend les transactions de son choix. À part la transaction coinbase, que le mineur crée pour se récompenser en cas de l'acceptation de son bloc, toutes les autres transactions sont passées à la vérification par le mineur *(est ce que les entrées que Bob veut dépenser existent et ne sont pas été utilisés)*. Si les transactions sont correctes le mineur achève sa création avec une preuve, avant de l'horodaté. Cette preuve permet de maintenir la coordination dans le réseau.

1.4 Algorithme de consensus blockchain

Avec l'absence du tiers centrale, il revient aux nœuds de gérer le réseau, et évidemment les décisions de ces différents nœuds peuvent différer, c'est la qu'intervient l'algorithme de consensus. Pour se faire, les nœuds s'échangent continuellement des messages pour maintenir le réseau. Ces messages peuvent prendre du retard, être l'objet d'une tromperie ou être perdus *(Dilemme des généraux byzantins)*.

Un algorithme de consensus d'une blockchain est mécanisme qui permet aux nœuds de cette blockchain de se coordonner dans leurs décisions pour gérer la tolérance aux pannes byzantines (**BFT**). Un système BFT est capable de continuer à fonctionner même si certains des nœuds échouent ou agissent de manière malveillante, mais cela nécessite d'abord que la majorité du réseau agit de maniéré bienveillante. Les algorithme de consensus blockchain les plus connus sont

la preuve de travail et la preuve d'enjeu.

La preuve de travail

La preuve-de-travail consiste à l'ajustement d'une valeur par incrémentation pour trouver une qui condensé avec le hash bloc, donne une empreinte numérique commençant par un nombre donné de bits à zéro [1], c'est à dire qu'on a une empreinte numérique comme référence *(comme celle en bleu de la figure 1.6)*, et le défit à relever sera de trouver une entrée dont l'empreinte numérique sera inférieure ou égale à l'empreinte numérique de référence.

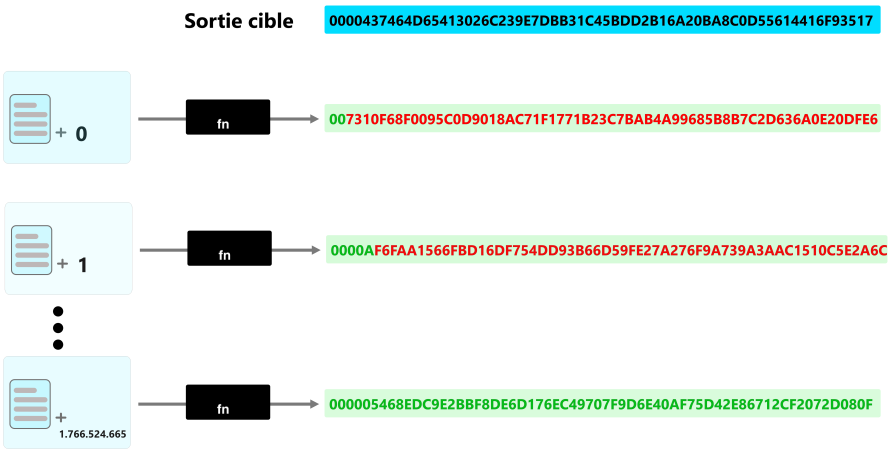


FIGURE 1.6 – Résolution d'une preuve de travail

Ces dans ce cadre que les mineurs plongent dans une résolution bien difficile. Ce processus prend évidement beaucoup de puissance de calcul, donc beaucoup d'électricité, mais c'est un moyen efficace pour retenir les nœuds malhonnêtes qui souhaiterait modifier un bloc. Dans l'exemple, après 1.766.524.665 tentatives, le mineur trouve une sortie convenable, alors ce nombre résout la preuve de travail de son bloc.

S'il n'y avait pas une preuve à fournir, il serait trop facile pour un nœud attaquant de vendre un nouveau bloc dans le réseau, avec des fausses données, dans le but de tricher ou même de saboter le réseau. Mais ce n'est pas la seule raison des preuves, elles permettent aussi de consolider la liaison des blocs. Car il ne sera plus possible d'apporter des changement à un bloc sans refaire sa preuve de travail, du fait que le nouveau condensé du bloc ne va pas matché avec la valeur de la preuve précédente. Étant donné que des blocs sont chaînés après le bloc considéré, le travail pour changer le bloc devrait inclure de refaire tous les blocs postérieurs [1].

Pour réguler la vitesse d'injection de blocs dans la chaine, la difficulté du minage varie en fonction du temps que les mineurs mettent à résoudre le puzzle *(temps qui est déterminé grâce à l'horodate des blocs)*, c'est a dire que la valeur de l'empreinte numérique de référence diminue

par augmentation des premiers bit à 0 *(ce qui rend le travail plus difficile)* dans le cas ou les mineurs mettent moins de temps que prévue pour résoudre la preuve de travail et vise versa.

Au cas ou le mineur arrive a trouver un nombre qui résout sa preuve de travail, il horodate son bloc. Les nœuds qui reçoivent le bloc doivent vérifier ses informations *(les transactions et l'entête)*, si tous leurs sembles correct, ils valideront le nouveau bloc en incluant le condensé de son entête dans leur bloc en création.

Il se pourrait qu'un nœud reçoit et valide un bloc d'un indice, juste avant de recevoir un autre du même indice. Dans ce cas, il rejettera tout simplement le deuxième bloc, qui peut être bien accepter par d'autre. C'est ce qui crée parfois une incohérence de chaine entre les nœuds. Donc pour que ses opérations soient reconnues, les nœuds se souvent mettent à jour, en abandonnant une sous chaine de bloc, pour rejoindre la plus longue chaine honnête. Ces blocs abandonnés sont appelés des blocs orphelins.

La preuve de participation ou preuve d'enjeu

Dans la preuve de participation les nœuds ne minent pas, ils la forgent plutôt. Cette astuce a été connu grâce à la blockchain peercoin en réponse à la surconsommation remarquable d'énergie des nœuds mineurs, un phénomène qui avait amener des villes, voir un pays *le Kosovo* à interdire la minage du Bitcoin.

Dans ce cas l'effort fournit par les forgeurs est de mettre en jeux des jetons, pour participer aux événements. *Le concept est base sur l'idée qu'un nœud qui a plus de ressource dans la blockchain a intérêt plus que personne d'autre à s'occuper de la sécurité du réseau.* Les forgerons qui ont plus misés, ont plus de chance de se voir voter ensuite par un groupe de nœuds qui sont nommés des validateurs, qui aussi doivent mettre des jetons en jeux pour être dans une liste dont le système pioche aléatoirement un groupe pour chaque création de bloc, plus un validateur mise gros, plus son vote pesse. Le forgeron choisi par les validateurs se voient attribuer le droit de créer un nouveau bloc. Ce nouveau bloc est donné à un des validateurs pour l'ajouter dans la blockchain, s'ils trouvent qu'il est correct.

Les autres nœuds du réseau ont la possibilité de signaler le bloc s'ils remarquent une incohérence. dans ce cas les nœuds rémunérés (les validateurs et le créateur de bloc) sont sanctionnés. ils n'ont plus de récompense et leur bloc sera recalé.

1.5 Structure

Le terme blockchain vient de sa structure, un ensemble de bloc enchainés grâce à une fonction de hachage *figure 1.7*. Cette chaine est copiée sur tous les serveurs de son réseau pair à pair, qui se synchronisent continuellement pour suivre tous une seule et longue chaine appelé la chaine de référence ou la chaine honnête. Maintenant voyons comment ça fonctionne à l'intérieur de la blockchain.

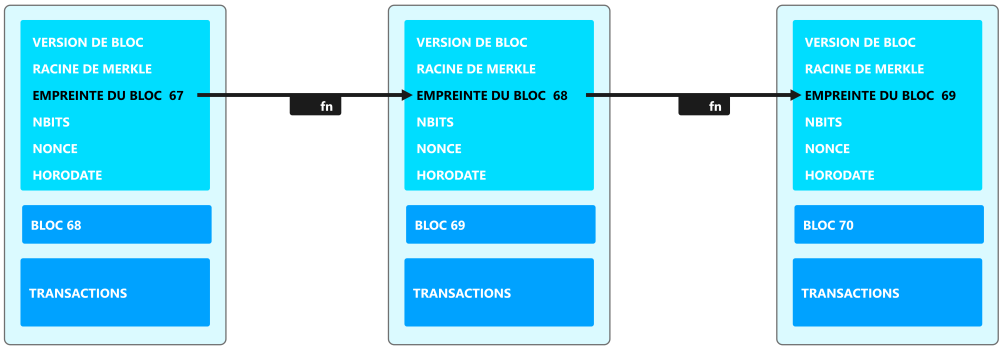


FIGURE 1.7 – Structure d'une chaine de bloc

Qu'est-ce un bloc ? Les blocs sont des fichiers dans lesquels les transactions sont enregistrées. Ils contiennent généralement les attributs : un entête, une hauteur et la liste des données à enregistrer [5].

1.5.1 L'entête de bloc

Il regroupe l'ensemble des attributs clés du bloc, qui sont entre autre :

— **Version de bloc :** les blocs ont une version, elle permet aux appareils d'appliquer le traitement recommandé sur un bloc et sur ses données.

— **La racine de Merkle :** pour garantir que les transactions ne seront pas modifiées sans modifier l'entête, la blockchain utilise l'algorithme de l'arbre de Merkle sur les transactions pour former un lien entre elles, et met le résultat dans l'entête du bloc pour lier les transactions à l'entête.

— **L'empreinte de l'entête du bloc précèdent :** Pour lier les blocs, les blocs successeurs prennent dans leurs entête l'hash de l'entête de leurs prédécesseurs.

— **L'horodate :** il représente le temps ou le créateur fini de construire le bloc. Les serveurs marque une date de création pour tous les blocs émissent sur le réseau.

— **La cible nbit et le nonce :** toutes les blockchains n'ont pas ces champs. Si le consensus stipule que les créateurs de bloc doivent fournir une preuve de travail alors ces champs vont bien exister.

La cible nbits, représente la sortie de référence que le mineur doit atteindre dans la preuve de travail. Et le nonce représente le nombre qui colle avec le bloc pour trouver une sortie convenable *(voir figure 1.6)*.

1.5.2 Hauteur

Chaque bloc a une hauteur, elle sert d'indexage pour les blocs.

1.5.3 La liste des données

Les données sont très variées en fonction des blockchains, il y a des blockchains populaires qui stockent des transactions et d'autre même qui stockent des dossiers médicaux, ... Mais la blockchain est open source, alors on peut l'adapter à nos besoins, la seule chose à retenir est que peu importe le genre de données qui sont mises dans cette liste, elles ne seront plus modifiables sans corrompre toute la base de données.

1.6 Les acteurs de la blockchain

La blockchain est venue avec l'idée de passer le contrôle d'un intermédiaire au grand public. Sa gestion se fait sur un réseau pair à pair, les acteurs du réseau ont chacun un rôle dans la gestion de la blockchain. Pour gérer ce réseau parfois libre, il va falloir savoir qui est qui.

Pour identifier un nœud, la blockchain utilise le principe de la cryptographie asymétrique. Chaque nœud possède au début une graine qui lui génère plusieurs clés privées, et des clés publiques qui sont générées de ces clés privées. Dans certaines blockchain, il est même considéré que les clés publiques doivent être protéger. Pour désigne des nœuds, elles utilisent des adresses, qui aussi sont génères des clés publiques. Les nœuds sont identifiés par leurs clés publiques ou leurs adresses. En plus ils ont des fonctions précises dans le réseau.

1.6.1 Les nœuds légers

Le terme léger désigne qu'ils ne conservent même pas l'état nécessaire à la validation des données et des blocs, Ils font confiance à des nœuds complets pour faire ça à leurs places. Un nœud léger peut conserver une quantité limitée de données afin de vérifier ses propres transactions sur le réseau. Ces genres sont très des clients qui font juste des simples transactions sur le réseau. Retenez qu'il n'y a pas seulement les nœuds légers qui peuvent faire des transactions, tous les types de nœuds le peuvent.

1.6.2 Les nœuds complets

S'il n'y a pas d'intermédiaire qui stockera les données, qui surveillera les opérations et sécurisera le réseau ? Ce sont tous les acteurs du réseau qui le font, mais tous les acteurs n'ont pas la capacité en terme de puissance, de stockage ou de disponibilité. Ceux qui remplissent ces fonctions sont les nœuds complets. Ils sont en quelque sorte ceux qui mettent de l'ordre dans le réseau. Ils vérifient, stockent et surveillent chaque bloc de la chaine.

— **Les nœuds d'archivage :** Ce sont les nœuds qui contiennent une copie de toute l'intégralité de la blockchain depuis sa création. Dès leur première connexion au réseau, ces nœuds téléchargent toute l'historique de la blockchain qu'ils ont ratés et continuent de se mettre à jour avec son évolution. S'il leurs arrive d'être absent, ils se mettront à jour à leurs arrivés, car ils sont obligés d'avoir l'intégralité de la blockchain avant faire quoi que ce soit à part se mettre à jour. Ils sont capables de vérifier, valider des transactions et des blocs.

Mais néanmoins ces nœuds stockent les indices des blocs. Pour faire leurs opérations, ils comptent sur les nœuds d'archivage pour leurs fournir le contenu d'un bloc grâce à son indice.

1.7 Les types de blockchain

1.7.1 Les blockchains publiques

Elles sont ouvertes à toute entité qui veut être membre du réseau. Tous les participants peuvent voir ce qui se passe, quand et quel nœud a fait quoi. Mais ils ne pourront pas savoir qui est ce qui est réellement dernière le nœud. *Vous verrez que dans la **figure 1.5**, les identités sont sous l'ombre, si Bob n'informe pas Alice, qui l'adresse qui lui a destiné la transaction est de lui, elle n'a aucun moyen de le savoir. Les identités sont coupés des adresses.*

1.7.2 Les blockchains privées

Elles n'appartiennent pas au grand publique, mais plutôt à des organisations. Donc aucune machine ne peut être nœud dans ces genres de blockchain sans avoir l'autorisation. Mais une fois intègre dans le réseau, elle aura le droit de voir ce qui se passe dedans.

1.7.3 Les blockchains consortiums

Ici les nœuds sont classés par niveau, chaque niveau diffère d'un autre par les privilèges qu'il offre dans le réseau. Il est généralement utilisé par les entreprises qui veulent rendre publique qu'une partie de leurs données.

1.8 La sécurité de la blockchain

Une donnée renseignée dans un bloc n'est plus modifiable sans corrompre la chaine. Avec l'ajout d'un seul point, le bloc sera changé, donc son entête dans le successeur devrait être changé aussi, et par conséquence tous les blocs successeurs suivront. À partir de là, toute la chaine sera compromit, à partir du bloc modifier.

Pour résoudre le problème, un nœud malhonnête doit relever le défit de chaque bloc qui se trouve dans la sous chaine corrompue. Mais là encore la modification n'est que chez le nœud, car une fois sur le réseau, ce nœud ne pourra faire aucune opération avec ce faux registre, car ces opérations seront tout de suite repérer par les nœuds honnêtes au moment des vérifications, donc pour continuer à travailler sur le réseau, il doit mettre à jour cette sa mauvaise chaine vers la chaine honnête.

1.9 La conclusion

Pour tenir un registrer, le blockchain est en ce moment la meilleure technologie. Elle ne permet pas d'insertion ou d'accès sans authentification, et ne donne jamais la possibilité de modification. Et reste la technologie blockchain jusqu'à présent sure grâce à l'utilisation d'un mélange de techniques de cryptographie sure. Elle est open source, elle peut être adapter en fonction du problème, mais pour être efficace, elle doit être gérer par une grande communauté et implémentée avec une règle de consensus bien réfléchit.

Chapitre 2

Traçabilité

2.1 Introduction

Dans le monde de la production, il arrive que les industries fassent des erreurs de production. Si elles sont connues, il va leurs falloir rappel les produits qui ne sont pas conforme. Un rappel de produit consiste à retirer un ensemble de lot de production non conforme de la chaine d'approvisionnement. Elle peut être volontaire, c'est à dire une initiative de l'entreprise productrice ou par obligation des figures d'autorité.

Maintenant pour limiter le risque de rappel, les entreprises doivent fournir des produits de meilleur qualité, ce qui implique une meilleure technique de surveillance constante des produits tout au long de la supplychain, cet acte est la traçabilité.
Dans ce chapitre nous définissons la traçabilité et son importance. Par la suite nous évoquerons les problèmes liés à sa mise en œuvre ainsi que quelque différente catégories de système de traçabilité connus.

2.2 Qu'est ce qu'est la traçabilité ?

La particularité du principe de prévention, est la réservation du principe de preuve, principe de RIO 1990 [3]. Les consommateurs veulent désormais une preuve de qualité sur ce qu'on leurs vend, la traçabilité alimentaire est venue dans ce cadre pendant la crise de la vache folle, pour prouver aux consommateurs français la provenance des viandes bovines, c'est a dire qu'elles ne provenaient pas d'Angleterre qui fut le domaine de la crise. Elle peut être considérée un délimiteur de responsabilité en cas de faille et aussi un outil pour savoir plus sur cette faille et minimiser les dégâts.

