LIVRE BLANC

LiaTrust

Gestion du certificat d'origine

Facilitation des transactions du commerce international

Table des auteurs

Auteurs	Profils
Maha Ouahi	Étudiante en système distribué à l'INPT LinkedIn
El Alaoui Hassani Meryem	Étudiante en Data Engineering à l'INPT LinkedIn
Moustadraf Hamza	Ingénieur IT diplômé de l'INPT LinkedIn
Khaddir Yassir	Étudiant en Cybersécurité à l'INPT LinkedIn
Bannouni Soufiane	Ingénieur IT diplômé de l'INPT LinkedIn
Aourir Zakaria	Ingénieur IT, DLT diplômé de l'INPT LinkedIn
Alaoui Mohamed	CTO, Architecte système distribué LinkedIn

List Of Images

List Of Tables

1. Introduction

La documentation autour d'une opération d'import export est la principale source de confiance facilitant le commerce international. Pour être compétitif dans le commerce international, il est important de dématérialiser les échanges des informations entre les acteurs d'une transaction avec un très haut niveau de confiance afin d'optimiser le traitement des transactions et réduire les coûts.

Sans citer en détail toute la documentation nécessaire pour une transaction, voici quelques exemples non exhaustifs de documentation dans le cadre du commerce international marocain :

- **Le Certificat d'Origine**
- La Déclaration Unique de Marchandise
- Les certificats sanitaires et de conformité
- Le connaissement ("Bill of Lading")
- Le Credit Management (Lettre de crédit, Le crédit documentaire, la Connaissance du contexte transactionnel KYT, KYC, KYCC :"Know Your Transaction", "Know Your Client", "Know Your Client Customers"

Pour répondre au hackathon organisé par l'agence nationale des ports du Maroc, nous avons conçu ce livre blanc pour traiter la facilitation de la gestion du certificat d'origine qui est un sujet critique pour le Maroc et dans le monde en général.
Le certificat d'origine est un ensemble de données sous forme de document constituant une preuve de l'origine du produit entrant dans le cadre d'un accord inter-pays. La procédure actuelle permettant la gestion du cycle de vie des preuves de l'origine des produits n'est pas pas optimisée pour des raisons divers et variées :

- Le processus est complexe, multi-langues avec des accords internationaux.
- La dématérialisation End to End du certificat d'origine est difficile de part l'existence de variabilités juridiques et technologiques
- Les acteurs sont multiples
- L'échange des données doit se faire avec confiance, intégrité et authenticité ce qui induit aussi des complexités techniques et juridiques.

Afin d'améliorer cette situation, Liatrust propose un écosystème permettant de répondre à une dématérialisation de la confiance de toute la chaîne de gestion du certificat d'origine.

Nous allons aborder dans ce qui suit les problématiques associées au certificat d'origine et la solution apportée par Liatrust.

2. La problématique du certificat d'origine et Liatrust

2.1. Description de la problématique

Lors des dernières années, un effort considérable a été effectué pour améliorer la gestion du certificat d'origine. En effet, la création de guichets uniques dans différents pays, les tentatives bi-latérales pour dématérialiser la gestion du certificat sont des initiatives qui vont dans le bon sens. Cependant le processus actuel demande des améliorations à bien des égards et en voici quelques uns dans le contexte national marocain.

Les efforts actuels de dématérialisation concernent principalement la déclaration de marchandise qui équivaut une délivrance du certificat par la douane nationale. Cependant, cette dématérialisation n'adresse que la partie nationale. La dématérialisation End To End n'est pas traitée. Par ailleurs, la notion même de délivrance à l'exportateur pose un certain nombre de problèmes d'ordre logistique et de sécurité :

- Suite à l'émission du certificat d'origine en format papier cacheté par la douane du pays exportateur, l'exportateur est chargé de le fournir à l'importateur pour que ce dernier puisse le présenter à la douane du pays importateur. Cette chaîne induit une complexité logistique évidente. L'exportateur se retrouve parfois en urgence obligé d'envoyer en DHL à l'exportateur le certificat émis par sa douane.
- Au-delà de sa complexité, il existe des failles quant à l'authenticité et l'intégrité des données du certificat. En effet, ce processus fait intervenir des "Man in the middle" ce qui augmente considérablement les risques de falsifications :
    - Fausses déclarations d'origine (origine douanière, préférentielle ou non)
    - Sous-évaluation des droits et taxes et/ou la description erronée de marchandises (fausse déclaration de valeur et/ou d'espèce tarifaire)
    - La contrebande et la contrefaçon de marchandises

Tout ceci nuit au commerce international marocain.

2.2. L'apport de Liatrust pour améliorer la situation

Afin d'améliorer la situation, Liatrust propose un canal sûr de communication sous forme de registre distribué permettant un échange de données multi-acteurs permettant un échange de douane à douane concernant le certificat d'origine. Ce registre permet de stocker les données d'une manière immuable et cryptographiquement sécurisée. Il permet de fournir un ensemble de preuves quant à l'intégrité et l'authenticité des données.

