Traçabilité du suivi des matières dangereuses dans les smart ports grâce aux technologies blockchain

Camille Simon, Claude Duvallet, Cyrille Bertelle, Jérôme Besancenot

TRAÇABILITE DU SUIVI DES MATIERES DANGEREUSES DANS LES SMART PORTS GRACE AUX TECHNOLOGIES BLOCKCHAIN

Camille Simon[(1)], Claude Duvallet[(1)], Cyrille Bertelle[(1)] et Jérôme Besancenot[(2)]

[(1)] Normandie Univ, UNIHAVRE, LITIS
25 rue Philippe Lebon - BP 1123
76063 Le Havre Cedex

[(2)] Direction des services informatiques
Haropa – Port du Havre
76600 Le Havre

Work in progress

Résumé :

L'accroissement des échanges de conteneurs à l'échelle mondiale amène les acteurs portuaires à repenser leur fonctionnement afin de fluidifier le passage portuaire en dématérialisant les documents de transport et de logistique tout en renforçant la traçabilité des marchandises.

Les solutions à base de blockchains offrent aujourd'hui une nouvelle façon d'échanger de l'information entre un ensemble d'acteurs tout en assurant la certification des données, l'automatisation de leur traitement et en renforçant la confiance que les acteurs peuvent avoir dans le système.

Dans cet article, nous présentons un modèle général de déploiement de ces technologies dans des transactions logistiques ; il est développé pour le cas d'usage de la traçabilité du transport des marchandises dangereuses.

Mots-clés : blockchain, traçabilité, logistique, certification, marchandises dangereuses, smart port.

1. INTRODUCTION

La mondialisation du transport maritime conteneurisé nécessite que les grandes places portuaires optimisent et fluidifient les processus de passage de la marchandise. La sécurisation des opérations est également un enjeu majeur dans le cadre de ces processus portuaires. À ce titre, une gestion efficace et fluide des conteneurs de marchandises dangereuses est une clé du développement de ces grandes places portuaires. Ces conteneurs sont soumis à des contraintes fortes en termes de traçabilité. Ils font obligatoirement l'objet de déclarations réglementaires avant leur arrivée et d'un suivi tout au long de leur présence au sein de l'espace portuaire.

Depuis quelques années, des systèmes d'information portuaires se développent sous le nom de Port Community System (PCS) ou Cargo Community System (CCS). Ces systèmes permettent aux divers acteurs sur une place portuaire de collaborer et d'accéder chacun à différents types d'informations. Un suivi efficace du transport de marchandises dangereuses nécessite ce type de système qui aide les ports dans leur stratégie de développement, notamment pour accélérer les opérations de contrôle sur les marchandises.

Dans de nombreuses situations, il est nécessaire d'accéder aux données les plus récentes d'un conteneur mais aussi à l'historique des opérations effectuées sur celui-ci. Cependant, les données collectées peuvent être confidentielles ou sensibles. Il est essentiel de disposer de droits d'accès différents selon le type d'acteurs. Le suivi des marchandises dangereuses est ainsi complexe en raison de ce nombre important d'acteurs et il entraîne un frein conséquent dans la fluidité de leur gestion en raison des multiples certifications relatives à ces différents acteurs. Une dématérialisation de ces opérations portuaires relèverait naturellement d'un système décentralisé et sécurisé auquel la technologie blockchain permettrait d'assurer la fluidité des contrôles tout en garantissant la confiance de chaque acteur.

Les ports disposent déjà de systèmes d'information de type PCS ou CCS auxquels viennent s'ajouter des modules spécifiques permettant le traitement des données relatives aux conteneurs de marchandises dangereuses. Aujourd'hui, HAROPA – Port du Havre utilise le logiciel TIMAD (Traitement Informatisé des MArchandises Dangereuses). Cette solution joue déjà le rôle de tiers de confiance dans un environnement où la dématérialisation et le déploiement de capteurs sur les navires, les conteneurs et les infrastructures portuaires soulèvent de nouveaux défis. Pour relever ces défis et renforcer ainsi de manière significative la fluidité et la sécurisation du transport des marchandises dangereuses, ce système d'information est en voie de

développement. Il embarquera de nouvelles fonctionnalités essentielles au passage à la dématérialisation de processus en assurant en apportant d'une part de la confiance aux différents acteurs dans les processus numériques mis en place. D'autre part, l'ensemble de la gestion de ces matières dangereuses est rendue plus fluide là où elle reste aujourd'hui un point d'attention particulière qui peut freiner l'efficacité et la rapidité du processus. On disposera ainsi d'un outil de traçabilité fiable et surtout capable de retracer de manière immédiate les opérations et les opérateurs intervenants. L'apport des technologies à base de blockchain contribuent ainsi de manière significative à la fluidité et à la sécurisation des opérations portuaires, notamment pour le suivi des matières dangereuses.