Le principe consiste à prendre des informations sur le produit (*qu'elles soient faites à la main ou informatique*) continuellement à l'intérieur et entre les maillons de la supplychain, comme l'exemple de l'élevage, de la production et la distribution du poulet dans la *figure 2.2*. Ces informations sont prises par ces maillons dans le but d'être préparés à des situations de non-conformité (*les cas de rappels*) et à des fins de marketing *(prouver la qualité supérieure des produits aux consommateurs en étant transparents sur la fabrication de ces produits*).

Par clarification, la traçabilité ne sert pas seulement à associer des informations sur les produits,

comme quoi elle perdrait rapidement son sens, ce qui est visible vue la quantité de mauvais produits dans le marché avec des fausses informations de production. Elle consiste aussi une suivie des règlementations afin de mener à bien son objectif. Par exemple *la loi stipule que lors du transport des médicaments, la température doit être constamment mesurée et surveillée.*

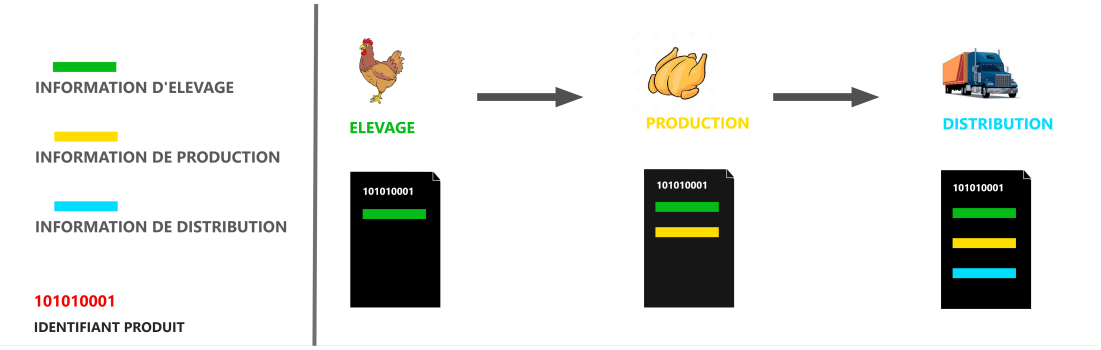


FIGURE 2.1 – Illustration de traçabilité dans la supplychain

.

2.3 Les branches de la traçabilité

La perspective de la nouvelle norme ISO 9000 : 2000, divise la traçabilité en deux volets, logistique et qualitative [3], la première consiste à traquer le produit (*le suivre à la trace : où il est, où il était, et comment sont passés ses déplacements ?*), et la deuxième s'intéresse sa qualité (*de quoi il est fait, comment et quand il a été fait ?*).

2.3.1 La traçabilité ascendante

Elle est associée à la qualité du produit. Elle intervient en fixant l'origine et les caractéristiques d'un problème de non conformité, ainsi que les causes tout au long de la supplychain. Elle est assurée par les producteurs, qui doivent prendre des informations lors de la production. Ces informations permettent reconnaitre les raisons de non conformité, en vérifiant *(c'est quoi le problème et d'où il vient)*. Dans la *figure 2.2*, si un consommateur se plaint d'une saucisse qu'il aurait acheté dans le point de distribution A, la traçabilité ascendante permettra de remonter à la source du problème en commençant par le point de distribution A vers le point de production du lot de saucisse numéro 4, ensuite vers le lot de poulet numéro 1 et 2. En ce moment ils devront voir si la traçabilité dans le maillon d'élevage est correcte, qu'il y avait un volaille malade dans le lot numéro 2. De là ils trouveront aussi le lot de saucisse 5 qui a été fait avec une partie du même lot de volaille infecté.

.

Elle opère sur trois champs, avant la chaine de production, **traçabilité en amont** qui s'occupe de la qualité des produits pères, dans la chaine de production, **la traçabilité interne**, et après

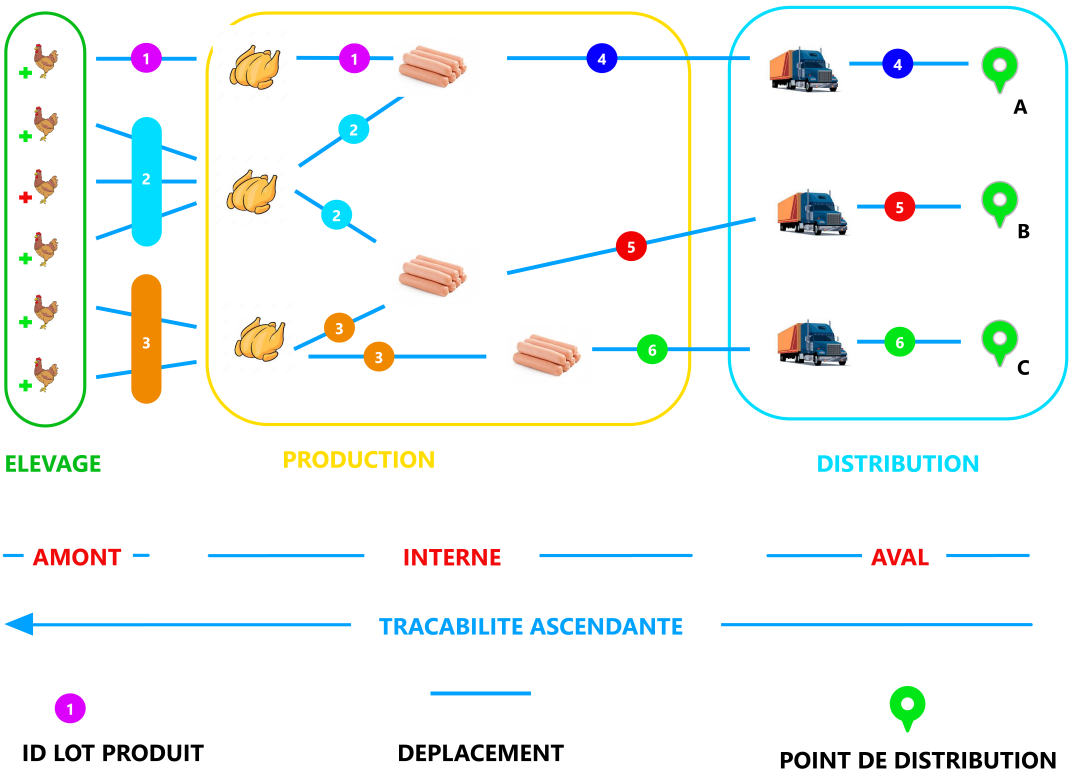


FIGURE 2.2 – Illustration d'une traçabilité ascendante

la chaine de production, **la traçabilité en aval**.

NB : dans la notion de qualité, certaines variables échappent à la traçabilité ascendante, il faut savoir que la qualité du produit peut être en jeux même en dehors de la chaine de production, c'est le cas dans plusieurs filières, pharmaceutique, agroalimentaire, etc. Un exemple plus simple est le non respect de la chaine de froid pendant les déplacements des produits, qui peuvent avoir des conséquences néfaste sur les produits voir les rendre dangereux on inconsommables.

2.3.2 La traçabilité descendante

Commune à plusieurs filières de traçabilité, elle est généralement assurée par les prestataires de service logistique. Elle opère en relevant des informations comme (*la localisation, les dates de livraisons, date de sortie, les conditions de transport, etc.*) du produit tout au long de la supplychain, dans le but d'optimiser le rappel de ce produit en cas de problème en précisant les zones potentielles d'intervention en cas de problème, *c'est à dire les points de consommations des produits défectueux ainsi que pour les autres produits liés avec la même étape de production ou avec le(s) même produit(s) père(s) défectueux*. Comme exemple il est observable qu'en cas de problème dans *le lot de volaille numéro 4 de la figure 2.3*, il n'y aura pas de difficulté à savoir que le lot est dans le point de distribution E après être passé par C, en plus du fait de partager le même point de production avec les lots 2 et 3.

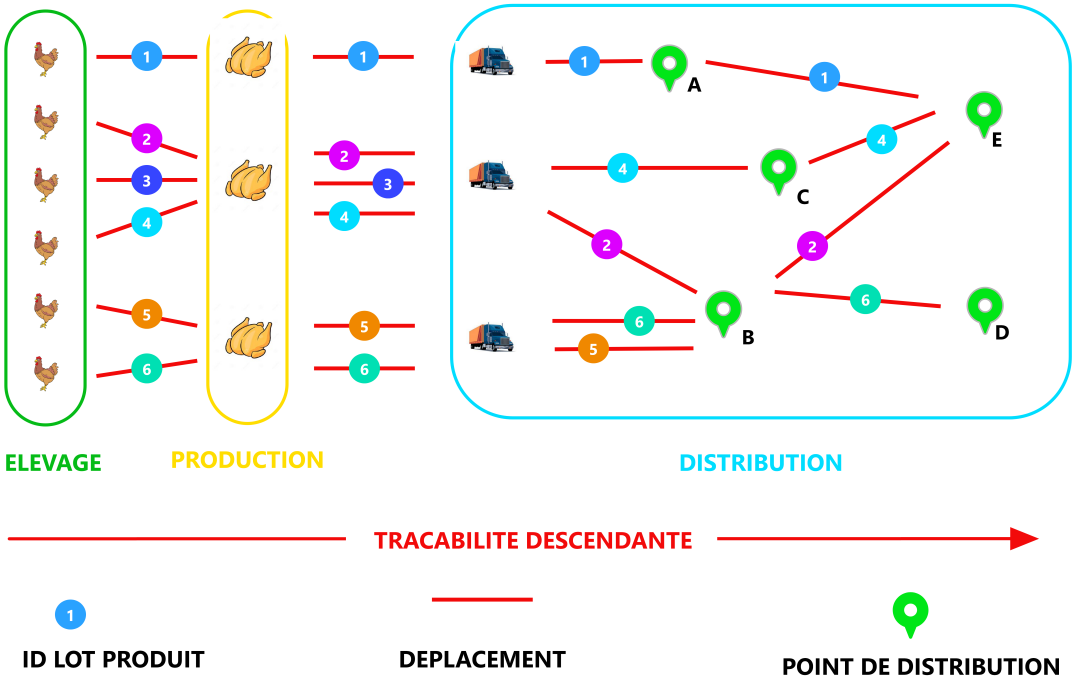


FIGURE 2.3 – Illustration d'une traçabilité descendante

2.4 Les problèmes de mise en place de la traçabilité

Le problème sérieux avec la mise en place de la traçabilité n'est pas les techniques déjà connues, mais le choix des informations a enregistrer et l'assurance de la confidentialité et l'intégrité de ces données et un manque de réglementation nécessaire. Dans une supplychain très longue, les informations des produits sont moins pertinentes à cause de leur quantité débordante et leur de manque de généralisation.

Ce manque de généralisation et de coordination peut être associée à manque de réglementation. il faut prêter attention à la logique selon laquelle les entreprise décide des informations à enregistrer et de la manière de s'y prendre, ce qui pourrait dénaturaliser le principal objectif de la traçabilité [3]. Cette crainte est fondée, les entreprises de productions considèrent plus la traçabilité comme un moyen de marketing qu'un outil de sécurité. Il faut un minimum de réglementation et une généralisation par filière ainsi qu'une transparence des systèmes de traçabilité vis à vis des consommateurs enfin de pousser les entreprises de productions à répondre aux exigences des consommateurs.

Un autre problème est lié à la fiabilité des informations *(sont-elles vraies)*. Les informations sont la clé de la traçabilité, elles déterminent sa qualité et sa performance face à la gestion de crise. La sécurité de ces informations joue aussi sur la qualité de la traçabilité. L'évolution de l'internet a permis celui de la traçabilité (*accès aux données et une facilitation d'échange entre*

les maillons de la chaine), mais il compromet également d'un point de vue la sécurité de ces données. Les différents maillons dans la chaine, afin d'assurer l'intégrité et la confidentialité de leurs données volumineuses qui transitent dans la chaine, font appel à des sociétés spécialisées dans le domaine de la gestion de stockage et de sécurisation de donnée.

2.5 Comment les entreprises ont répondu à la traçabilité ?

2.5.1 Les labels

Dans ce cas, ce sont des entreprises de certification comme **le label rouge** qui jouent le tiers de confiance entre les consommateurs et les producteurs, elles se portent garantes pour classer les produits pour les consommateurs, selon des principes qui peuvent partir d'un respect de cahier de charge par la marque ou de provenance géographique. Ce système existe jusqu'à nos jours, opérant comme le système d'étiquetage mise en place dans les années 80 par les producteurs de viande bovine pour faire comprendre les clients qu'ils pouvaient compter sur ces viandes étiqueté, cet étiquetage tout seul ne suffit pas de prouver grand-chose, car de la même façon que les éleveurs et ou les vendeurs pouvait se tromper sur la provenance de la viande et l'état de santé des bovins, ces labels le peuvent.

2.5.2 La communication corporate

C'est un moyen de conquête de client. Il est base sur la communication, dans laquelle les entreprises de production vendent les produits à travers leurs images, vis à vis des clients. Dans ce système de traçabilité, une information représenterait tout un genre de produit fabriquées (information statique, c'est à dire pour chaque lot de produit de même type, ce sont les même informations de qualité qui sont affichées). Ce genre de pratique existe jusqu'à maintenant, du fait que les consommateurs ont tendance à valoriser les produits par l'image de la marque plus qu'a la maniéré dont les produits qu'ils ont dans la main ont été faits. C'est une pratique qui n'est pas vraiment un support sur lequel on peut compter pour mettre en place un système de traçabilité efficace.

2.5.3 Le marketing de la preuve

Cette approche est la plus solide, elle tourne au tour de la preuve. Les entreprises productrices se contente de fournir des preuves sur la fabrication de leurs produits et laissent le libre choix aux consommateur de juger. Dans ce genre d'approche les informations d'un maillon dépendent de celles de autres, car les produits sont jugé par la somme des preuves cumulés tout au long des transformations subit et de changement de responsable dans la supplychain.

L'avantage de cette solution est que les entreprises de production se verront d'avantage forcer à faire attention à leurs productions mais aussi aux produits de leurs fournisseurs et de leurs clients, en ce voyant inclure dans une chaine de responsabilité qui dépassent sa chaine de production.

2.6 Conclusion

Dans ce chapitre nous avons présenté la traçabilité, ses 2 volets ainsi que ses problèmes de mises en place et les différentes types de solution qui existe pour assurer les consommateurs. Après

une vingtaine d'années, les crises alimentaires sont toujours aussi fréquemment pressentent dans la supplychain. La traçabilité agroalimentaire est toujours inefficace dans certains maillons, pas par insuffisance du concept, mais par une mauvaise approche. Par tout dans le monde les crises observées dans l'agroalimentaire résument la capacité insuffisante des systèmes de traçabilité actuels. Comme le montre un communiqué de presse de l'OMS en 2015, les maladies d'origine alimentaire touchent plus de 91 millions de personnes uniquement dans les régions africaines, 77 millions dans les régions américaines, 150 millions dans les régions de l'Asie du sud-Est et 23 millions dans les régions européenne. Il faut une orientation d'approche vers une transparence totale vis à vis des consommateurs, prendre en charge tout lot de production de façon unique et pouvoir garantir aux consommateurs la fiabilité des informations sur ce lot. Un contrôle minimum avec lequel les producteurs se verront dans l'obligation d'avancer que des vraix argument et de veiller sérieusement sur la qualité de la production.

Chapitre 3

Systèmes de traçabilité

3.1 Introduction

Viguera [4], le point commun entre les définitions de la traçabilité est la présence « d'une chaine ininterrompue d'informations, une base reconnue par l'institution nationale ou internationale et une application générique ». Du point de vue information, un système de traçabilité repose sur deux systèmes [6] : un système d'identification et un système d'information.

— Le système d'identification physique des lots : il permet d'identifier de façon unique les produits à l'aide d'étiquette code barre, ou puces électroniques, etc. Il existe plusieurs système d'identification dans la supplychain : les étiquettes, les boucles d'oreilles pour les animaux, les marquages de produit, les code barre, les puces RFID, etc.

— Le système d'information : il permet de garder l'historique des actions effectuées sur les produits (fabrication, distribution, consommations, responsable de production, etc). Il peut être sous forme papier ou informatique. Un système informatique, est rapide dans des circonstances de crise, et engendre moins d'erreur.

Dans ce chapitre nous allons présenté deux travaux de mises en place de système de traçabilité, par la suite nous développerons les avantages et les inconvénients de chacun de ces travaux. Nous conclurons ce chapitre en définissant notre solution de traçabilité tout en tenant compte des avantages et inconvénients des travaux présentés, en précisant les idées que nous allons emprunté et celles que nous améliorons dans notre système.

3.2 État de l'art 1 : mise en place de la traçabilité alimentaire dans une entreprise de fabrication de saucisson

C'est un travail réalisé par clément Dupuy [6] en collaborations avec le groupe AOSTE (*une entreprise de création de jambon de porcs*). Ils partent du principe que les systèmes de traçabilité sont plus efficaces dans la réaction face aux crises, s'ils font moins de dispersion en terme de fabrication et d'information. Le travail a été de modéliser les traçabilités internes et logistique enfin de les analysées et les optimisées et remettre en place un meilleur système adapté à la chaine de production et logistique avec le minimum de dispersion possible de produit et d'information

enfin de réduire le couts de rappel et augmenter le temps de réaction du système. L'approche est divisée en 4 parties dont nous verrons que les 2 premiers qui sont basées sur la solution :

— Une méthode et un modèle spécifique pour la traçabilité interne et la dispersions des lots.
— Une modélisation par brique du processus d'enregistrement du flux pour la traçabilité de la chaine logistique.
— Un modèle mathématique pour minimiser la dispersions de lots
— Et la mise en œuvre de leurs solutions proposées.