2.3. Cas d'utilisation à l'exportation

Afin d'étayer nos propos, nous allons décrire en détail le cas du processus du certificat d'origine dans le cadre de Liatrust.

2.3.1. Les acteurs du processus

Les différents acteurs participant à la gestion d'un certificat d'origine sont les suivants :

Acteurs	Typologies	Notes
Exportateur ou Exporter	Trader sell side	Vendeur de la marchandise
Importateur ou Importer	Trader buy side	Acheteur de la marchandise
Douane de l'exportateur Exporter's Customs	Trust provider	Émetteur et validateur du certificat d'origine dans notre contexte
Douane de l'importateur Importer's Customs	Controller	Contrôleur de l'authenticité et de l'intégrité du certificat d'origine validé.

Table 1. Acteurs de la gestion du certificat d'origine

Afin de simplifier nos propos, nous n'allons pas étudier les cas du certificat d'origine faisant intervenir d'autre acteurs comme les chambres de commerces, les guichets uniques d'import export ou des organismes de certification et de conformité. Leur typologie rentre dans les cas traités (Trust provider ou Controller) et donc leur interaction avec l'écosystème peut être étendue.

2.3.2. Nos hypothèses

Nous ferons l'hypothèse dans cette section qu'il existe un entrepôt de données contenant les informations suivantes :

- Les bases de références des produits marchands avec leur nomenclature standard international.
- La base de règles d'origine construite à partir des accords internationaux.
- Une cartographie des catalogues marchands des exportateurs en relation avec les nomenclatures standards et la référence vers la base des règles d'origine.

Les données précédentes sont des données référentielles autour des transactions commerciales internationales.

Cet entrepôt permet de sourcer par défaut un ensemble d'information utile à l'émission du certificat d'origine. Dans le cadre d'une généralisation du statut d'exportateur agréé au Maroc, les informations permettant l'émission d'un certificat d'origine sont disponibles sans que l'exportateur n'intervienne. Si la marchandise de la transaction n'est pas référencée, une mise à jour sera toujours possible.

Cette stratégie permet de simplifier au maximum la délivrance du certificat. C'est précisément la direction prise par la douane marocaine afin de faciliter les procédures des exportateurs en rendant la déclaration de marchandise équivalente à la délivrance du certificat. Cependant, il faudrait aller plus loin pour adresser tout le cycle de vie du certificat d'origine.

Nous allons aussi considérer que les différents acteurs sont connus par l'écosystème Liatrust. Nous aborderons dans une autre section l' onboarding des acteurs. En effet, chaque utilisateur possède un Liatrust Trade Wallet lui permettant d'interagir avec l'écosystème. Ce Trade Wallet est cryptographiquement sécurisé et représente l'identité de l'acteur.

Le processus de dématérialisation de la confiance entre les acteurs de la chaîne est le suivant. Nous considérons comme point de départ une déclaration de l'opération d'exportation existante:

Liatrust Flow			
	Step 1	**Step 2**	**Step 3**
Trust Provider as exporter's customs	**Action :** Emission du certificat d'origine et vérification des données	**Action :** Calcul de l'empreinte unique du certificat d'origine et signature de cette empreinte en la stockant dans un registre distribué immuable et horodaté avec des statuts de gestion.	
Controller as importer's customs	**Action :** Récupération du certificat d'origine.	**Action :** Calcul de l'empreinte du certificat d'origine et vérification de son intégrité et son authenticité avec un accès au registre distribué.	**Action :** Dans le cas d'un système intégrant toutes les données de la transaction, la douane de l'importateur peut enrichir les données de transaction avec la tarification douanière validée et des statuts de gestion.
Exporter as sell side trader	**Action :** Suivi du processus de certificat d'origine	**Action :** Reprise et correction de certaines informations du certificat d'origine si nécéssaire pour une revérification de la douane de l'exportateur.	
Importer as buy side trader	**Action :** Suivi du processus de certificat d'origine	**Action :** Dans le cas d'un système intégrant toutes les données de la transaction. L'importateur peut interagir en ajoutant des données pertinentes ainsi que des statuts de reception	

Figure 1. Cas d'utilisation : certificat d'origine via Liatrust

Commentaire du tableau :

- L'émission du certificat d'origine se fait en agrégeant les données pertinentes provenant de l'entrepôt de données pour la construction du certificat d'origine. Cette opération peut être faite automatiquement par les services de la douane via des APIs Liatrust.
- L'empreinte numérique du certificat d'origine identifie d'une manière univoque ce document. Cette opération se fait automatiquement via les APIs de Liatrust.
- Les données du certificat d'origine stockées dans le registre distribué sont obfusqués. Seules les empreintes signées des données et leur statuts modifiés sont stockés. Cette stratégie permet d'alléger les données dites onChain (donnée dans le registre). Le registre se positionne comme un fournisseur de preuve d'authenticité et d'intégrité.
- A l'aide d'APIs fournis par Liatrust, la douane de l'importateur récupère l'intégralité des données du certificat d'origine. Elle peut reconstituer l'empreinte univoque lui permettant ainsi de vérifier l'intégrité du certificat d'origine. Elle vérifie également la signature faite par la douane de l'exportateur. Ces actions sont effectuées via des services cryptographiques fournis par Liatrust.
- Suite au contrôle d'intégrité et d'authenticité de la douane de l'importateur, ce dernier peut enrichir les données des transactions avec des données pertinentes, telles que les statuts de validation ou les données de pricing puis les signer. Cette étape

d'enrichissement n'est pertinente que si l'on souhaite une intégration complète des données de la transaction.