Notre contribution vise ainsi à proposer les premières bases de spécifications pour permettre d'intégrer des solutions « blockchain » dans un système d'information tel que le système TI-MAD.

Dans la section 2, nous présentons la technologie blockchain et les bénéfices de son apport au domaine de la logistique portuaire ainsi que les notions clés et les verrous actuels pour en faire un déploiement opérationnel à l'échelle d'une place portuaire comme celle du Havre. Nous y développerons notamment la notion de confiance que cette technologie apporte lors de la dématérialisation de la chaîne d'information concernant les diverses transactions.

Dans la section 3, nous développerons un modèle générique d'échange entre des systèmes à évènements, des systèmes d'informations et une blockchain.

Dans la section 4, nous exposons un exemple d'utilisation appliquant ce modèle générique au cas de la gestion des conteneurs de marchandises dangereuses lors du passage portuaire. Nous nous intéressons notamment à l'inscription de leurs déplacements permettant d'automatiser et de fluidifier les processus tout en déployant un mécanisme de traçabilité sûr et infalsifiable. Enfin, nous concluons avec les perspectives d'évolutions du modèle ainsi que de son implémentation.

2. LA BLOCKCHAIN POUR SÉCURISER LES TRANSACTIONS

Dans la première partie de cette section, nous expliquons le fonctionnement de la blockchain en tant que technologie garantissant la sécurité et la confiance dans les transactions, notamment

en utilisant les *smart contracts*. Dans une deuxième partie, nous présentons l'intérêt de la blockchain pour renforcer la confiance et améliorer la fluidité dans les processus logistiques.

2.1. La blockchain, un registre numérique décentralisé pour certifier les transactions

La blockchain, que l'on retrouve sous l'appellation *distributed ledger* en anglais, peut être vue comme un registre partagé et distribué entre les différents membres qui gèrent cette blockchain et se structurent en réseau pour partager des informations. La technologie blockchain s'appuie sur d'autres technologies pré existantes tels que les réseaux pair à pair et la cryptographie. L'articulation de ces technologies permet de définir une nouvelle approche de la confiance dans les transactions numériques. Cependant, la blockchain nécessite encore de la maturation aussi bien dans l'ingénierie de son déploiement à un niveau industriel que dans certaines parties des technologies utilisés qui contraignent son passage à l'échelle (UNECE 2019).

La blockchain est utilisée dans plusieurs domaines tels que l'agroalimentaire (Kamble et al. 2020), la santé (Kuo et al. 2017) ou encore la protection des données personnelles (Politou et al. 2018). Dans le domaine qui nous intéresse, la logistique portuaire et les *supply chains*, on note également de nombreuses publications (Queiroz et al. 2019, Lambourdiere & Corbin 2020).

Historiquement, le Bitcoin, décrit dans le livre blanc de Satoshi Nakamoto (Nakamoto 2009), est le premier modèle de blockchain. Elle sert de registre pour l'échange de la cryptomonnaie Bitcoin. Grâce à la technologie blockchain, il n'y a plus besoin de tiers de confiance comme les banques pour garder trace, authentifier et valider l'ensemble des transactions.

Dans le cas du Bitcoin et plus généralement des blockchains de première génération, les transactions sont des échanges de valeurs simples, comme des cryptomonnaies, entre les participants du réseau. Chaque membre du réseau possède une copie de la blockchain que l'on peut ainsi considérer comme le registre numérique des transactions. Les transactions y sont inscrites et regroupées par « paquets » appelés blocs.

2.1.1. Intégrité des données par la cryptographie

À chaque bloc, on applique sur l'ensemble des données qui le constitue, *une fonction de hachage* qui retourne un *hash*, également appelée signature ou empreinte de cet ensemble de donnée. Il est de taille fixe (Zhang et al. 2019). Le hachage de la même donnée retournera le même *hash*. Cependant, si la donnée est altérée ne serait-ce que d'un bit, le *hash* résultant sera complètement différent. Le Tableau 1 montre les *hashs* obtenus à partir de deux documents n'ayant qu'un seul caractère de différence.

Données	Hash obtenu avec l'algorithme SHA256
Texte intégral *20000 Lieues sous les mers* de Jules Verne	460531D8D9B14C255219CAD74C8AC6EB A5F80ECB661D0A233337A2770041D1CF
Texte intégral *20000 Lieues sous les mers* de Jules Verne avec l'ajout du caractère "*" au début du fichier	C2FFDA04B818608F0F61A98BF7078B761 4DCADE2362C1C43298918DDEB707DD2

Tableau 1 : Exemple de *hash* obtenu avec l'algorithme SHA256.

Dans les blockchains, le *hash* du bloc précédent est enregistré dans le bloc courant de la blockchain, permettant ainsi de créer une chaîne de blocs inaltérable. La Figure 1 illustre ce mécanisme de chaînage entre les blocs.

Figure 1 : Représentation d'une chaîne de blocs.