3.2.1 Méthode et modèle spécifique pour la traçabilité interne et la dispersion des lots

Limiter au maximum la dispersion *(c'est à dire le mélange de produit)* est aussi un facteur important dans la traçabilité. Cette première étape vise à modéliser la chaine de production de l'entreprise pour mettre en place une traçabilité interne adéquat qui viserait à optimiser la dispersion. Elle se déroule en 4 phases :

— La modélisation du système existant.
— L'analyse et amélioration des processus de fabrication et de l'organisation.
— Définition de nouveau système de traçabilité.
— Et la mise en place du nouveau système de traçabilité.

Phase 1 : modélisation du système existant

Cette phase est réalisée en 4 étapes, d'abord ils définissent les TRU existants *(les lots de production)*. Ils modélisent l'enchainement et la dispersion de ces TRU, pour ensuite analyser et optimiser leur système de traçabilité existant à partir du modèle obtenu.

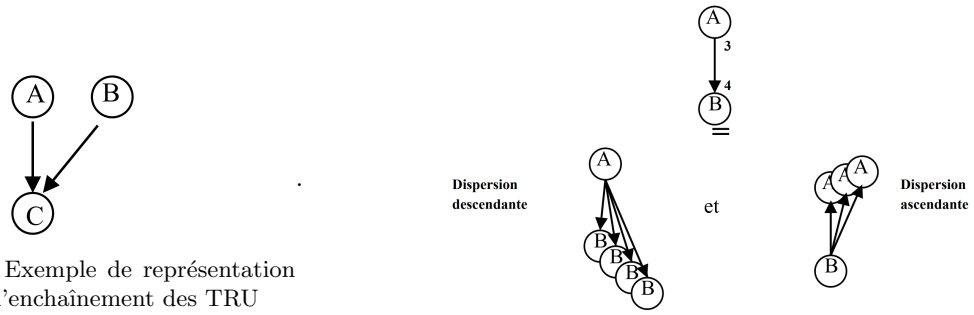
Étape 1 : définition des TRU existants Un TRU (Traceable Resource Unit) représente «un groupe homogène d'une classe de ressource utilisée / consommée / produit / libérée par une activité élémentaire dans une quantité non nulle et finie de cette classe».

Étape 2 : modélisation de l'enchainement des TRU Après la définition des TRU, ils ont construit leur enchainement à l'aide d'un graphe de type nomenclature *(voir figure 3.1)* pour obtenir un modèle de la chaine de production à analyser.

Étape 3 : détermination de la dispersion Après la modélisation de la chaine de production, ils ont déterminé les dispersions ascendantes et descendantes des TRU. La dispersion descendante entre un TRU père A et son TRU fils B mesure le nombre de lots du TRU B liés à des lots du TRU A. La dispersion ascendante entre un TRU père A et son TRU fils B mesure le nombre de lots du TRU A dont est issu un lot du TRU B.

Soit l'exemple tiré du document *fig 3.1(b)*, dans le cas de la production de steaks hachés, si un bac de préparation de hachage (TRU A) se retrouve dans 4 mêlées différentes (TRU B) et si une mêlée est constituée de 3 bacs de préparations alors on obtient la dispersion présentée.

Étape 4 : analyse du système de traçabilité existant Après avoir modéliser le système existant, ils ont commenté et analyser le modèle : les points faibles, points forts et les améliorations possibles.



(a) Exemple de représentation de l'enchaînement des TRU

(b) Modélisation de la dispersion

FIGURE 3.1 – Exemple de modèle de dispersion [6]

Phase 2 : Analyse et amélioration des processus de fabrication et de l'organisation

Étape 5 : Analyse du graphe de dispersion L'objectif de cette étape est de repérer les zones d'amélioration dans le graphe réalisé dans l'étape 3, c'est-à-dire repérer les parties du processus de fabrication qui peuvent être optimisées. De là, ils ont créé un nouveau graphe de dispersion, *graphe de dispersion optimal* dont les valeurs de dispersion correspondent au minimum acceptable par l'entreprise. En comparant ce nouveau graphe au graphe de dispersion initial, ils ont mis en évidence les zones d'amélioration possibles dans la chaine de production.

Étape 6 : modélisation des processus de fabrication et de l'organisation Après avoir mis en évidence les secteurs d'amélioration des processus de fabrication et de l'organisation, ils ont cherché des solutions d'amélioration, secteur par secteur en proposant un maximum d'amélioration possibles puis de choisir la plus pertinente pour chaque secteur à améliorer.À partir des décisions prises dans cette étape, ils ont construit un troisième graphe de dispersion : *le graphe de dispersion objectif* qui sera proche du graphe de dispersion optimal *voir figure 3.2.*

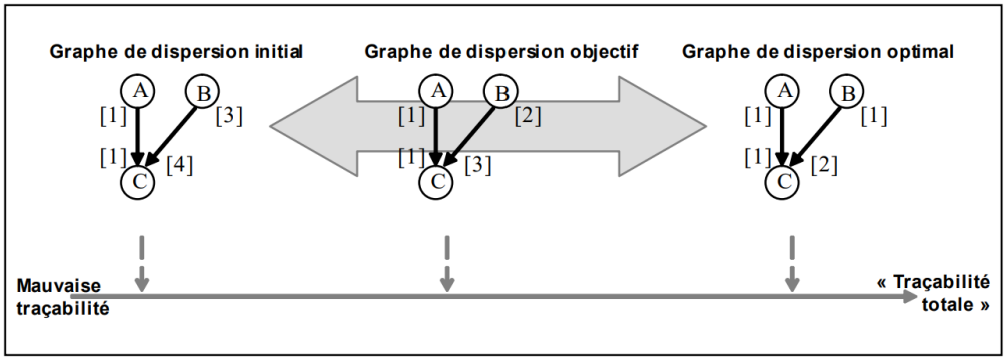


FIGURE 3.2 – Les différents graphes de dispersion [6]

Phase 3 : définition du nouveau système de traçabilité

Après l'optimisation du graphe, ils ont procédé á la définition du nouveau système d'information en passant par la définition des enregistrements, la définition de l'identification des TRU, la définition de la base de donnée.

Étape 7 : définition des enregistrements L'enregistrement d'un lot de production correspond à la déclaration de son existence dans la base de donnée. Cela passe par la création et l'enregistrement d'un code d'identification et des informations liées aux lots *(modèle)*.

Étape 8 : définition de l'identification des TRU Elle permet de suivre les lots de façon univoque. Cette étape permet de définir le type d'identification qui sera utilisé pour marquer les TRU lors de leurs créations.

Étape 9 : définition de la base de donnée Cela fait partie du système d'information, l'identification et les enregistrements sur les produits sont stockés sur une base de données. Cette base de données servira de trace et permettra de lancer des requêtes sur les données enregistrées.

Phase 4 : Mise en place du système de traçabilité

C'est l'étape final, après la définition du système de traçabilité, cette dernière phase consiste à mettre en place le système défini. La mise en place varie en fonction de l'entreprise. Il faut mettre en œuvre un système ergonomique, facile d'utilisation et moins pénalisant pour la productivité des différents ateliers de production.

3.2.2 Modélisation du système de traçabilité de la chaine logistique

La traçabilité à aujourd'hui surtout été étudié dans la littérature scientifique d'un point de vue qualité ou commercial et peu d'un point de vue optimisation de la chaîne logistique. L'optimisation de la chaine logistique est souvent abordée sous un angle de diminution des couts (stockage, de transport, de production, ...) et peu sous l'angle de l'optimisation de l'échange d'informations [6]. Optimiser la traçabilité dans la chaine logistique revient aussi à :

— **Diminuer la dispersion physique des lots**, donc la dispersion de l'information sur la chaine logistique, pour facilité les rappels.

— **Augmenter le périmètre et la fiabilité des informations partagées**, c'est-à-dire partager le plus d'informations pertinentes sur les lots et être en mesure de garantir leurs véracités, enfin d'augmenter la satisfaction des clients.

— **Augmenter la rapidité de réponse du système** enfin de gérer au mieux les problèmes en cas de crise.

Dans cette deuxième partie, ils empruntent également le même procédé que celui dans la chaine de production, ils mettent en œuvre des modèles génériques qui puissent s'appliquer à la plupart des processus d'enregistrement des flux dans l'industrie, à chaque étape du processus correspond un des modèles génériques. Ces modèles sont enchainés comme des briques pour modéliser la chaine logistique complète. L'étape suivante sera d'analyser l'enchainement de ces modèles génériques enfin de l'optimisé.

Modélisation des processus d'enregistrement des flux matière

La modélisation ARIS L'abréviation ARIS signifie ≪**AR**chitecture des **S**ystèmes d'**I**nformations intégrées≫. C'est un concept appliqué, qui a pour fonction de proposer des méthodes d'analyse pour de décrire les processus d'un système d'information sur différent point de vue (nature, fonction, interaction) [7].

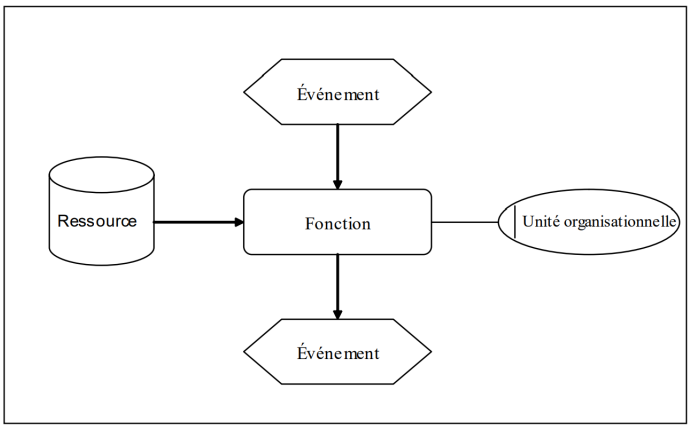


FIGURE 3.3 – Formalisme de la modélisation ARIS [6]

Les systèmes de traçabilité passent par l'enregistrement du flux de matière. L'objectif de cette partie est de modéliser l'ensemble de ces processus d'enregistrement des flux en utilisant des modèles génériques. À chaque étape d'enregistrement des flux, ils ont repéré trois actions possibles *voir figure 3.4* : la réception de lot et ou fabrication de lot et ou expédition de lot. Ils ont élaboré des modèles CPE pour chacune de ces fonctions avec le formalisme de la modélisation ARIS ***figure 3.3***. La *figure 3.5* représente le modèle CPE de la fonction fabrication. Chaque étapes d'enregistrement de flux du système sera modélisé par un des 3 modèles générique.

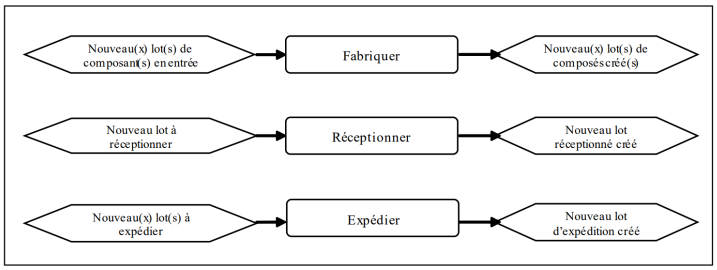


FIGURE 3.4 – Les 3 fonctions de base [6]

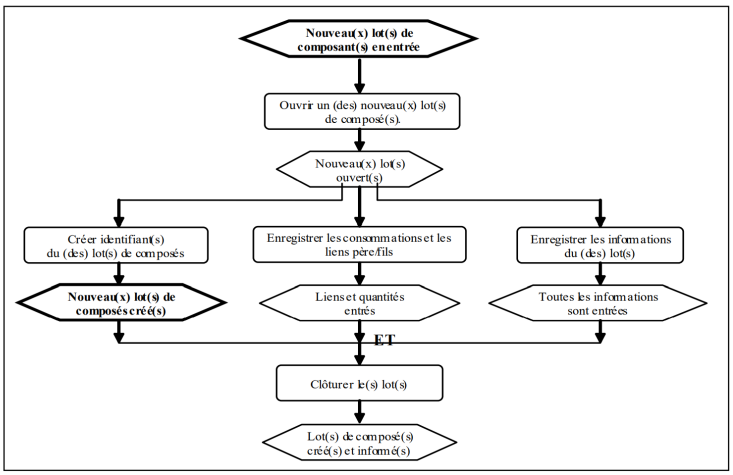


FIGURE 3.5 – Modèle CPE de la fonction fabriquer [6]

Une fois le squelette du processus modélisé par l'enchainement des évènements et des fonctions *(voir figure 3.6)*, ils ont ensuite développé chacune des fonctions de bases par leurs CPE *(voir figure 3.7)*. Après ce processus permet au système d'être visualiser sous plusieurs vues *(données, fonction, organisation)* et on peut lui affecter des ressources *(humaines ou matérielles)* et des unités organisationnelles *(rôles et responsabilités)*.

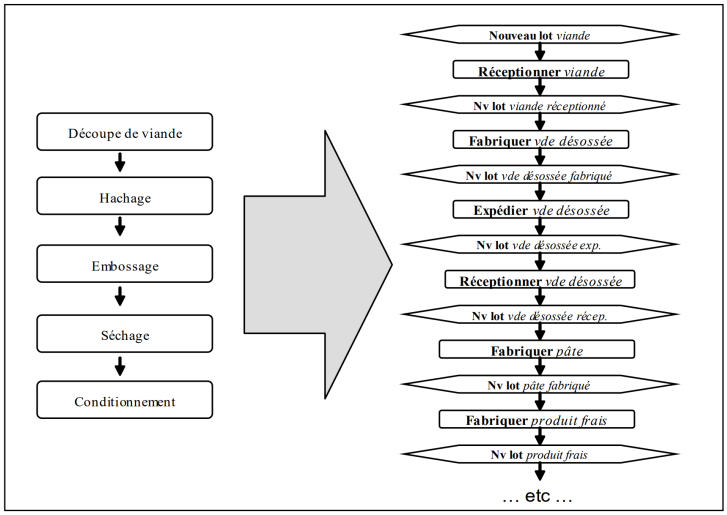


FIGURE 3.6 – Premier niveau de modélisation appliqué au cas du groupe AOSTE [6]

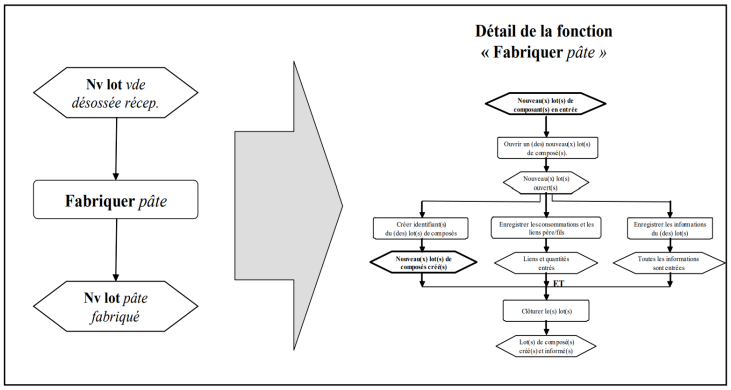


FIGURE 3.7 – Exemple du passage du premier niveau au second niveau de modélisation pour la fonction « fabriquer pâte » [6]

Mise en œuvre des modèles

Comparaison des modèles et conception du système : en effectuant une comparaison des modèles génériques présentés et le modèle d'un processus d'enregistrement de flux matière du système existant grâce au logiciel ARIS, il est facile de mettre en évidence des carences et incohérences, repérer les zones d'amélioration potentielles du processus existant qui peuvent être optimiser grâces aux modèles générique. Une fois l'enchainement des modèles génériques créé, des ressources matérielles et organisationnelles peuvent être associées aux fonctions du modèle obtenu. Le modèle devient alors un réel support d'aide à la conception qui garantit la cohérence du système cible à mettre en place.

Mise en place d'indicateur de performance : un indicateur de performance permet de mesure l'avancement des actions dans un objectif visé. Il est formé par l'association d'un objectif et des variables d'action. La *(figure 3.8)* représente un exemple d'indicateur de performance mis en place.

Toujours dans le cadre de l'optimisation du système, ils proposent l'application de ce principe à la traçabilité avec un objectif globale (optimiser la traçabilité) et des sous objectifs comme (augmenter la fiabilité des données, augmenter la productivité des opérateurs charges de l'acquisition de données, diminuer le temps de réponse d'une requête, diminuer la dispersion physiques de lots de productions, diminuer la dispersion d'information). Les variables d'action dépendent des indicateurs de processus qui rendent compte de l'évolution des activités qui participent à un processus *(comme la dispersion physique de lot, la dispersion de l'information, le nombre d'article tracé, fiabilité du système de traçabilité, la rapidité à retrouver les lots recherchés)*. Un des intérêts de l'utilisation d'indicateur de performance est le benchmarking, une méthode permettant de comparer, à indicateur égal, des entreprises différentes.