Il y a donc ici plusieurs aspects de cohérence : une première cohérence locale à chaque bloc garantie grâce au *hash,* une seconde cohérence globale à l'échelle de la blockchain garantie par le chaînage des *hashs* entre les blocs et une troisième cohérence globale à l'échelle du réseau garantie par la duplication de la blockchain sur chaque nœud membre du réseau. Si l'un des membres du réseau altère un bloc de sa blockchain locale, un nouveau *hash* est généré. Celui-ci ne sera pas celui qui est enregistré dans le bloc suivant qui invalidera ainsi cette modification.

Par ailleurs, ce nouveau *hash* n'est pas identique à celui des autres participants et le réseau rejettera cette modification.

De plus, les informations enregistrées sur la blockchain sont sécurisées grâce à l'utilisation du cryptage asymétrique, le couple clé privée / clé publique garantissant l'identité de l'émetteur de l'information. Cela permet notamment de lutter contre la fraude en s'assurant de la légitimité des informations inscrites.

2.1.2. Gestion des consensus

Pour que la blockchain puisse jouer son rôle de certification, il faut que des opérations de validation soient définies au niveau des transactions, par exemple, pour s'assurer qu'une opération de transfert financier est réalisée par un participant disposant des ressources nécessaires. Mais, il faut également avoir confiance en cette validation qui repose sur un ensemble de membres comme nous allons l'expliquer plus loin. Cela renforce la confiance par rapport à une validation qui serait assurée par un seul participant. Les nœuds membres du réseau rentrent donc dans un processus de compétition qui va permettre à tous les nœuds autorisés de pouvoir participer à la validation. Cette validation proposée par un nœud devra ensuite être vérifiée par les autres participants. La confiance dans le système est donc assurée par ce dispositif distribué appelé consensus ou encore preuve et qui correspond à la procédure permettant de valider un bloc à ajouter à la blockchain (Cachin 2017).

Dans la description précédente de cette procédure, plusieurs aspects restent à définir. Comment choisit-on les nœuds autorisés à pouvoir faire la validation ? Quel est le mécanisme de compétition entre les potentiels validateurs du bloc de transactions ? La manière de répondre à ces deux questions conduit ainsi à définir plusieurs consensus.

Les trois consensus les plus connus sont la preuve de travail (en anglais, Proof of Work ou PoW), la preuve d'autorité (en anglais, Proof of Authority ou PoA) et la preuve d'enjeu (en anglais, Proof of Stake ou PoS). On nomme *validateur*, ou *mineur* dans le cas de la preuve de travail, les membres du réseau participant au consensus.

La preuve de travail est le consensus utilisé par de nombreuses blockchains et notamment par Bitcoin (Gervais et al. 2016) ou Ethereum à ce jour. Dans cette situation, tous les mineurs sont en compétition : chacun d'entre eux doit résoudre un problème cryptographique coûteux en

temps d'exécution. Le premier à trouver la solution est rémunéré et propage son bloc contenant la solution à travers le réseau. Chaque membre du réseau recevant la solution peut la vérifier. Si une majorité de validateurs confirme le bloc propagé alors ce dernier peut être ajouté à la blockchain qui est dupliquée dans chacun des nœuds. Un système de vérification électronique récompense le validateur qui a produit le premier la solution. Ce mécanisme permet de faire fonctionner un dispositif de validation décentralisé, ouvert et dont l'intérêt sous forme de rémunération reste indépendant du contenu de l'information. En revanche, il nécessite un coût global de calcul particulièrement énergivore du fait que chaque nœud travaille simultanément à la résolution du problème cryptographique.

La preuve d'autorité est un consensus au sein duquel l'ordre des validateurs est connu. On sait à l'avance quel validateur prendra en charge la validation du prochain bloc (De Angelis et al. 2017). Ici, les membres du réseau ne sont pas en concurrence, c'est l'identité fournie avec le bloc qui permet de certifier que le bloc validé provient bien du bon validateur. Ainsi, le coût de la validation devient quasiment négligeable par rapport à celui de la preuve de travail.

Enfin, la preuve d'enjeu est une preuve mettant en compétition les validateurs en les faisant miser sur leur capacité à produire un bloc dans un temps imparti. Plus un validateur va miser un nombre de jetons important, plus ses chances d'être tiré au sort seront élevées. Une fois sélectionné, le validateur dispose d'un temps limité pour produire un bloc valide diffusé à travers le réseau (Li et al. 2017). Là encore, le coût de la validation est bien moins important que pour la preuve de travail et on maintient un mécanisme de sélection où le choix du validateur va varier de manière non déterministe d'une validation à l'autre.

2.1.3. Les différents types de blockchain

Il existe plusieurs types de blockchain. Elles sont catégorisées en fonction de l'accessibilité au réseau et des droits de validation (Dib et al. 2018) :

- Les blockchains publiques : elles sont ouvertes. C'est-à-dire que la blockchain peut être téléchargée et lue sans restriction et son code source est public. Il n'y a ni condition pour rejoindre le réseau, ni pour devenir validateur de blocs. La gouvernance, c'est-à-dire l'ensemble des règles de fonctionnement de la blockchain, est ouverte et décentralisée. Il existe de nombreuses blockchains publiques comme Bitcoin (Nakamoto 2009) ou Ethereum (Buterin 2013) pour les plus célèbres. Un grand nombre de nœuds permet

d'assurer une meilleure robustesse du réseau. De plus, la facilité d'accès à ce type de blockchains les rend attractives.

- Les blockchains privées : elles sont généralement déployées au sein de réseaux privés, chez des acteurs de confiance en raison de la nature sensible des informations inscrites dans la blockchain que l'on ne souhaite pas partager sur une blockchain publique. Seuls les nœuds acceptés par une autorité centrale peuvent rejoindre le réseau et devenir validateurs. Souvent un des acteurs gère cette blockchain et donne les autorisations d'adhésion. Cet acteur particulier est ainsi le garant ou responsable du système de transactions.
- Les blockchains hybrides : elles couplent une blockchain privée, contenant les informations ne souhaitant pas être partagées, et une blockchain publique sur laquelle sont stockées d'autres types d'informations comme le *hash* des blocs de la blockchain privée. L'utilisation des deux types de blockchains, privée et publique, permet de bénéficier des avantages offerts par chacune d'elles.
- Les blockchains de consortium : ces blockchains permettent à des acteurs, parfois concurrents, de collaborer ensemble en partageant les informations stockées sur une blockchain privée qu'ils gèrent de manière collaborative. L'utilisation d'une blockchain commune leur permet de fluidifier leurs échanges et d'instaurer une confiance mutuelle. Chaque acteur dispose du droit de validation de blocs et participe à la gouvernance du réseau.

2.1.4. Transactions et *smart contracts*

On distingue plusieurs générations de blockchains : les blockchains de première génération et les blockchains de seconde génération.

Dans le premier cas, les transactions pouvant être inscrites sont limitées à des valeurs simples, des échanges de cryptomonnaies, par exemple.

Les blockchains de seconde génération apportent un changement majeur. Les nœuds en plus de leurs habituelles capacités à vérifier, propager, synchroniser la blockchain, peuvent maintenant exécuter du code à la manière d'une machine de Turing (Jiao et al. 2018). Ce code est appelé *smart contract* et peut, automatiquement ou à l'appel, être exécuté par un nœud. Les *smart*

contracts peuvent également communiquer entre eux à l'aide de messages. Cette nouvelle fonctionnalité, ajoutée aux blockchains de seconde génération, permet d'enregistrer des transactions pouvant être conditionnées par différents évènements et différents acteurs intervenants dans la transaction. Un *smart contract* peut servir à définir des processus d'identification concernant un objet, par exemple un conteneur de marchandises. Il est également possible par la suite de définir des transactions qui correspondent alors à des changements d'états appliqués à cet objet et opérés par des acteurs dont l'identité doit être vérifiée : déplacement, changement de responsabilité, autorisation administrative, température relevée par un capteur, position, etc.

Les *smart contracts* vont ainsi contribuer à mettre en place de l'automatisation au sein des processus logistiques. Le déclenchement d'un contrat peut s'effectuer à une date ou un intervalle de temps défini à l'enregistrement du contrat dans la blockchain. Ainsi, à chaque fois que les conditions sont remplies, le *smart contract* exécutera les tâches pour lesquelles il est programmé.

2.2. Apport de la blockchain pour la confiance et la fluidité dans les processus logistiques

Avec la dématérialisation des processus, la signature électronique par exemple, les utilisateurs d'un système d'information peuvent perdre confiance dans la version numérique de ces outils qu'ils utilisent en devant s'en remettre aux systèmes d'informations qui les gèrent. La blockchain accompagne cette dématérialisation en apportant des garanties grâce aux mécanismes de sécurisation comme le chaînage et le hachage, qui permettent ainsi de réintroduire de la confiance entre les utilisateurs et les outils.

De plus, la blockchain peut intégrer tout type d'information numérique y compris des documents dématérialisés. Les *smart contracts* quant à eux peuvent gérer et certifier que des processus d'automatisation de tâches sur ces documents se déroulent correctement et ainsi sans délai d'attente. Cette automatisation permet une fluidification très notable du traitement de l'information.

Ces plus-values apportées par la blockchain en logistique sont décrites dans le livre blanc de l'UN/CEFACT (UNECE 2019). Cet organisme de standardisation travaille à l'élaboration de normes sur la blockchain appliquées à la logistique. L'établissement de ces standards permet

de définir les bases d'une interopérabilité entre les acteurs du monde portuaire et d'assurer la pérennité de cette technologie. Cependant, l'ingénierie de déploiement de solutions blockchain est un problème ouvert et la section suivante présente notre contribution.