Indicateur : Temps de réponse
Sous objectif concerné : rapidité de réponse du système. **Valeur** : temps mis par un utilisateur formé pour trouver l'identification et l'emplacement des balancelles de saucisson concernées par un nombre défini de lots de viande réceptionnés. **Mesure** : chronométrage de l'utilisateur. **Variables d'action** : l'ergonomie et les fonctionnalités du système ont une très grosse influence sur le temps de réponse d'une requête donnée.

FIGURE 3.8 – exemple d'indicateurs de performance de la traçabilité [6]

Avantages du système

Système sur mesure c'est un système utile pour les grandes entreprises de production dans la simplification de la complexité des processus, du fait que le système permet de visualiser toute la chaine pour fixer un modèle optimisé que possible.

Réaction rapide du système le fait qu'il soit un système sur mesure permet d'obtenir le modèle minimum possible qui réduit le plus possible la dispersion autant des produits que les informations. Cette optimisation contribue à la simplification de la complexité du système et la résolution rapide des problèmes.

Inconvénients

Système sur mesure le travail prend en compte les produits et les processus pendant la mise en place de la traçabilité. D'où chaque modification dans la chaine de production ou logistique peut déclencher une réévaluation de tout le système.

Le deuxième point, est que le système de traçabilité n'est pas un système général, chaque entreprise de production a un système propre à sa traçabilité, alors les frontières des entreprises de production peuvent rendre certaines informations liées au produit peu intéressantes, donc une perte et de l'impertinence d'information. Ces raisons peuvent influencer négativement la rentabilité des systèmes de traçabilité face aux collaborations inter-entreprise.

La fiabilité des données n'est pas garantie les bases de données simples jusqu'à preuve du contraire ne sont pas à l'abri de modifications et d'indisponibilités potentielle même si leurs réplications et récupérations sont prises en charge par les services Cloud. Après tout il n'est pas moins probable de contourné les marges de sécurité des systèmes centralisés, donc la non répudiation n'est pas assurée ni l'intégrité des données. Ces manques causent un doute dans la fiabilité et la disponibilité rapide des données.

3.3 État de l'art 2 : mise en place de la traçabilité grâce à la blockchain

Cet deuxième état de l'art est réalisé par Juan F Galvez, J.c Mejuto et Simal-Gandara [8]. Il consiste à mettre en œuvre un système de traçabilité à l'aide de la technologie blockchain. Sur ceux ils proposent des concepts à mettre en place pour consolider leur système de traçabilité basé sur la blockchain tel que :

3.3.1 Authentification des produits

La déclaration de qualité supérieure de produit couteux sont souvent la cible de fraude [8]. C'est pourquoi la provenance des produits alimentaires est important pour garantir leurs qualités et l'assurance des consommateurs. L'authenticité des produits alimentaires est reconnue comme un critère de qualité important, c'est un processus par lequel la conformité des aliments avec leurs descriptions d'étiquettes *(comme l'origine géographique, la méthode de production, la technologie de transformation, la composition, etc.*) est testée et confirmée par des laboratoire.

D'abord ils ont commencé par proposé d'inclure les test authentification des aliments comme informations supplémentaire des paquets alimentaires des produits dans la blockchain.

3.3.2 Généralisation des informations pour les maillons de la supply-chain

Blockchain permet de réunir un ensemble de maillons de la supplychain dans un seul grand système de traçabilité, ce qui nécessite un langage commun entre ces acteurs de la supplychain. Ils proposent de sélectionner des informations appropriées pour tous les maillons de la supply-chain, en mettant particulièrement l'accent sur les exigences des consommateurs ainsi que des normes appropriées.

3.3.3 Utilisation des contrats intelligents

Dans une supplychain, certaines collaborations entre maillons sont difficile à modéliser et à contrôler, il est alors évident qu'un maillon ait des difficulté à faire confiance à un autre pour intervenir dans la traçabilité de ses produits. ils proposent d'utiliser des contrats intelligents pour renforcé l'impact de la traçabilité en mettant des exigences et des transaction par déclenchement pour automatiser les collaborations. *Par exemple : une entreprise peut réduire les risques que ses prestataires de services logistique utilisent des camions qui respectent les normes convenues.*

3.3.4 Restriction des fonctions d'écriture dans la blockchain

Un système de traçabilité doit être transparent, c'est-à-dire que les informations qui s'y trouve sont accessibles à tous, mais l'ajout de ces informations est réservé aux propriétaires des produits. Alors il faut une blockchain à écriture restreinte. Ils proposent d'utiliser des jetons comme licence d'enregistrement. Ces jetons peuvent être délivrer par une autorité de certification.

3.3.5 Utilisation des objets connectés

Dans les services logistiques, utilisation des IoT est beaucoup adoptée, en raison de son automatisme et son faible coût d'application. Ils proposent une utilisation généralisée de ces technologies émergentes pour une meilleure automatisation de saisie, vérification et assurance des produits tout au long de la supplychain enfin d'améliorer la qualité d'information liée au système.

3.3.6 Avantages du système

La première importance de la traçabilité grâce à une technologie blockchain est sa différence avec les systèmes de traçabilité standards, qui est sa capacité de généralisation des systèmes. Elles permettent une traçabilité de bout en bout en réunissant les maillons de la supplychain qui ne se connaissent pas, en un seul système fonctionnant sur un seul langage technologique. Elle permet une collaboration fructueuse entre ces parties prenantes dans l'aboutissement de leurs animations de fournir à leurs consommateurs la preuve de leurs qualités supérieures, en passant par l'établissement de la confiance et la transparence entre ces acteurs.

Le deuxième avantage avantage est la transparence qu'assure les blockchains. Les blockchains permettent aux parties prenantes d'échanger des informations (*informations produits, évaluation de produit, échange de valeur, convention, etc.*) qui sont prises en compte et copiées sur l'ensembles des nœuds du réseau. Après cette étape chacune de ces informations seront consultables dans la blockchain sans interruption tout en ayant la possibilité de savoir de qui elles viennent, et la probabilité importante de déterminer celles qui sont douteuses et celles qui ne le sont pas. Cette possibilité de doute provient de la nomenclature des produits stockés dans la blockchain, c'est-à-dire qu'partir des chaines de productions de second niveau, les productions ont en évidence des produits pères qui sont intervenus dans leurs fabrications. Ce concept est l'un des bases de toute transaction de blockchain monétaire qui en partant des entrées uniques créent des sorties uniques, c'est la même logique dans les systèmes de traçabilité grâce à la blockchain, elles ont la possibilité de fixer un lien possible entre les produits.

Le troisième avantage de la blockchain est la sécurité des données. Une donnée échangée sur la blockchain est toujours intègre, c'est-à-dire qu'elle ne peut pas subir de transformation *(modification ou supprimer)*, du fait qu'elle a une copie sur l'ensemble des nœuds de la blockchain. Cette sécurité est soulageante pour les parties prenantes de la traçabilité, qui sont souvent obligées de fondée des liens avec des spécialistes des gestions de données.

Cependant l'intégrité des données n'est pas le seul critère de sécurité à prendre en compte dans un système de traçabilité, mais il s'agit aussi de détermine si elles sont fiables. La fiabilité des données est leurs véracités *(sont-elles vraies)*. Une partie de ce critère peut être gérer par la transparente et la logique de transaction blockchain, mais aussi par l'encapsulation des fonctionnalités d'enregistrement. La blockchain nous donne la possibilité de faire que ce dont on le droit, en utilisant le principe de la cryptographie de double clé.

Le quatrième avantage est la forte dépendance du système à tous les membres. Ce n'est pas la blockchain seule qui souhaite une participation correcte de plus que de la moitié des nœuds qui la compose, mais la traçabilité grâce à la blockchain aussi. Dans un système de traçabilité grâce à la blockchain, les responsabilités sont liées, du fait de la liaison des produits. Alors une collaboration avec un maillon X peut être néfaste pour la confiance envers une entreprise même si elle est sur des bonnes intentions dans le cas où le maillon X devient ou était déjà douté.

Le cinquième avantage d'un tel système de traçabilité est l'automatisation de transaction grâce aux contrats intelligents. Les autres systèmes de traçabilité peuvent s'ils sont informatiques, évidemment réagir avec des contrats intelligents dans le cadre d'élargissement des capacités de leurs fonctions, mais le problème derrière sera l'organisation des structures de données entre ces systèmes et la blockchain du contrat.

Inconvénients

Le premier inconvénient d'un système de traçabilité blockchain est la mise en place. Cet inconvénient peut se résumer en plusieurs points. La difficulté de la mise en place et le choix de la blockchain ainsi que la migration des données d'un système de traçabilité externe vers ce système basé sur blockchain.

3.4 Définition de notre système

La première partie de l'état de l'art 1, consiste à modéliser la chaine de production pour l'optimiser et la remettre en place. Les 3 premières phases sont essentielles à la minimisation de la dispersion, mais cela se passe en dehors du système. Dans le cadre de la définition de notre propre système, nous passons directement à la phase 3 qui est la définition du système de traçabilité.

3.4.1 Identification des produits

La maquette d'un produit est composé d'un **identifiant externe** qui caractérise le type de produit (*exemple : le code produit ou numéro de lot*) et paquet alimentaire qui constitue les informations concernant ce produit.

L'objectif d'un identifiant de produit est l'identification des lots de façon univoque. Dans la supplychain les produits sont souvent identifiées que par les codes produit ou les numéros de lot ou les dates de fabrication et d'expiration. Pour l'efficacité de la traçabilité, il n'y aura pas deux identifiants identiques dans notre système, chaque produit est identifiée de maniéré unique et distinctement de tous les produits du même type ou pas. Nous utiliserons une identification facile et basée sur 4 cases *voir figure 3.9* : identifiant entreprise donné par le système, numéro partie prenante dans cette entreprise, code produit, numéro de produit.

3.4.2 Authentification des produits

Présenter une preuve d'authenticité des produits peut être un plus dans la fiabilité des données. Dans notre système nous réservons un espace dans lequel les producteurs peuvent lier

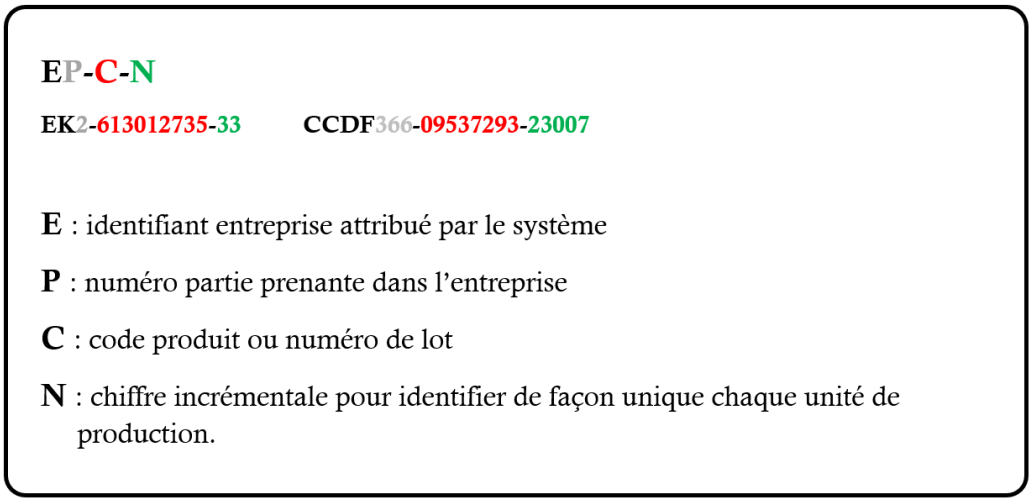


FIGURE 3.9 – Système d'identification de notre système de traçabilité

à leurs paquets alimentaires des certificats d'analyse effectués par des laboratoires de d'analyse certifiés sur dans la blockchain.

3.4.3 Généralisation des informations pour les maillons de la supply-chain

Pour la pertinence des données dans la chaine d'approvisionnement, il faut un minimum de généralisation. Nous avons pris des caractéristiques de produit fréquentes dans l'agroalimentaire. Ces caractéristiques sont celles imposées par le système, mais il offre la possibilité aux producteurs d'ajouter autant d'attributs à type de production pour plus de clarification. Les caractéristiques imposés dans les paquets alimentaires sont citées si-dessous :

— **Pour les produits agricoles** : date de semis, date de récolte, organisme génétiquement modifié, liste des produits souches, liste de produits chimiques utilisées dans l'agriculture.

— **Pour les produits d'élevage, sans compter le lait** : date de naissance, numéro de travail, race, identifiants des parents, maladies fréquentées, traitements reçus.

— **Pour les produits de pêche** : classification du produit, date de pêche, lieu de pêche, composition chimique.

— **Pour les produits de fabrication, y compris le lait** : date de production, étape de production, type d'emballage, identifiants uniques de chaque produits pères.

Pour finir, les 3 types de productions prises en charge auront en commun, identifiant unique du produit ou du produit ou lot de produit, un poids, une date limite de consommation, une liste des tests effectués sur le produit (*s'il en existe*), et la société de production.

3.4.4 Utilisation des contrats intelligents

Pour l'automatisation du système de traçabilité, nous proposons un espace de contrat où les parties prenantes peuvent déclarer des convention qui suivent les productions ou les échanges entre partie prenante du système, afin d'effectuer des transactions programmées ou par simple preuve d'engagement

— **Contrat de rappel** : pour permettre aux producteurs de prouver leurs volontés de fabrication qualité ainsi que pour gérer les rappels de maniéré rapide, nous proposons un espace dans le système qui permettrait à ces producteurs de prouver par un engagement à leurs clients sur un type de production donné, qu'ils rembourseront et ou fixer des engagements qu'ils tiendront en cas de rappels (*par exemple le remboursement à taux élevé ou pas de remboursement, ou des engagements de prise en charge pour les cas de consommation des produits rappelé etc.*).

  La mise en place des contrats de rappel n'est pas obligé par le système. Mais elle offre plutôt une occasion aux producteurs de prouver leurs preuves d'engagements et aussi pour renforcer le climat de confiance avec leurs consommateurs.

— **Contrat d'échange ou de transport** : dans une vaste chaine d'approvisionnement, la relation entre les parties prenantes sont complexes. Nous proposons la surveillance automatique dans les échanges, ou chaque partie peut fixer des conditions à respecter tout le long de l'échange jusqu'à leurs signatures pour y mettre fin. *Exemple : un producteur de jambon qui exige sur ses fournisseurs que des bétails qui n'ont fréquentés aucune maladie durant les 3 dernières années. Ou la possibilité aux producteurs et les prestataires de services logistiques de fixer les termes pendant le transport des productions alimentaires.*

3.4.5 Encapsulation de la fonctionnalité d'enregistrement

Les transactions blockchain sont faites via des adresses, cela garantit la non répudiation de *qui a fait quoi*, mais sa ne garantit pas par contre qui est dernière l'opération faite via l'adresse. pour assurer qu'une adresse ne soit pas utilisée par la mauvaise entité, nous espace spécifique pour vérifier chaque opération faite dans le système, mais aussi pour attribuer le droit d'écriture à chaque adresse disposant un identifiant d'entreprise de production reconnu.

3.4.6 Utilisation des objets connectés

Les enregistrements automatiques par les objets connectés sont essentiels dans la traçabilité enfin de diminuer les erreurs de saisie et de fournir des informations essentielle sur les productions. Nous proposons un ajout possible d'objets connectées qui peuvent émettre des données en tant que partie prenante sous la responsabilité de l'adresse qui l'ajoute.

3.4.7 Utilisation des systèmes externes opérant sur la blockchain

Un bon système de traçabilité doit aussi pouvoir contrôler l'authenticité des entreprises ainsi que la fiabilité liée à leurs enregistrements. Pour assurer ces contrôles sans perdre la logique de la décentralisation, nous proposons l'authentification de certaines données par des systèmes externes tournant sur la blockchain. Les identifiants d'entreprise par le système d'identification des entreprises, les identifications produit par le système d'identification des produits, les certifications d'analyse sur les produit par un système de certification d'analyse.

Système d'identification des entreprises : il est destiné aux autorités délivrant des identifiants d'entreprise *(comme ONS en Algérie qui délivre le NIS, ou INSEE en France qui délivre les SIREN et SIRET)*. Ce système permettra de certifier l'existence de l'identifiant d'une entreprise agroalimentaire ou un type de production (code produit ou numéro de lot) et leurs appartenances à une adresse ethereum.

Un système d'identification des produits : ce système d'identification est destiné aux entreprises comme le GS1 qui fournissent des GTIN pour identifier un type de production. Son rôle est d'attribuer des code d'identification des types de production et leurs associés à des adresse propriétaires.

Système d'analyse des produits : ce système concerne les laboratoires d'analyse comme *R-Biopharm*. Il permettra de certifier qu'un produit donné a subit un test donné par un laboratoire d'analyse donné.

3.5 conclusion

Dans ce chapitre nous avons présente un système de traçabilité standard basé sur l'optimisation du système, dont nous avons appris qu'il est important de diminuer la dispersion des produits et les informations dans un système de traçabilité pour avoir un temps de réaction rapide et un système moins complexe. Nous avons présente ensuite un système de traçabilité fonctionnant sur la blockchain, dont nous avons remarqué une vaste importance au profit du système précédent qui sont la factorisation des petits systèmes de traçabilité et l'encouragement des coopérations inter-entreprise dans la supplychain, la transparence, la fiabilité et la disponibilité continue des données, ainsi que l'extension facile du système, comme l'utilisation des contrats. Après nous définis notre système en tant que système de traçabilité basé sur la blockchain, en tenant compte des avantages et inconvénients des deux systèmes présentés. Notre système propose une solution basée sur 7 points clés. Chaque point regroupe une ou plusieurs fonctionnalités qui peuvent être classée selon les parties clés de notre système qui sont la chaine d'approvisionnement qui regroupe la chaine de production et de distribution, et comme deuxième partie, nous avons l'authentification des données qui sont dans la chaine d'approvisionnement.

Chapitre 4

Conception

4.1 Introduction

Dans le chapitre précédent, nous avons définit notre système de traçabilité en tenant compte des atouts et faiblesses de mise en place d'autre systèmes de traçabilité. Dans ce chapitre nous le mettons en œuvre. Pour le choix de la blockchain de notre système, nous utiliserons ethereum qui est une blockchain soutenue et sollicitée. C'est un réseau dont les nœuds sont capables à l'aide de leurs EVM (**E**thereum **V**irtual **M**achine) d'exécuter des **bytes codes** appelés des **contrats intelligents** (SC).

Les DApps pour **App**lications **D**écentralisées sont des systèmes logiciels qui utilisent généralement la blockchain comme support pour stocker et échanger des informations via des contrats intelligents. Dans le cadre de la mise en place de notre système, nous développerons un DApp. Un système de DApps complet est divisé en deux parties : une partie back-end qui regroupe les composants de la blockchain *(contrats intelligents, bibliothèques, structures de données)* et une partie front-end qui regroupe les applications d'interaction avec l'utilisateur *(comme les applications web, mobiles ou bureaux).*

La production des logiciels blockchain manque encore d'un processus de développement discipliné, organisé et mature [9]. Nous procèderons par une méthode de développement DApps mieux réfléchie, la méthode **ABCDE** pour **A**gile **B**lo**C**kchain **D**Apps **E**ngineering. C'est une méthode base sur le framework Scrum utilisant des pratiques Agiles. La méthode conserve les concepts de Scrum comme : les users stories, la découpe du projet en itération ou sprint, les rôles à savoir (le product owner, l'équipe de réalisation et le Scrum master) et les réunions de fin de sprint. La seule différence est qu'elle divise les activités de développement en deux flux à savoir la partie back-end avec les contrats intelligents et la partie front-end avec une application externe qui interagit avec la blockchain.

4.2 Développement avec la méthode ABCDE

Les étapes de la méthode de conception ABCDE, qui se concentre actuellement sur la blockchain Ethereum et le langage Solidité, sont illustrées à la *figure 4.1.* La plupart des étapes sont exécutées plusieurs fois, car l'approche est itérative et incrémentale (*Scrum*).

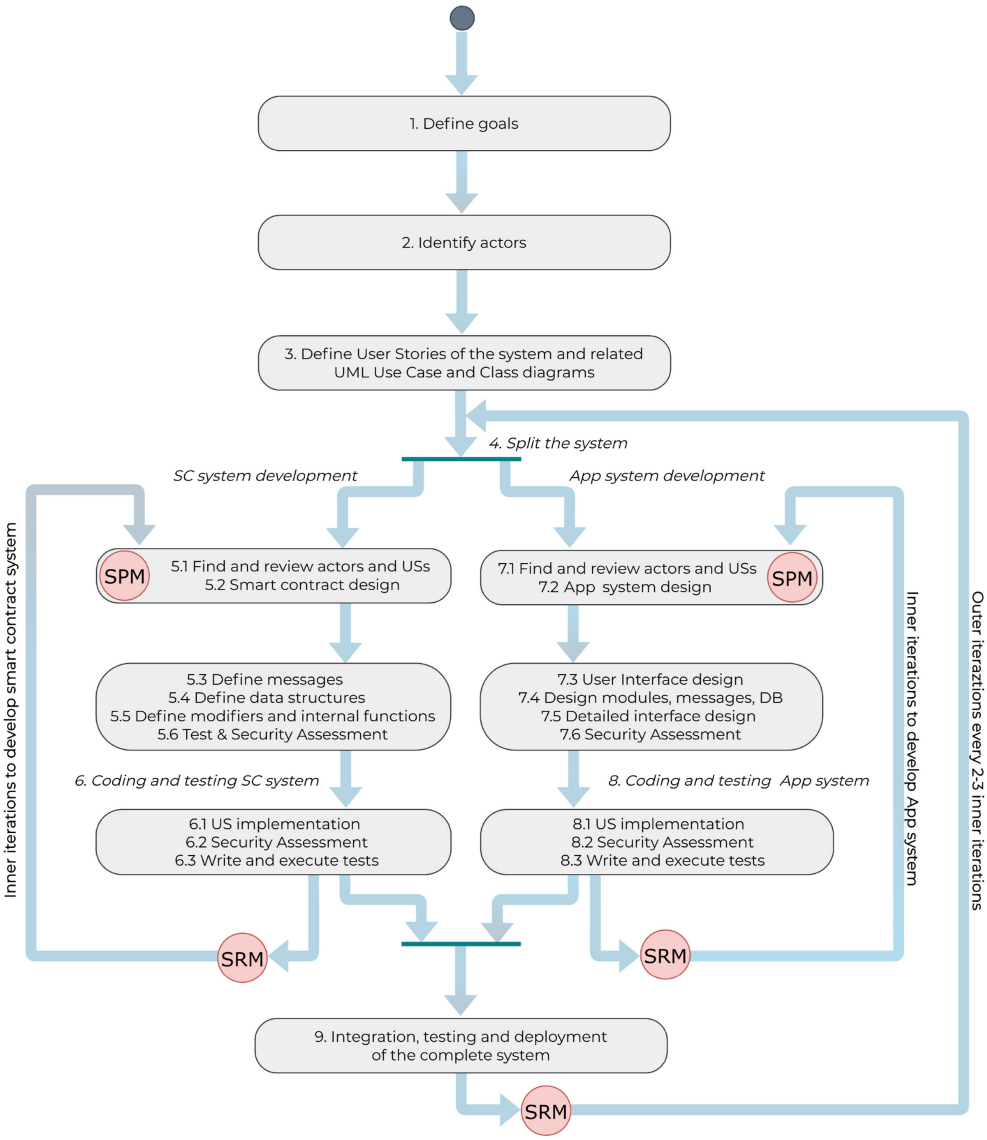


FIGURE 4.1 – Processus ABCDE [9]

Dans la figure :

— Les cercles roses présentes les réunions de planification de sprint(SPM) tenues au début de chaque sprint.

— Les réunions de révision de sprint (SRM) tenues à la fin de chaque sprint.

4.2.1 Objectif du système

Comme défini dans le chapitre 3, notre système doit assurer deux choses principales, à savoir l'authentification des données liées à la supplychain et la gestion de la supplychain, ces deux aspects sont importants d'un système de traçabilité efficace. Le premier sous objectif est la ges-

tion de la chaine d'approvisionnement : (gérer les productions et les distributions, les espaces de production ou de distribution et les activités de coopération entre les parties prenantes). Et le deuxième sous objectif est l'authentification des données via des systèmes externes ou directement dans le système.

4.2.2 Identification des acteurs

Les acteurs de notre système sont le public, et les acteurs qu'on peut rencontrer dans la supplychain : à savoir les producteurs, les prestataires de service logistique (distributeur ou transporteur), et les contrats intelligents qui interviennent dans notre système.

Les visiteurs

Un système de traçabilité efficace doit être transparent, les consommateurs doivent pouvoir voir les évènements et les actions subit par les produits. Pour assurer ce concept, il faut que les informations liés aux produits soient accessibles facilement et sans restriction. Cette raison fait du public l'acteur de base de notre système. Ils peuvent retrouver un toutes les informations nécessaires liés à un identifiant de produit ou partie prenante ou d'espace de travail.

Les parties prenantes

Ces sont les acteurs qui ont le droit d'écriture dans la blockchain. Elles le deviennent par appropriation d'un espace d'enregistrement ou par intégration dans un espace d'enregistrement. Parmi elles nous avons :

- **Les producteur** : ce sont les acteurs qui interviennent dans la chaine de production. Ils assurent la traçabilité produit, en enregistrant l'ensemble des étapes franchis par les produits dans les chaines de production.

- Les prestataire de service logistique : ce sont les acteurs qui interviennent dans la traçabilité logistique. Ils effectuent des enregistrement sur la logistique des produits *(les transports et les distributions)*.

Les contrats intelligents

Notre système repose de 3 contrats intelligents :

- **Supplychain :** c'est un contrat qui assure les enregistrements des parties prenantes sur les produits dans la blockchain.

- **Authentification** : c'est un contrat qui assure la fiabilité des données en interrogeant des contrats externes. Il permet aussi de vérifier si une adresse donnée a le droit d'effectuer une opération donnée dans le système.
- **Convention** : c'est un contrat qui permet aux parties prenantes du système de fixer des conventions dans le but de surveiller automatiquement les échanges, les transports de produits, les rappels et les intégrations des nouvelles parties prenantes dans le système.

4.2.3 Définition des historiques d'utilisateur et les cas d'utilisation relatives

Un user story est un moyen d'exprimer le besoin des utilisateurs dans le système de manière très simple et claire.Cette partie montre les acteurs et les user stories dans lesquelles ils sont impliqués, et des diagrammes use case pour appuyer la compréhension.

Historiques d'utilisation du public

En tant que	visiteur
Je veux	scanner un identifiant ou le saisir dans le système
Afin de	consulter les informations liées à cet identifiant. *(voir figure 4.2)*

Test d'acceptance

— Si l'identifiant entré existe dans la blockchain.

Résultat : je reçois le résumé de toutes les informations liées à l'identifiant.

FIGURE 4.2 – Cas d'utilisation consulter système

En tant que	visiteur
Je veux	déclarer mon entreprise dans le système
Afin de	avoir un espace d'enregistrement (EE). *(voir figure 4.3)*

Test d'acceptance

— Si je possède une adresse ethereum
— Si le système externe d'identification des entreprises reconnait l'identifiant de l'entreprise saisie
— Si le système externe d'identification des entreprises reconnait mon adresse comme l'adresse propriétaire de l'identifiant de l'entreprise
— Si cet identifiant d'entreprise n'est utilisé qu'une dans le système

Résultat : mon espace sera créé avec comme propriétaire mon adresse, qui disposera de tous les droits d'enregistrement sur cet espace en fonction de son type.

FIGURE 4.3 – Cas d'utilisation déclarer espace d'enregistrement

En tant que	visiteur
Je veux	signer une convention de participation à un espace de travail
Afin de	être une partie prenante dans cet espace. *(voir figure 4.19)*

Test d'acceptance

— Si mon adresse correspond à celle de la partie prenante à initier

Résultat : mon adresse sera ajouté dans l'unité d'organisation par défaut *(nouveaux partie prenante : qui n'a aucun rôle d'enregistrement dans cet espace)*.

Historique d'utilisation d'un producteur

En tant que	producteur
Je veux	définir un nouveau modelé de produit
Afin de	l'utilisé pour instancier les paquets alimentaire dans la déclaration des produits. *(voir figure 4.5 et 4.5)*

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration dans l'espace depuis lequel j'enregistre
— Si le système externe d'identification de produit reconnait l'existence du code produit et son appartenance à l'adresse propriétaire de l'espace depuis lequel j'enregistre
— Si le code produit n'est pas déjà en utilisation dans l'espace depuis lequel j'enregistre
— Si le nouveau type de production n'a pas un attribut déjà imposé par le système

Résultat : le modèle de produit sera disponible dans mon espace pour instancier et initialiser des nouveau paquet alimentaire des produits de ce modèle pendant leurs déclarations.

En tant que	producteur
Je veux	définir un nouveau modèle de lot de produit
Afin de	l'utiliser pour créer les paquets alimentaire dans la déclaration des produits. *(voir figure 4.6)*

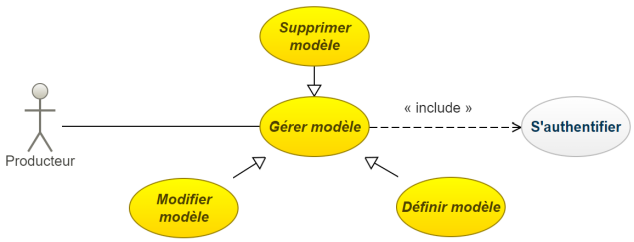


FIGURE 4.4 – Cas d'utilisation gestion de modèle de produit

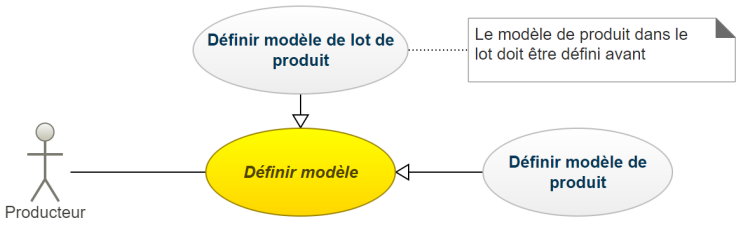


FIGURE 4.5 – Cas d'utilisation définition de modèle de produit et de lot de produits

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le système externe d'identification de produit reconnait l'existence du numéro de lot et son appartenance à l'adresse de mon espace de travail
- Si le numéro de lot de produit n'est pas déjà en utilisation dans le système
- Si le modèle de produit que contient le modèle de lot de produit est déjà défini dans mon espace

Résultat : le modèle de lot de produit sera disponible dans mon espace pour instancier et initialiser des nouveaux paquet alimentaire des lots de produits de ce modèle pendant leurs déclarations.

En tant que	producteur
Je veux	supprimer un modèle de produit
Afin de	arrêter la déclaration de ce type de produit dans mon espace d'enregistrement. *(voir figure 4.6)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de produit existe dans mon espace d'enregistrement
- Si le modèle de produit n'est pas utilisé dans un modèle de lot de produit

Résultat : le modèle disparaitra des modèles définis dans mon espace

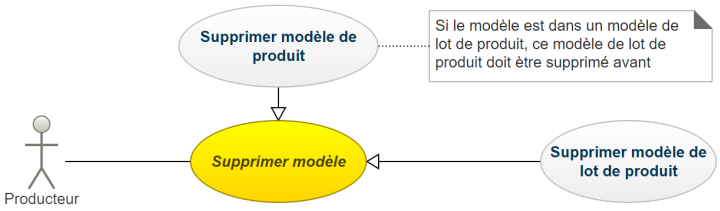


FIGURE 4.6 – Cas d'utilisation supprimer un modèle

En tant que	producteur
Je veux	supprimer un modèle de lot de produit
Afin de	arrêter la déclaration de ce type de produit dans mon espace d'enregistrement. *(voir figure 4.6)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de produit existe dans mon espace d'enregistrement

Résultat : le modèle disparaitra des modèles définis dans mon espace

---

En tant que	producteur
Je veux	ajouter un attribut à un modèle de produit ou de lot de produit
Afin de	le voir dans chaque paquet alimentaire qui dériveront de ce modèle *(voir figure 4.7)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de produit ou de lot de produit existe dans mon espace d'enregistrement
- Si cet attribut ne fait pas partie des attributs déjà exigés par le système
- Si cet attribut n'est pas déjà dans le modèle

Résultat : l'attribut sera ajouté, et tous les produits ou lots de produits de ce modèle qui vont être déclarer après l'ajout de l'attribut, auront le nouveau attribut dans leurs paquets alimentaires.

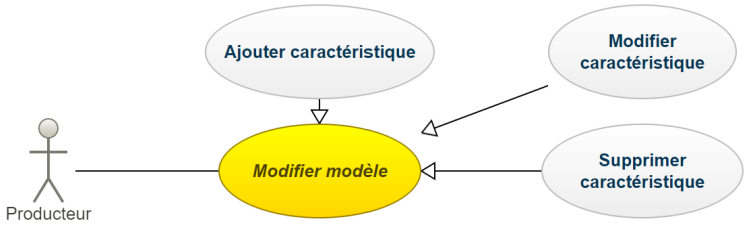


FIGURE 4.7 – Cas d'utilisation modification de modèle

En tant que	producteur
Je veux	modifier un attribut d'un modèle de produit ou de lot de produit *(voir figure 4.7)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de produit ou de lot produit existe dans mon espace d'enregistrement
- Si cet attribut existe dans le modèle
- Si c'est un changement de valeur dans le modèle, cet attribut doit être statique
- Si l'exigence du type de valeur est respecté

Résultat : l'attribut sera modifié, et tous les produits ou lot de produit déclarés après la modification, auront le changement dans leurs paquets alimentaires.

En tant que	producteur
Je veux	supprimer un attribut d'un modèle
Afin de	l'enlever des paquets alimentaires qui seront créer après la suppression. *(voir figure 4.7)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de lot produit existe dans mon espace d'enregistrement
- Si cet attribut existe dans le modèle
- Si cet attribut n'est exigé par le système

Résultat : l'attribut disparaitra du modèle, et tous les produits déclarer après la suppression, n'auront plus cet attribut dans leurs paquets alimentaire.

En tant que	producteur
Je veux	déclarer un produit
Afin de	lui attribuer un paquet alimentaire *(voir figure 4.8)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le modèle de produit existe dans mon espace d'enregistrement
- Si la liste des produits pères ne contient pas des identifiants de paquet alimentaire non reconnus dans le système
- Si la liste des produits pères ne contient des identifiants dont les paquet alimentaire qui ne sont pas près ou déclarer comme clôturer

Résultat : un paquet alimentaire est créé pour le produit avec un identifiant unique généré par le système pour faire la jointure du paquet alimentaire avec le produit physique.