3. UN MODÈLE GENERIQUE D'APPORT DE LA BLOCKCHAIN DANS UN PROCESSUS DE TRANSACTION EVENEMENTIELLE

Notre approche consiste dans un premier temps en l'élaboration d'un modèle abstrait sur lequel une méthode générique sera mise en place afin de pouvoir s'adapter à de nombreux cas d'usage, où l'on recherche à inscrire des informations dans une blockchain en complément d'un système d'information qui réagit à différents évènements (voir Figure 2). C'est une situation qui est très courante dans de nombreux processus logistiques ou de gestion de supply chains.

Le but est de certifier et de pouvoir tracer des transactions liées à ces évènements. Il s'agit notamment de pouvoir retrouver les opérations, leur nature, les éventuels intervenants et les dates de leur exécution en cas de litige.

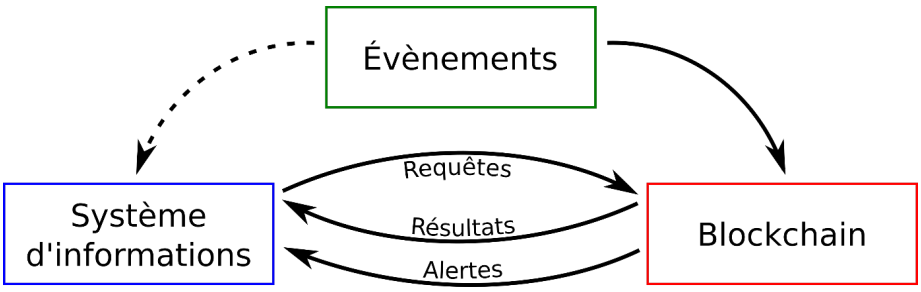

Figure 2 : Modèle général présentant les modalités d'interaction entre des évènements, un système d'information et une blockchain.

Dans un processus sans blockchain, les évènements sont directement transmis au système d'information (flèche en pointillés sur la Figure 2).

Dans le modèle proposé, où une blockchain est introduite, le système d'information communique avec la blockchain sous forme de requêtes lui permettant ainsi de notariser (c'est-à-dire d'inscrire de manière infalsifiable) des informations dans la blockchain et ensuite d'y d'accéder en ayant la certitude qu'elles n'ont pas été altérées. Par ailleurs, des évènements peuvent aussi

être notarisés dans la blockchain, permettant donc de retracer de manière fiable l'ensemble du processus de manière automatique et immédiate. Cette blockchain est répliquée sur plusieurs serveurs. Des mécanismes de synchronisations et vérifications s'assurent que les copies sont identiques. Dans notre modèle, la blockchain aura pour objet d'assurer la cohérence d'un ensemble de données critiques caractérisant la traçabilité des opérations. Elle se charge de lever des alertes en cas d'évènements anormaux, notamment lors de tentatives d'altération de données ce qui se traduira par une non concordance de ces données. Il peut s'agir, par exemple, d'un objet dont les déplacements sont soumis à autorisation. Ces autorisations sont enregistrées dans la blockchain via un *smart contract*. De plus, l'objet émet à intervalle de temps régulier sa géolocalisation qui est elle aussi enregistrée dans la blockchain. En cas de non concordance des autorisations et de la géolocalisation, la blockchain lève une alerte.

Dans la section suivante, nous appliquons ce modèle au cas d'usage qui nous intéresse, la traçabilité des transactions des marchandises dangereuses.

4. CAS D'USAGE : TRANSPORT DE MARCHANDISES DANGEREUSES

Les conteneurs de marchandises dangereuses sont soumis à des normes imposant la tenue de 13 documents tout au long du séjour du conteneur au sein de l'espace portuaire. Ces documents sont des déclarations ainsi que des relevés de traçage du conteneur. Au total, on estime que 375 000 conteneurs de marchandises dangereuses transitent tous les ans par le port du Havre. Si 30 enregistrements sont effectués pour chacun de ces conteneurs durant la totalité de leur présence sur le port, le taux de transactions à assurer devra donc être au minimum de 22 transactions par minute. Une solution s'appuyant sur des technologies blockchains doit donc être en mesure d'enregistrer ces différents évènements avec ce taux de transactions. Le nombre de transactions à effectuer par minute est un point de vigilance pour choisir une plateforme blockchain dont les plus courantes à ce jour, fonctionnent à partir de la preuve de travail qui limite cette fréquence. L'objectif de ce papier n'est pas de rentrer dans ces aspects assez techniques mais il est bon de préciser que les activités de recherche permettent déjà de voir apparaître de nouvelles plateformes blockchain autorisant des nombres de transactions élevés mais dont les outils de développement et de déploiement nécessitent encore un peu de maturation pour un usage aussi aisé que les blockchains connues telles que Hyperledger, Bitcoin et Ethereum.

4.1. L’enregistrement des évènements

La blockchain permet d'améliorer la fluidification des données et des documents concernant les conteneurs. En effet, ils sont soumis à une réglementation leur imposant des points de contrôle. Grâce à la blockchain, il sera possible de notariser numériquement et automatiquement chacun de ces contrôles rendant ainsi le traitement des données plus court et plus efficace.

Les informations ainsi enregistrées dans la blockchain permettent de garantir le respect des normes réglementaires et fournissent une notarisation ainsi qu’une traçabilité continue et infalsifiable de l’état des conteneurs.

La Figure 3 présente les échanges de données pour chaque évènement pendant la prise en charge du conteneur sur le port et qui subit ainsi plusieurs opérations telles que le chargement avec un identifiant unique. Des informations critiques sur le suivi de ce conteneur sont inscrites sur la blockchain. Celles-ci proviennent aujourd’hui d’opérateurs portuaires ou d’informations déjà présentes dans des TOS (Terminal Operating System). Elles pourront provenir dans le futur de différents capteurs présents sur les conteneurs et les infrastructures portuaires.

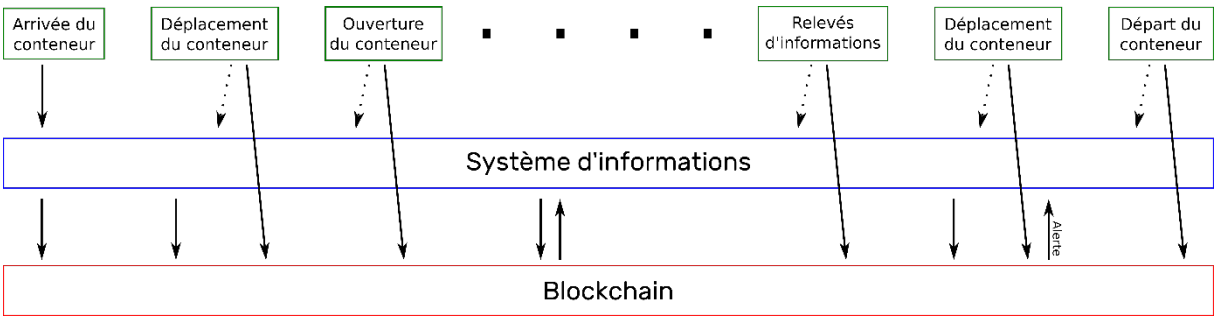

Figure 3 : Interaction des évènements avec le système d'informations et la blockchain.

La liste des opérations à effectuer sur le conteneur est enregistrée par le système d'information dans la blockchain. L'inscription dans la blockchain permet d'obtenir une traçabilité infalsifiable et sûre de l'ensemble du suivi du conteneur.

Attachons-nous maintenant à compléter le modèle abstrait précédent en y ajoutant la gestion de *smart contracts*.

4.2. Modèle générique intégrant des *smart contracts*

La blockchain peut être séparée en deux sous-ensembles : le registre, c'est la partie dans laquelle les transactions sont enregistrées, et les *smart contracts* qui effectuent le traitement automatisé des données.

Comme montré sur la Figure 4, il y a plusieurs types de *smart contracts* dans notre cas d'usage. Chacun est affecté à une tâche particulière.