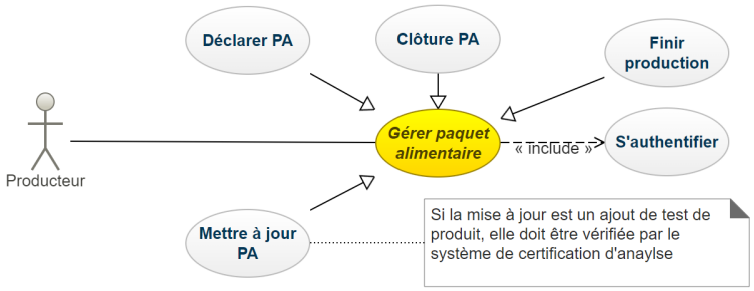


FIGURE 4.8 – Cas d'utilisation gestion de paquet alimentaire

En tant que	producteur
Je veux	mettre à jour un paquet alimentaire *(voir figure 4.8)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le paquet alimentaire existe dans mon espace d'enregistrement
- Si le paquet alimentaire appartient à mon espace de travail
- Si les champs à modifier existent
- Si les champs à modifier ne sont pas définis comme des champs statiques
- Si c'est un ajout de certification d'analyse, alors il doit être confirmé par le système externe de certification d'analyse de produit

Résultat : les valeurs des attributs seront modifiées dans le paquet alimentaire.

En tant que	producteur
Je veux	déclarer un produit comme prés
Afin de	indiquer qu'il a terminé l'étape de production *(voir figure 4.8)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le paquet alimentaire existe dans mon espace d'enregistrement
- Si le paquet alimentaire n'est déjà pas déclarer comme prêt

Résultat : aucun enregistrement dans la chaine de production ne peut encore être effectué sur le paquet alimentaire.

En tant que	producteur
Je veux	déclarer un produit comme clôturé
Afin de	indiquer qu'il est déjà consommé *(voir figure 4.8)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si le paquet alimentaire existe dans mon espace d'enregistrement
- Si le paquet alimentaire n'est pas déjà clôturé

Résultat : aucun enregistrement ne peut être effectué sur le paquet alimentaire.

En tant que	producteur
Je veux	rappeler des produits
Afin de	alerter le système et de rendre ces paquets alimentaires inutilisable *(voir figure 4.9)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si les paquets alimentaires existent
- Si le paquet alimentaire appartiennent à mon espace d'enregistrement

- Si le paquet alimentaire n'est pas déjà clôturé

Résultat : aucun enregistrement ne peut être effectué sur le paquet alimentaire.

FIGURE 4.9 – Cas d'utilisation rappel

Historique d'utilisation d'un prestataire de service logistique

En tant que	prestataire de service logistique
Je veux	signaler un transport de produit
Afin de	d'ouvrir un dossier de transport *(voir figures 4.10, 4.30)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si les paquets alimentaires ciblés pour le transport existent dans mon espace d'enregistrement ou si j'ai signe une convention pour transporter ces produits

Résultat : un dossier de transport sera ouvert, et mis à jour régulièrement *avec les conditions des produits* après chaque 6 blocs

FIGURE 4.10 – Cas d'utilisation rappel

En tant que	prestataire de service logistique
Je veux	signer une convention de transport de produit
Afin de	entamer un procédure de transport

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration
— Si la convention est déjà signée par un producteur
— Si l'adresse du transporteur dans la convention est la mienne

Résultat : la convention sera mise en vigueur avant de signaler un transport de produit

Historique d'utilisation d'une partie prenante (producteur et prestataire de service logistique)

En tant que	partie prenante
Je veux	rédiger une convention de rappel sur un modèle de produit
Afin de	de le signer pour le mettre en vigueur en tenant la blockchain comme témoin

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration
— Si le modèle de produit appartient a mon espace

Résultat : la convention sera mise dans mon espace et pourra être déclenche avec une signature du propriétaire de l'espace.

En tant que	partie prenante
Je veux	m'authentifier
Afin de	avoir une session afin d'enregistrement dans le système *(voir figure 4.11)*

Test d'acceptance

— Si mon adresse fait partie d'un espace
— Si mon adresse n'a pas une session ouverte
— Si ma phrase d'ouverture de session est correct

Résultat : mon adresse aura une session pour effectuer des enregistrements. La session se ferme

après 3 blocs d'inactivité

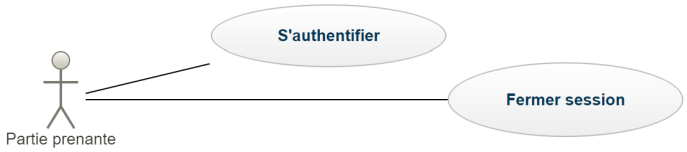


FIGURE 4.11 – Cas d'utilisation gestion session

En tant que	partie prenante
Je veux	fermer une session
Afin de	retirer le droit d'enregistrement de mon adresse *(voir figure 4.11)*

Test d'acceptance

— Si mon adresse appartient à un espace
— Si mon adresse a déjà session

Résultat : mon adresse n'a plus le droit d'écriture dans la blockchain jusqu'à une nouvelle authentification

---

En tant que	partie prenante
Je veux	créer une unité d'organisation
Afin de	lui ajouter des parties prenantes et de leurs attribuer des rôles *(voir figure 4.12 et 4.13)*

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration
— Si cette unité d'organisation n'existe pas déjà dans mon espace

Résultat : un nouveau répertoire de partie prenante sera créé dans mon espace

---

En tant que	partie prenante
Je veux	créer un stock
Afin de	y ajouter et enlever des produits *(voir figure 4.14)*

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration

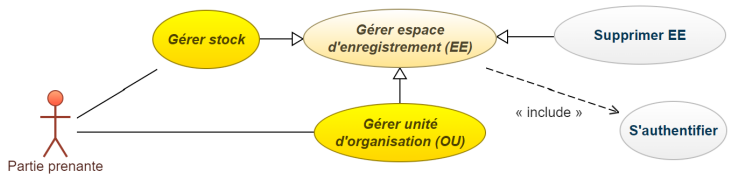


FIGURE 4.12 – Cas d'utilisation gestion d'espace d'enregistrement

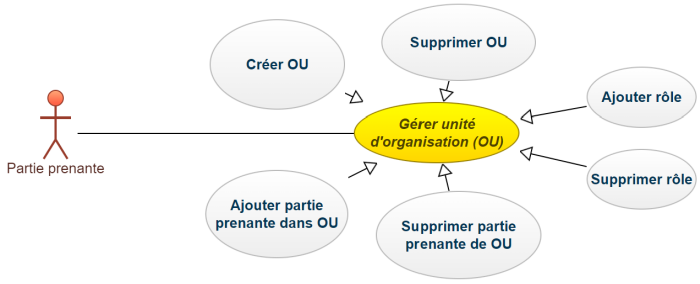


FIGURE 4.13 – Cas d'utilisation gestion unité d'organisation

— Si ce stock n'existe pas déjà dans mon espace

Résultat : Un nouveau répertoire de produit sera créé dans mon espace

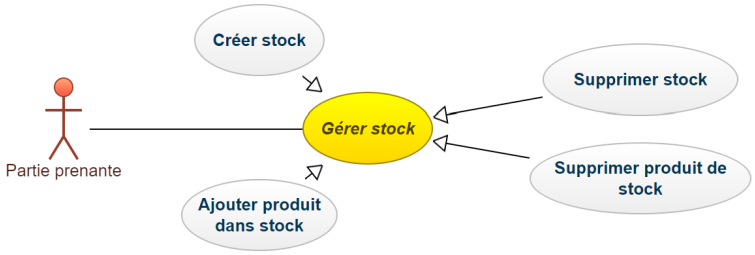


FIGURE 4.14 – Cas d'utilisation gestion stock

En tant que	partie prenante
Je veux	rédiger une convention d'échange entre deux adresses
Afin de	que les deux adresses puissent le signer pour leurs engager dans un contrat d'échange *(voir figure 4.15 et 4.16)*.

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration
— Si les adresses de la convention sont toutes correctes

Résultat : une nouvelle convention sera créée et en attente de la signature des deux participants

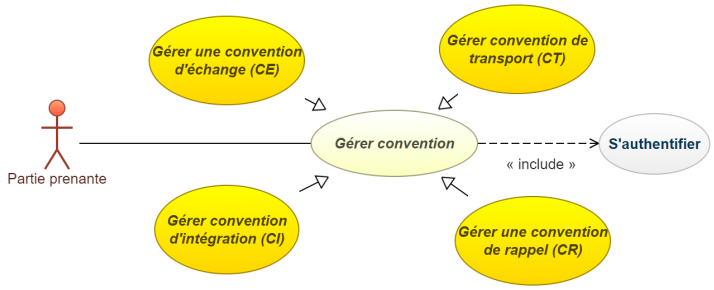


FIGURE 4.15 – Cas d'utilisation gestion conventions

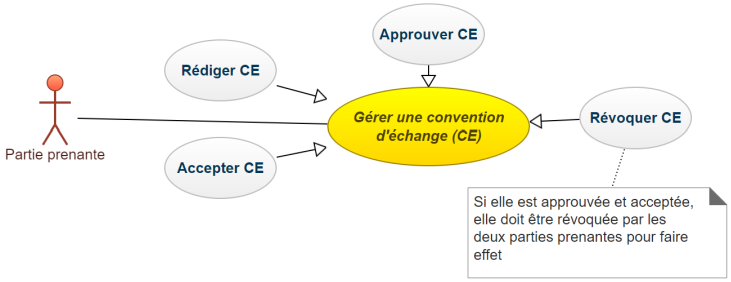


FIGURE 4.16 – Cas d'utilisation gestion convention d'échange

En tant que	partie prenante
Je veux	rédiger une convention de transport entre deux adresses
Afin de	que les deux participant puissent la signée pour de leurs engagés dans un contrat de transport *(voir figure 4.17)*.

Test d'acceptance

— Si mon adresse a une session
— Si j'ai ce droit d'administration
— Si les adresses de la convention sont toutes correctes
— Si au moins une des deux adresses est une adresse de prestataire de service logistique

Résultat : une nouvelle convention sera créée et en attente de la signature des deux participants

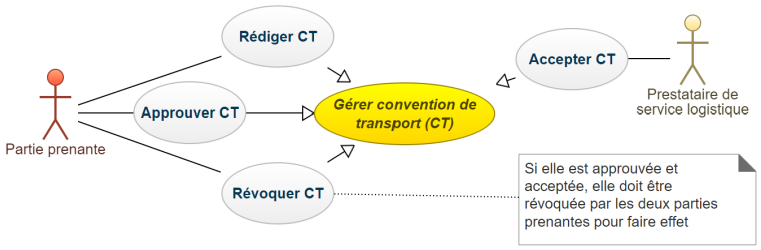


FIGURE 4.17 – Cas d'utilisation gestion convention de transport

---

En tant que	partie prenante
Je veux	signer une convention d'échange
Afin de	pour participer à cette convention *(voir figure 4.16)*

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si la convention est toujours valable
- Si mon adresse est dans la convention

Résultat : la convention collectera ma signature et se mettra en attente de celle de la partie prenante externe. Elle commencera à opérer après les deux signatures.

En tant que	partie prenante
Je veux	annuler une convention
Afin de	la rendre obsolète avant la signature de l'adresse externe

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si la convention est toujours valable
- Si la convention n'est pas déjà signer par la partie prenante externe
- Si je suis l'auteur de la convention

Résultat : la convention ne sera plus accessible.

En tant que	partie prenante
Je veux	approuver une convention de rappel sur un modèle de produit

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si la convention appartient à mon espace d'enregistrement

Résultat : une nouvelle convention de rappel sera activée, et exercée sur les produits du modèle déclarés après la signature de la convention.

En tant que	partie prenante
Je veux	approuver une convention d'intégration d'une adresse
Afin de	ajouter cette adresse comme partie prenante dans mon EE *(voir figure 4.19)*.

Test d'acceptance

- Si mon adresse a une session
- Si j'ai ce droit d'administration
- Si mon adresse est désigné par le contrat

Résultat : mon adresse sera considéré comme une partie prenante de l'espace d'enregistrement du créancier, après avoir configurer mon mot de passe.

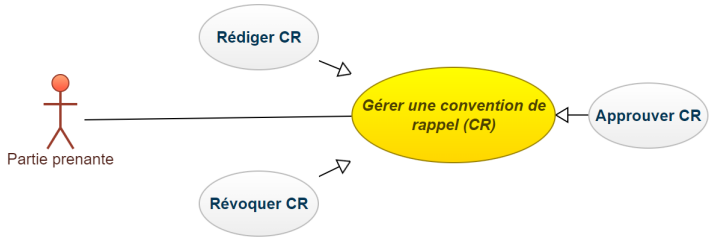


FIGURE 4.18 – Cas d'utilisation gestion convention de rappel

4.2.4 Division du système

L'application est repartie en deux sous système, le sous système SC qui contient l'infrastructure blockchain : à savoir l'ensemble des contrats, les structures de données dans les contrats, ainsi que les transactions effectuées entre ces contrats et provenant du système externe). Le sous système de relais contient l'infrastructure web, qui consiste l'ensemble des librairies et framework utilisés, les dépendances, ainsi que l'ensemble des interfaces pour rendre l'application mieux utilisable.

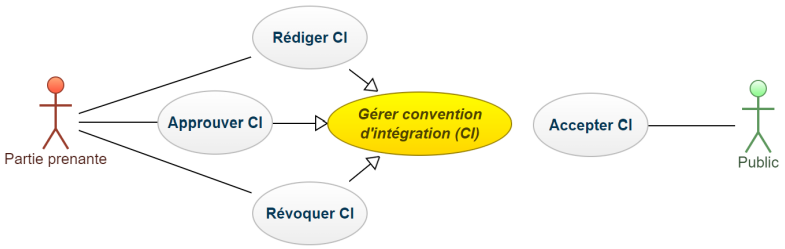


FIGURE 4.19 – Cas d'utilisation gestion convention d'intégration

4.2.5 Conception du sous système SC

Contrat de la chaine d'approvisionnement

Nous avons déjà défini les SC qui interviennent dans notre application pendant l'identification des acteurs, dans cette étape , nous allons concevoir ces SC. Contrairement à la définition des user stories, nous allons regroupé les cas d'utilisation par contrat et non par entité. Nous concevons chaque contrat avec en tenant compte des structures nécessaires et des fonctions qu'il exécute. Nous ne montrons pas les modificateurs, les émissions ainsi quelle que certaines fonctions internes qui n'intervient pas directement dans les traitements d'information. Nous avons omis en plus le contrat outil, qui sert de conversion de type. Nous définissons par contre l'ensemble des fonctions montrées dans les contrats comme des fonctions externes au lieu de publiques, dans le cadre de l'optimisation des coûts de transaction. Dans les interactions, nous modélisons que les actions qui partent des parties prenantes, mais certaines actions déclenchés par contrat son consignées dans les diagrammes de classes.

Nous avons trois SC (supplychain, authentification, et convention), chaque contrat réagit avec les deux autres via des interfaces qu'il propose.

Contrat de la chaine d'approvisionnement

Nous commençons par le traitement des enregistrements des parties prenantes dans la supplychain. Chaque partie prenante (les producteurs et les prestataires de services logistiques) après avoir reçu une habilitation du contrat authentification peut effectuer des enregistrements dans la blockchain via le contrat supplychain. Ce contrat couvre le nécessaire des enregistrements qui peuvent être effectués par les parties prenantes. Par enregistrement :

— un producteur peut définir un modèle de produit ou de lot de produit *(voir figure 4.19).*
— Mettre à jour un modèle.
— ajouter ou modifier ou supprimer des caractéristique a un modèle.
— Déclarer un produit *(voir figure 4.20).*
— Mettre à jour un paquet alimentaire *(voir figure 4.21)*
— Rappeler un produit.
— Et un prestataire de service logistique peut tenir un rapport de transport de produit.
— Les deux parties prenantes peuvent gérer des stocks pour gérer facilement leurs productions *(voir figure 4.22 et 4.23).*
— le mettre à jour (figure x).

— ajouter et enlever des produits dans des stocks.