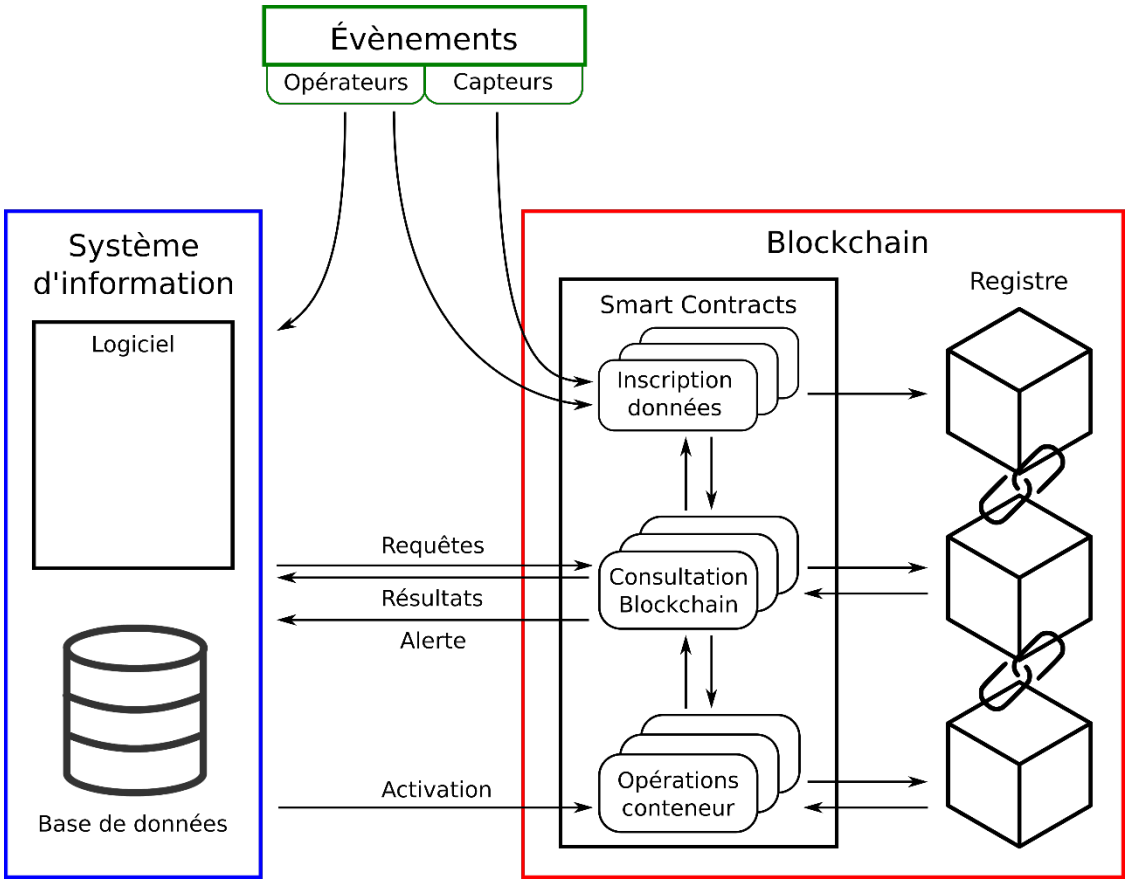

Figure 4 : Modèle générique de blockchain intégrant des *smart contracts*.

- L'inscription d'informations critiques : un *smart contract* reçoit les informations critiques pour la traçabilité. Celles-ci sont transmises par des opérateurs, par le TOS ou encore par des capteurs. Le *smart contract* les inscrits dans la blockchain. Dans certains cas, certaines données présentées doivent coïncider avec des données déjà inscrites. Si ce n'est pas le cas, alors le *smart contract* doit générer une alerte qui est envoyée au

système d'information (position d'un conteneur qui n'est pas en mouvement, par exemple).

- Les opérations sur les conteneurs : certaines opérations produisent des données critiques qui sont utiles à la traçabilité que l'on souhaite opérer. Dans ce cas, elles vont instancier des *smart contracts* qui vont permettre de faire les inscriptions de données souhaitées dans la blockchain. Grâce aux informations lues dans le registre et reçues du monde réel le *smart contract* vérifie que chaque opération a été réalisée conformément aux attentes. Les éventuels changements, erreurs, oublis ou incohérences sont transmis au système d'informations par des *smart contracts* qui produisent des alertes.

- L'interrogation de la blockchain : ce *smart contract* permet au système d'informations d'accéder à une information identifiée par un *hash* dans le registre et de la comparer à une information spécifiée. Un calcul du *hash* de l'information spécifiée est réalisé afin de le comparer avec le *hash* de la donnée du registre. Ce processus permet de s'assurer de l'authenticité de l'information.

L'utilisation de la blockchain telle que décrite ci-dessus présente deux avantages :

- Premièrement, elle simplifie l'identification de la responsabilité. En effet, les opérations enregistrées sont signées et l'intégrité de la blockchain garantit l'identité de l'acteur à l'origine de l'opération.

- Deuxièmement, l'utilisation de la blockchain et plus précisément des *smart contracts* permet d'automatiser des processus de dématérialisation. Ces étapes n'imposent plus la circulation de documents papiers, les signatures étant maintenant numériques grâce à un système de clés cryptographiques certifié. La dématérialisation apporte de la fluidité à l'ensemble du processus.

4.3. Exemple de gestion du déplacement d'un conteneur dans le dispositif évènements/systèmes d'information/blockchain

Prenons maintenant un exemple concret afin d'illustrer le fonctionnement d'un ensemble de *smart contract* basé sur le modèle abstrait précédent. Soit un conteneur de marchandises dangereuses qui est surveillé par différents opérateurs ou par le TOS ou qui pourrait être équipé

dans le futur d'un ensemble de capteurs (pression, température, position, lecteur de badge). Nous allons détailler ici les différentes étapes d'un déplacement donnant lieu à des inscriptions ou des accès dans la blockchain.

1. L'opérateur s'identifie avec sa clé privée ce qui génère un enregistrement dans la blockchain. Il instancie un *smart contract* de demande de déplacement qui contient les modalités de l'opération : le conteneur à déplacer, la position de départ ainsi que la position d'arrivée. Ce contrat est signé par l'opérateur avec sa clé privée et inscrit dans la blockchain. L'inscription dans la blockchain nécessite une validation qui va ici autoriser ou non cette demande par rapport aux processus gérés par le système d'information. Nous supposons dans la suite que la demande est validée pour étudier le déroulé du processus.

2. L'opérateur passe son badge devant le lecteur de cartes connecté du conteneur qui est dédié à une démarche d'authentification. Ce lecteur de cartes connecté émet un signal contenant son identifiant ainsi que celui de l'opérateur déclenchant la génération d'un *smart contract* d'association. Ce *smart contract* lit les précédents enregistrements dans la blockchain et vérifie qu'il existe une demande de déplacement validée et correspondant à cette association. Une fois cette vérification faite, le *smart contract* inscrit dans la blockchain que le déplacement est actif. L'inscription de l'activation du déplacement désarme les alarmes de surveillance de positions.

3. Une fois le déplacement effectué, l'opérateur indique à la blockchain que l'opération est terminée. Le *smart contract* de demande de déplacement s'assure que le conteneur est bien à la place déclarée à la signature du contrat puis appelle le contrat d'association qui réactive les alarmes.

4. CONCLUSION ET PERSPECTIVES

Après avoir présenté les concepts fondamentaux de la blockchain ainsi que son apport à la logistique, nous avons introduit un modèle générique permettant d'enregistrer de façon sécurisée et infalsifiable la certification d'évènements du monde réel dans la blockchain. Ce modèle a ensuite été développé dans un cas d'usage concernant le suivi de conteneur de marchandises dangereuses. Après avoir décrit les principaux types d'inscriptions dans la blockchain pour assurer la traçabilité de ce suivi, un exemple a permis d'illustrer la gestion du déplacement d'un conteneur.

L'objectif est de proposer une méthodologie générique avec un taux de transposabilité important sur différents cas d'usage, notamment pour des transactions d'opérations logistiques et de management de supply chain.

Dans ce papier, nous avons présenté un travail de collaboration avec HAROPA – Port du Havre pour finaliser une preuve de concept basée sur cette approche et permettant de faire évoluer la version du logiciel TIMAD en intégrant les technologies blockchain grâce au modèle générique que nous proposons. Des premiers exemples de spécifications de *smart contract* ont été présentés, notamment pour le suivi du déplacement d'un conteneur de marchandises dangereuses. Le travail d'interfaçage avec les processus actuels et le déploiement en cours des technologies de capteurs doit être approfondi pour aboutir à la preuve de concept attendue et directement exploitable et déployable sur le port du Havre.

Bibliographie

Buterin, V. (2013). *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum.org. https://ethereum.org/whitepaper/

Cachin, C. (2017). Blockchains and Consensus Protocols: Snake Oil Warning. *Proceedings of the 2017 13th European Dependable Computing Conference (EDCC)*, Sep 4, 2017 - Sep 8, 2017, Geneva, Switzerland, pp. 1-2. https://doi.org/10.1109/edcc.2017.36

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. *Proceedings of the Second Italian Conference on Cyber Security (ITASEC),* Feb 6, 2018 – Feb 9, 2018, Milan, Italy, pp. 1-11. https://doi.org/10.5281/zenodo.1169272

Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium Blockchains: Overview, Applications and Challenges. *International Journal on Advances in Telecommunications, 11* (1 & 2), pp. 51-64. IARIA Journals.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* Oct 24, 2016 – Oct 28, 2016, Vienna, Austria, pp. 3-16. https://doi.org/10.1145/2976749.2978341

Jiao, J., Lin, S.-W., & Sun, J. (2020). A Generalized Formal Semantic Framework for Smart Contracts. *Proceedings of International Conference on Fundamental Approaches to Software Engineering (FASE),* pp. 75-96. Lecture Notes in Computer Science, vol 12076. Springer, Cham. https://doi.org/10.1007/978-3-030-45234-6_4

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International Journal of Information Management*, *52*, 101967. Elsevier. https://doi.org/10.1016/j.ijinfomgt.2019.05.023

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24* (6), 1211-1220. Oxford Academic. https://doi.org/10.1093/jamia/ocx068

Lambourdiere, E., & Corbin, E. (2020). Blockchain and maritime supply-chain performance: dynamic capabilities perspective. *Worldwide Hospitality and Tourism Themes*, *12*(1), pp. 24-34. Emerald Publishing Limited. https://doi.org/10.1108/whatt-10-2019-0069

Li, W., Andreina, S., Bohli, J.-M., & Karame, G. (2017). Securing Proof-of-Stake Blockchain Protocols. *Lecture Notes in Computer Science*, Lecture Notes in Computer Science, vol 10436. Springer, Cham. pp. 297-315. https://doi.org/10.1007/978-3-319-67816-0_17

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. https://bitcoin.org/bitcoin.pdf

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), pp. tyy001. Oxford Academic. https://doi.org/10.1093/cybsec/tyy001

Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management: An International Journal*, *25*(2), pp. 241-254. Emerald Publishing Limited. https://doi.org/10.1108/scm-03-2018-0143

United Nations Economic Commission for Europe. (2019*). White Paper: Blockchain in Trade Facilitation* (N°2). https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys, 52*(3), pp. 1-34. https://doi.org/10.1145/3316481