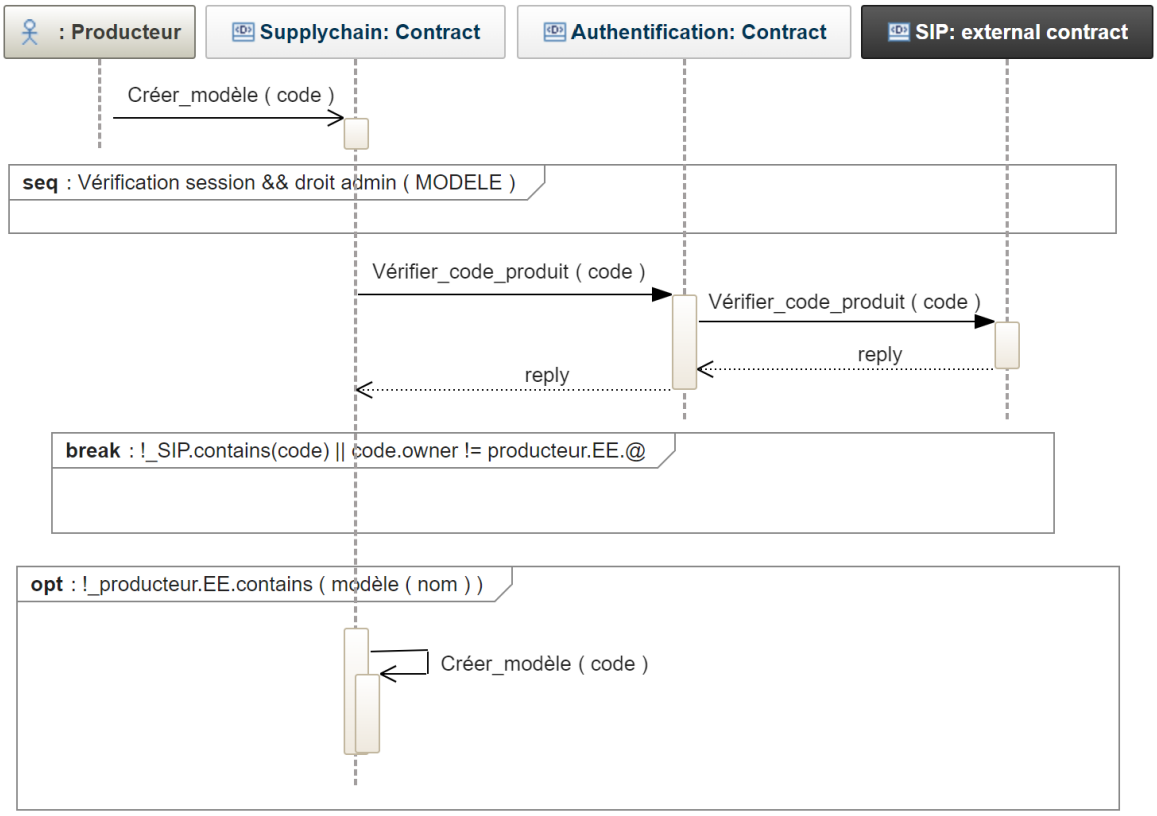


FIGURE 4.20 – Diagramme de séquence : Définition d'un modèle de produit

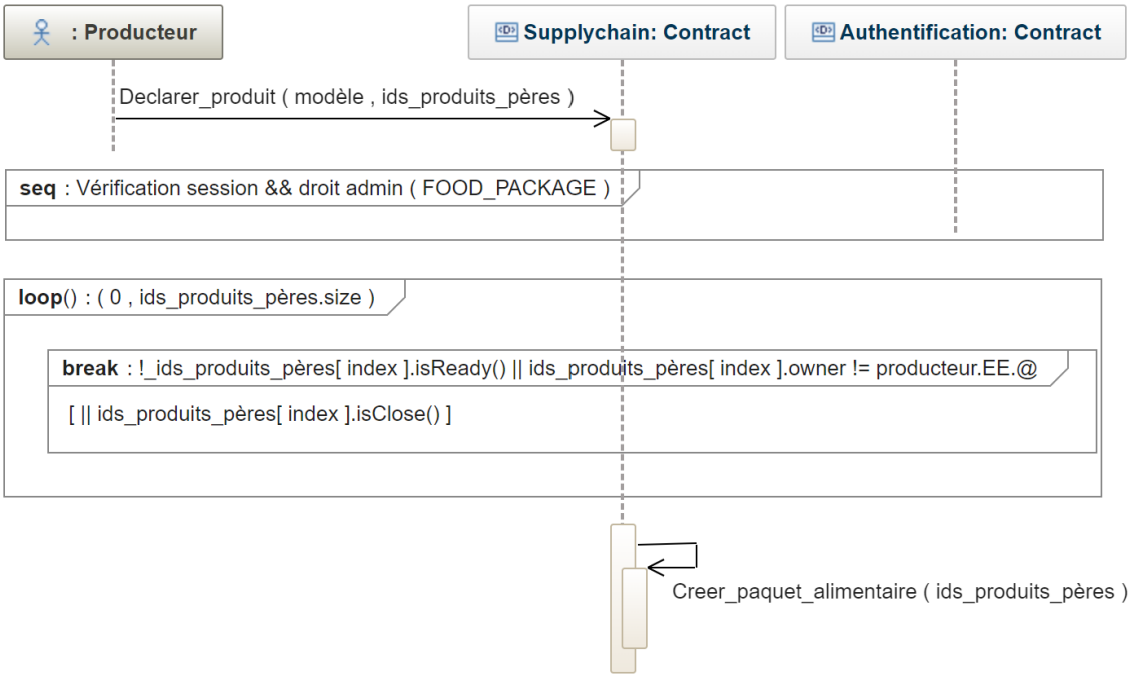


FIGURE 4.21 – Diagramme de séquence : Déclaration d'un produit

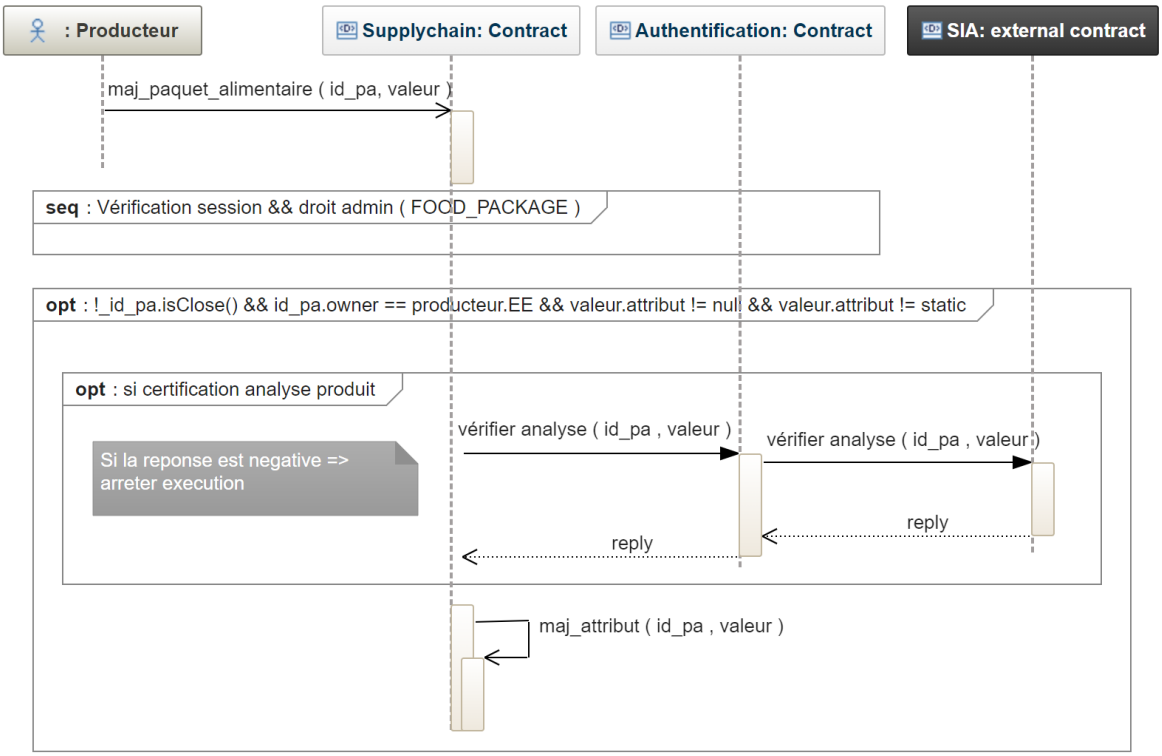


FIGURE 4.22 – Diagramme de séquence : Mise à jour d'un paquet alimentaire

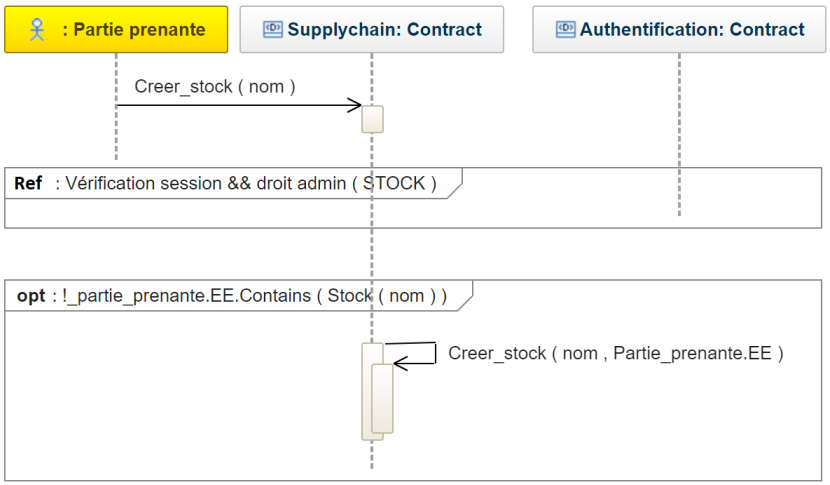


FIGURE 4.23 – Diagramme de séquence : Création d'un stock

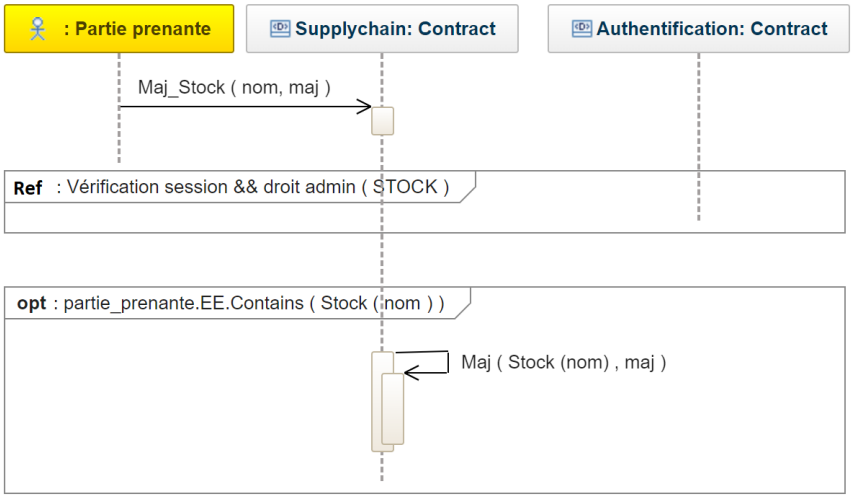


FIGURE 4.24 – Diagramme de séquence : Mise à jour d'un stock

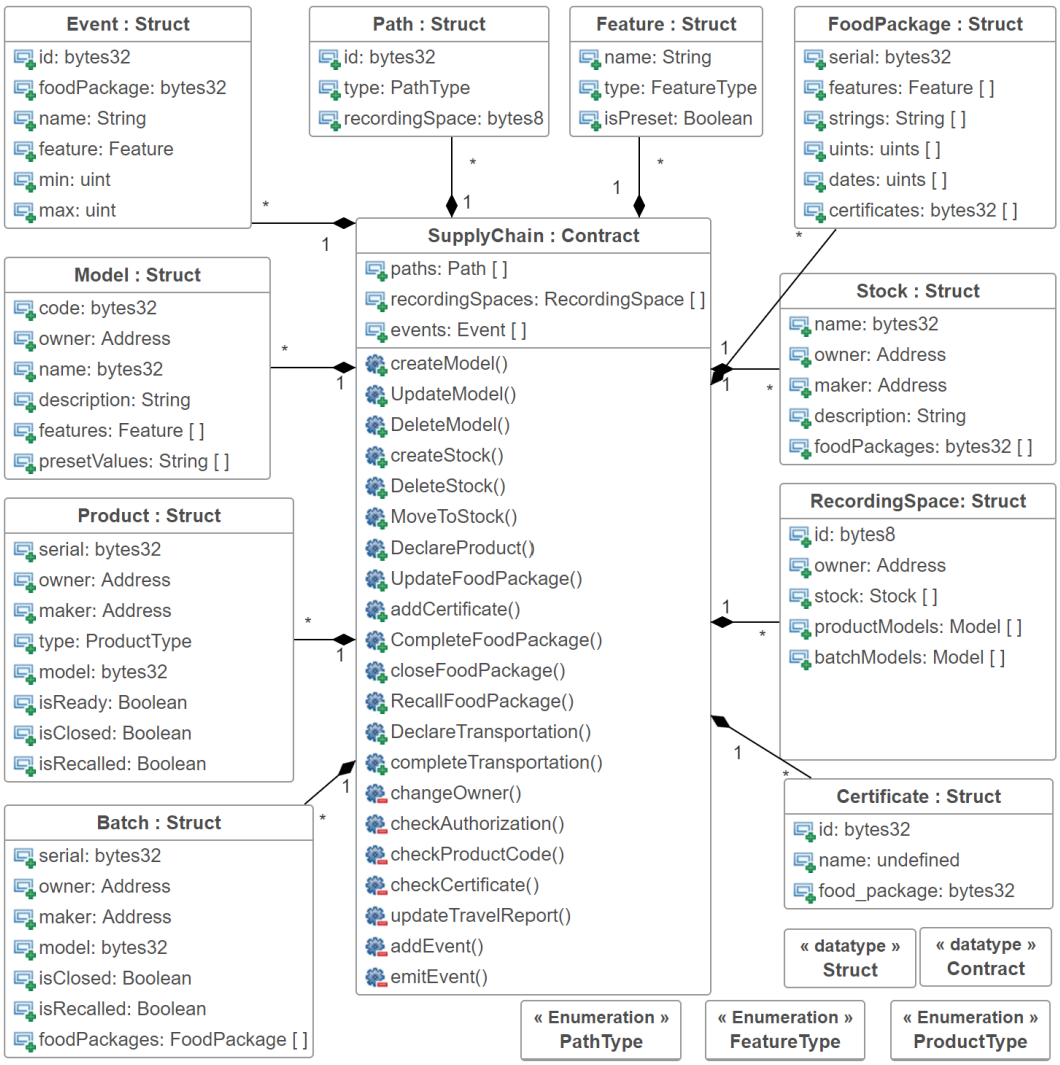


FIGURE 4.25 – Diagramme de classe : Contrat chaine d'approvisionnement

Visitez le contrat intelligent Supplychain via le lien suivant :

https://github.com/coulibaly1212/-DApp-for-food-traceability/blob/master/contracts/Supplychain.sol.

Contrat d'authentification

Avant chaque enregistrement le contrat supplychain doit demander une approbation du contrat authentification qui doit assurer la crédibilité de la partie prenante en disant si elle a une session et qu'elle fait partie d'une unité d'organisation dans son espace d'enregistrement qui lui attribut le droit d'effectuer l'enregistrement qu'elle demande. Aussi il s'assure que les données à enregistrées sont fiables en effectuant des vérifications dans des contrats externes au système.

— Un visiteur (public) peut déclarer un espace d'enregistrement.
— Une partie prenante peut s'authentifier.
— Une partie prenante peut fermer sa session.
— Une partie prenante peut ajouter d'autre partie prenante

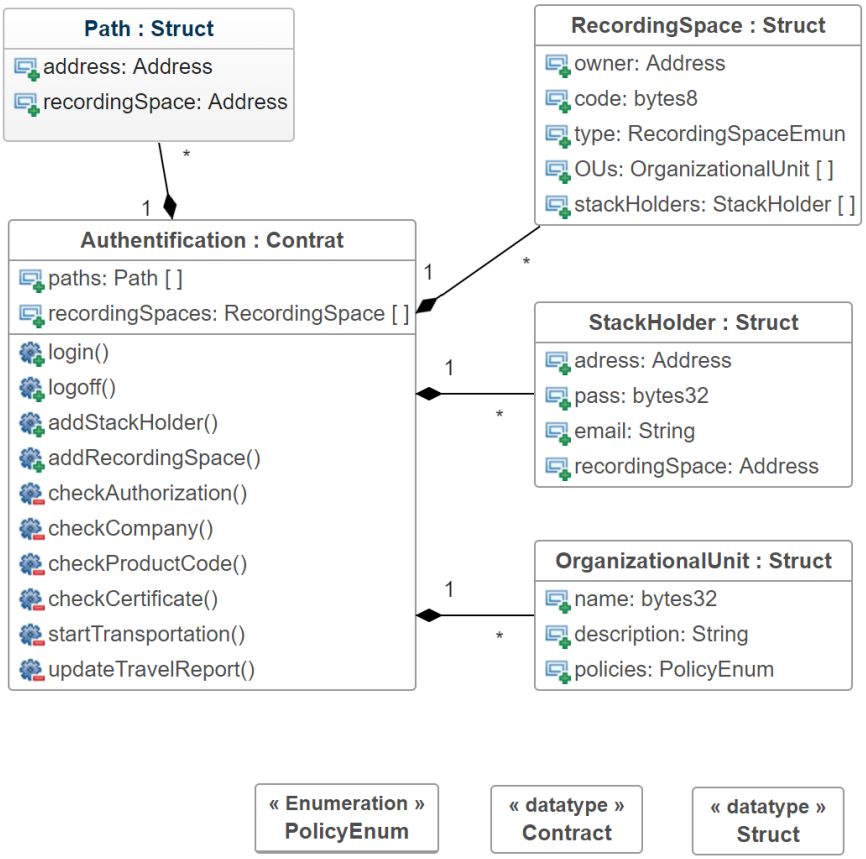


FIGURE 4.26 – Diagramme de classe : Contrat authentification

Visiter le contrat intelligent Authentification via le lien suivant :

https://github.com/coulibaly1212/-DApp-for-food-traceability/blob/master/contracts/Authentification.sol.

Contrat de convention

Pour finir nous concevons le contrat de convention qui permet entre autre de déclarer des conventions dans le but de simplifier les interactions des parties prenantes non automatiques. Le contrat de convention prend en charge 4 types de convention : pour intégrer une partie prenante, pour échanger, pour s'engager en cas de rappel et pour conclure une attente sur les conditions de transport. Par les actions dans un contrat de transport :

— Une partie prenante peut créer un modèle de convention dans le but de ne pas se reprendre.
— Une partie prenante peut instancier un modèle de convention.
— Une partie prenante peut activer une convention.
— Une partie prenante peut accepter une convention dans laquelle elle est citée.
— Une partie prenante peut clôturer une convention
— Deux parties prenantes peuvent interrompre une convention.

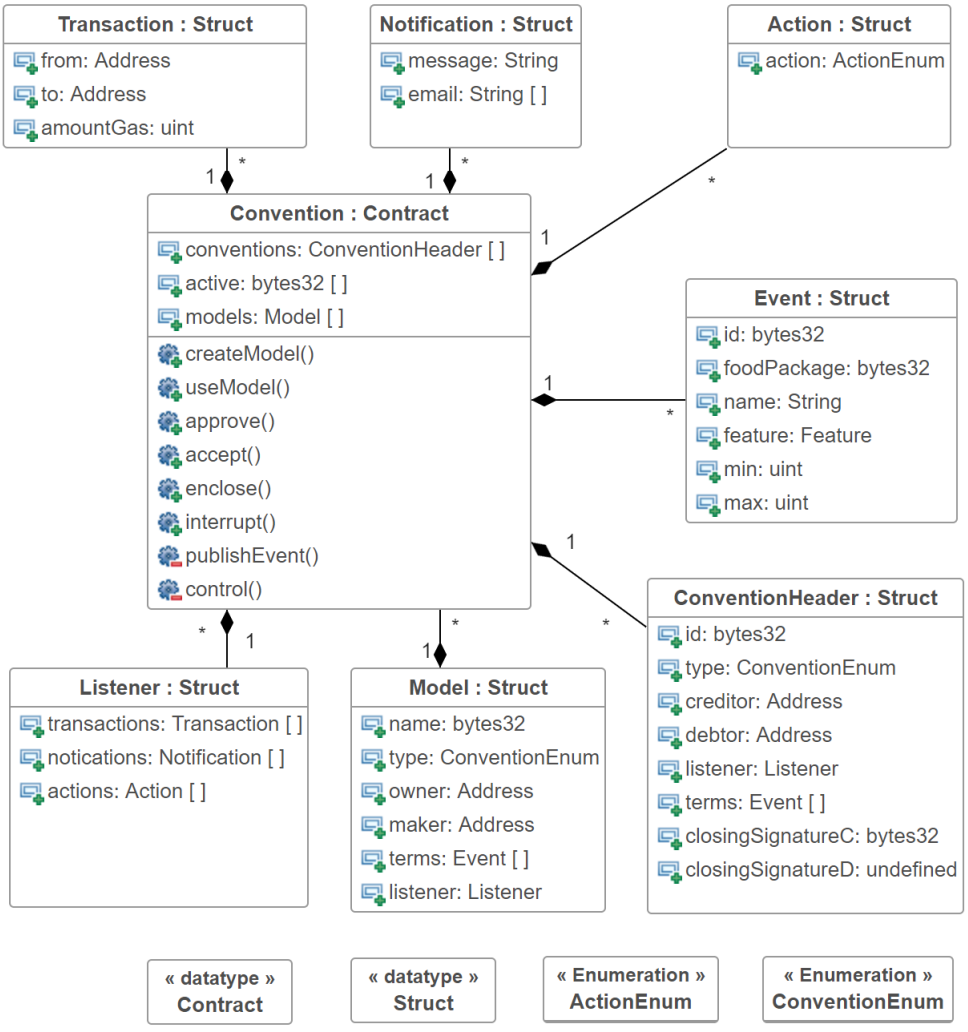


FIGURE 4.27 – Diagramme de classe : Contrat convention

Visitez le contrat intelligent Convention via le lien suivant :

https://github.com/coulibaly1212/-DApp-for-food-traceability/blob/master/contracts/Convention.sol.

4.2.6 Conception du sous système App

Dans cette partie nous allons concevoir l'application web. Cette application Web permettra de jouer le pont entre les wallets des parties prenantes et la blockchain, elle doit être associée à un portefeuille capable de stocker des Ethers et d'envoyer des transactions à la blockchain Ethereum *(figures 4.27, 4.28, et 4.29)*. Chacun des interactions et enregistrements présentés dans les SC est représentés dans cette application sous forme graphique.

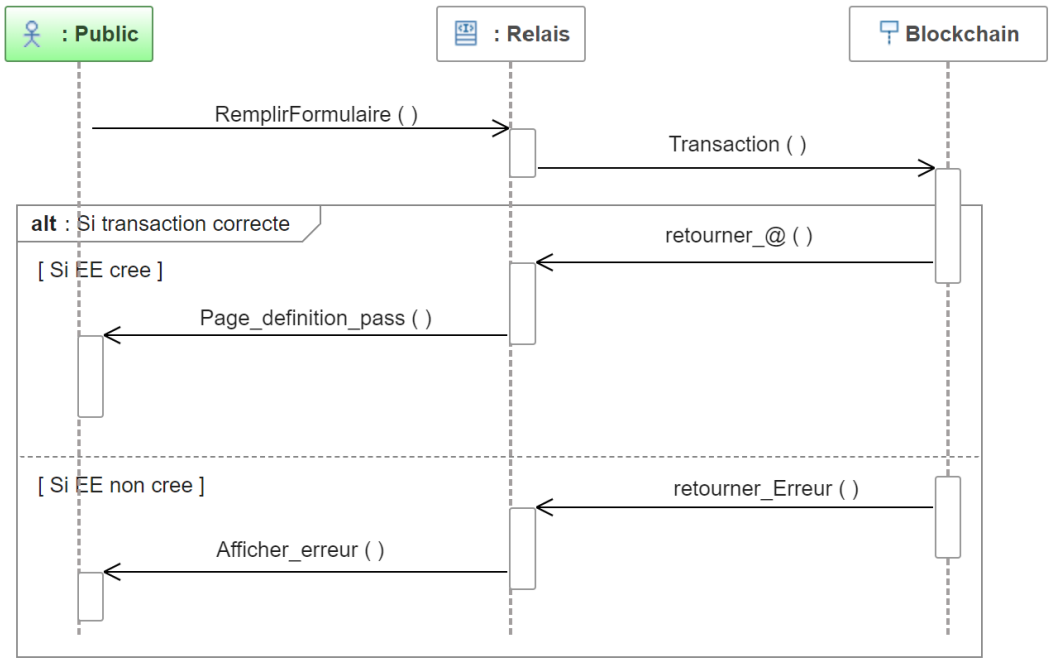


FIGURE 4.28 – Diagramme de séquence : Réservation d'un espace d'enregistrement, vue du coté Web

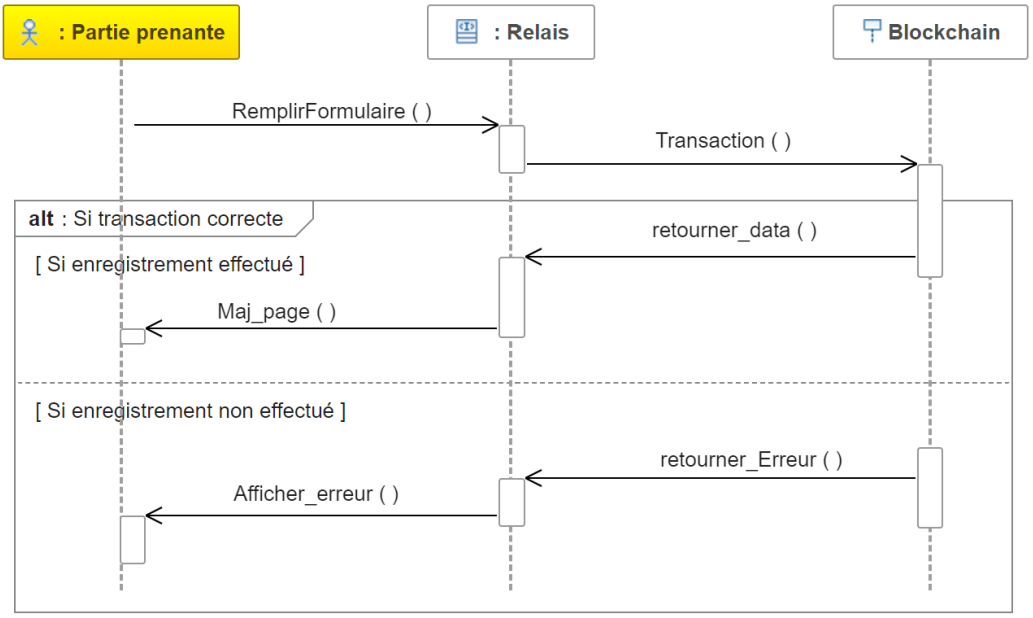


FIGURE 4.29 – Diagramme de séquence : Procédure d'enregistrement par une partie prenante, vue du coté Web

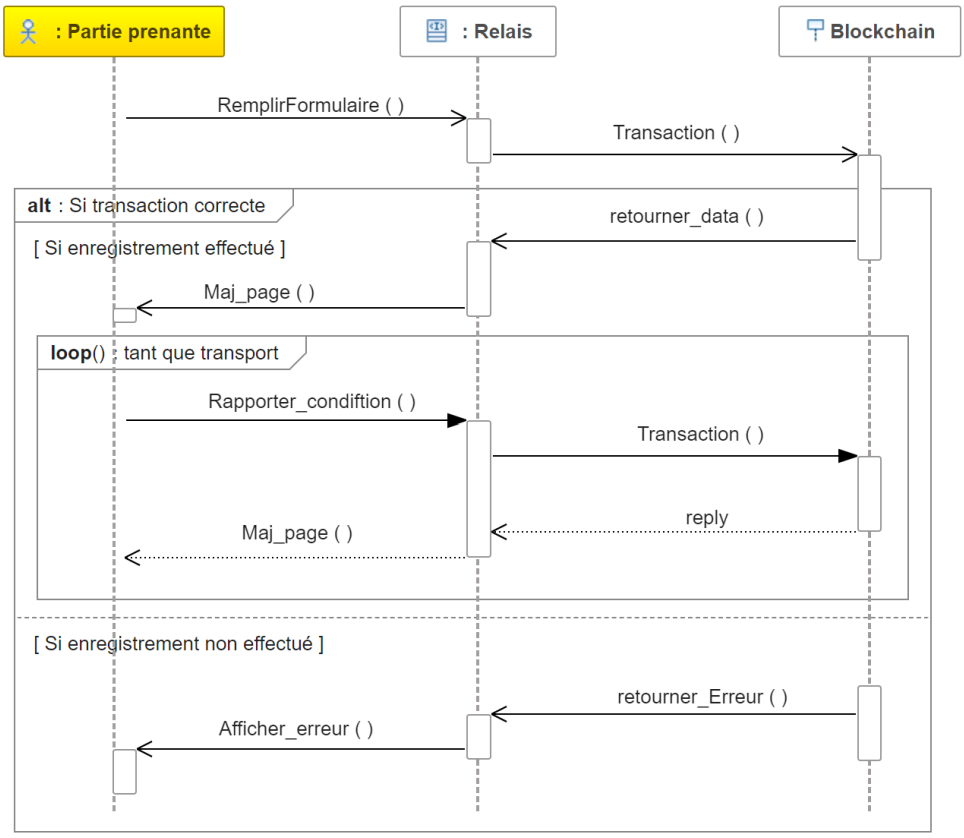


FIGURE 4.30 – Diagramme de séquence : Procédure transport produit, vue du coté Web

Pour l'architecture de l'application Web, nous optons pour l'architecture MVC. **M**odel **V**iew **C**ontroller, est une architecture efficace dans la réalisation des applications Web dynamiques. Il a pour objectif est de séparer les aspects de traitement, des données et des présentation. Elle structure une application Web en 3 modules :

— Le modèle qui permet de gérer les données. Il récupère les informations dans la base de données *(la blockchain pour notre application)* et les passer au contrôleur.

— La vue qui permet d'afficher les données via des des composants graphiques.

— Et le contrôleur qui assure l'intermédiaire entre le modèle et la vue. Il récupère les données dans le modèle et les affichées grâce la vue. Il comporte la partie traitement des données en plus de la récupération et le passage à l'affichage.

ReactJS

React est une bibliothèque javaScript utilisé dans les construction d'interface utilisateur. Dans le cadre de la réalisation de l'application nous utiliserons react pour la partie interface utilisateur.

Web3.js

Web3.js est une collection de librairies qui permettent d'interagir avec un nœud ethereum via le protocole HTTP, IPC ou WebSocket. Nous l'utiliserons comme pont vers la blockchain.

4.3 Conclusion

Nous avons basé notre système sur la blockchain ethereum. Dans ce chapitre nous avons fait une conception de notre DApp, dans laquelle nous avons utilisé une la méthode ABCDE. Nous avons commencé par lister les actions possibles qui peuvent être effectuées dans notre DApp. Nous avons commencé par concevoir la partie back-end dans laquelle nous avons listé les enregistrements possibles par les acteurs du système. Et la partie front-end dans laquelle nous avons montré un aperçu globale de la connection de l'application Web à la partie blockchain.

Conclusion générale

Ce document se porte principalement sur la technologie blockchain et son application dans la traçabilité alimentaire. Dans cette solution, nous avons commencé par présenter la technologie blockchain dans le chapitre 1. Nous avons présente des concepts nécessaires pour la compréhension de la blockchain avant de passer à son fonctionnement, dans lequel nous avons présenté l'idée derrière la technologie *(qui consiste à passer vers un système de transaction qui nécessite pas le besoin de tiers de confiance)*, et ses mécanismes, à savoir les procédures de transaction, et de la notion de preuve. Après nous sommes passés à sa structure avant de présenter quelque types de blockchain. Par la suite de cette étude nous avons conclu que la blockchain était la meilleure technologie de registre grâce à sa transparence et son mécanisme de consensus qui ne permet aucun moyens de triche.

Après l'étude de la blockchain, nous avons présenté le problème à résoudre dans le chapitre 2, en présentant le concept de la traçabilité. Âpres cette présentation, nous avons discuté des deux types de traçabilité établis avant de poser les problèmes de la mise en place de la traçabilité rencontrés par les acteurs de la traçabilité alimentaire. Par la suite nous avons présenté quelle que manières de traçabilité adoptées par les acteurs de la supplychain et terminer avec la maniéré que nous voulons utilisé.

Dans le chapitre 3, nous avons étudié deux systèmes de traçabilité différents. Le premier est un système de traçabilité mise en place dans une entreprise de saucisson, dans lequel nous avons appris qu'il est important de réduire le mélange, qu'il soit des produits ou des informations dans les deux chaines de traçabilité *(chaine de production et chaine logistique)*. Le deuxième est un système proposé qui est mise en place grâce à la technologie blockchain, dans lequel nous avons remarqué le large avantage du système de traçabilité mise en place grâce à la blockchain par rapport au premier système. Après, nous avons proposé notre système, en tenant compte des avantages et inconvénients, ainsi que les conseils des deux systèmes présentés.

Pour finir, dans le dernier chapitre, nous avons procédé à la conception de notre système, dans laquelle nous avons décidé de créer une DApp supervisée par une méthode développement blockchain nommé ABCDE. Dans le cadre de la conception, nous avons commencé par lister et modélisé toutes les actions possibles des acteurs *(les parties prenantes et les contrats intelligents)* de la partie back-end. Pour finir nous avons effectué une modélisation globale de l'interaction de la partie front-end avec la blockchain, et nous avons listé les bibliothèques et framework utilisés dans la conception de cette partie front-end.

Bibliographie

[1] Satoshi, Nakamoto, *A Peer-to-Peer Electronic Cash System.* 2008

[2] Drescher, Daniel, *Blockchain Basics : A Non-Technical Introduction in 25 Steps.* 2017.

[3] Raúl Green, Michel Hy, *La traçabilité : un instrument de la sécurité alimentaire* . 2002.

[4] JEAN-LUC VIRUÉGA, *Traçabilité Outils, méthodes et pratiques* . 2005.

[5] developer.bitcoin.org

[6] Clément, Dupuy. *Analyse et conception d'outils pour la traçabilité de produits agroalimentaires afin d'optimiser la dispersion des lots de fabrication.* 2004.

[7] Scheer, A.-W. *ARIS : des processus de gestion au systeme integré d'applications.* 2002.

[8] Galvez, J. F., Mejuto, J. C., Simal-Gandara, J. (2018). *Future challenges on the use of blockchain for food traceability analysis.* TrAC Trends in Analytical Chemistry, 107, 222-232.

[9] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli ; Tonelli, Roberto. Abcde –agile block chain dapp engineering : *Research and Applications*, 1 :100002, 12 2020. doi :10.1016/ j.bcra.2020.100002.