- Ainsi, les différents statuts et les informations liées à la gestion du certificat d'origine en sont consultables d'une manière fiable par les différents acteurs de la chaîne. L'importateur et l'exportateur peuvent consulter les différentes informations avec les bons niveaux d'autorisations.

2.3.3. Critiques des hypothèses

Nous avons initié le processus en considérant une opération d'export déjà déclarée et avec un exportateur agréé en dehors de l'écosystème Liatrust. Idéalement, la procédure d'agrément et la déclaration de l'opération d'exportation devrait être intégrée dans l'écosystème.

En effet, dans le cas contraire, l'implication de l'exportateur dès le début du processus pour fournir les données nécessaires au certificat d'origine est nécessaire. Ce qui alourdit la gestion du certificat et qui surtout ne permet pas de préparer une intégration complète des données des transactions dans l'écosystème au-delà du certificat d'origine.

Dans le cadre d'une dématérialisation de la confiance dans les données de transaction dans leur globalité, il serait pertinent d'intégrer la déclaration de la transaction et toutes autres interactions de l'exportateur dans le système afin d'atteindre un niveau de confiance complet sur toutes les données de la transaction. Par ce biais, l'intervention de l'exportateur dans certaines procédures peut être souvent évitée.

2.3.4. Propositions pour simplifier la gestion du certificat d'origine

Afin de faciliter à la douane du pays exportateur l'émission du certificat d'origine sans l'intervention de l'exportateur, comme dit précédemment, il serait pertinent d'intégrer toutes procédures liées à la transaction comme la déclaration de la transaction/marchandise et l'agrément de l'exportateur. Ainsi, lors de l'émission du certificat, la douane marocaine a en sa possession un ensemble de données fiables pour établir le certificat comme la codification des produits liés à la transaction.
Les données référentielles associées aux règles d'origine doivent être aussi disponible numériquement pour une émission automatisée. Ainsi, leur codification sous forme de règles de décision d'origine peut être un apport certain pour la fluidification du processus. En effet, ceci permettrait aussi de matérialiser le lien existant entre les codes du système harmonisé mis en place par l'OMD (Organisation Mondiale Des douanes) pour la désignation et la codification des marchandises avec la règle d'origine associée ainsi que le lien avec la transaction. Ce lien peut être fiabilisé dans l'écosystème LiaTrust et constitue une preuve numérique de l'origine. Cette

stratégie est un atout certain pour le Maroc, car elle permet de répondre par construction à la transparence demandée par le World Trade Organisation.

Les règles d'origine sont réparties sur plusieurs accords et circulaires, il est possible de construire une base de données regroupant toutes ces règles établies pour chaque pays, avec les produits concernées. Liatrust a commencé ce travail en cartographiant les règles actuelles (voir Base de règles).

Le but de Liatrust est d'intégrer toutes les procédures d'échange d'informations nécessitant un haut niveau d'intégrité et d'authenticité dans une transaction de commerce international. Ainsi, nous ouvrons la porte à une dématérialisation de la confiance sur les données échangées. Le certificat d'origine est le premier candidat pour cet écosystème.

Dans les sections suivantes, nous allons détailler certains points autour de l'ingénierie et de la conception de Liatrust.

3. Ingénierie Liatrust

Afin de montrer la valeur ajoutée de l'écosystème Liatrust, nous tenterons de rester générique quant aux vocabulaires utilisés. Nous nous permettrons de parler de Trade Data en tant que données de la liasse des documents d'une transaction. Les données du certificat d'origine sont un sous-ensemble de ces Trade Data.

Par ailleurs, nous allons simplifier les typologies des différents acteurs de la chaîne. Nous allons considérer trois fonctions différentes :

- Un Exportateur
- Un importateur
- Un Trust Provider : validateur de la donnée
- Un Controller : vérificateur de la donnée

Les différents acteurs d'une chaîne de responsabilité peuvent avoir l'une ou plusieurs de ces fonctions à un instant donné. Par souci de simplification, quand cela nous est possible, nous allons confondre les acteurs avec leur entité légale.

3.1. Cycle de vie des Trade Data

Dans le schéma qui suit, nous allons expliciter le cycle de vie des Trade Data en précisant les rôles des différents acteurs concernés.

Notons que les organismes de certification et les institutions financières ont été ajouté pour montrer les différents cas d'utilisation au delà du certificat d'origine :

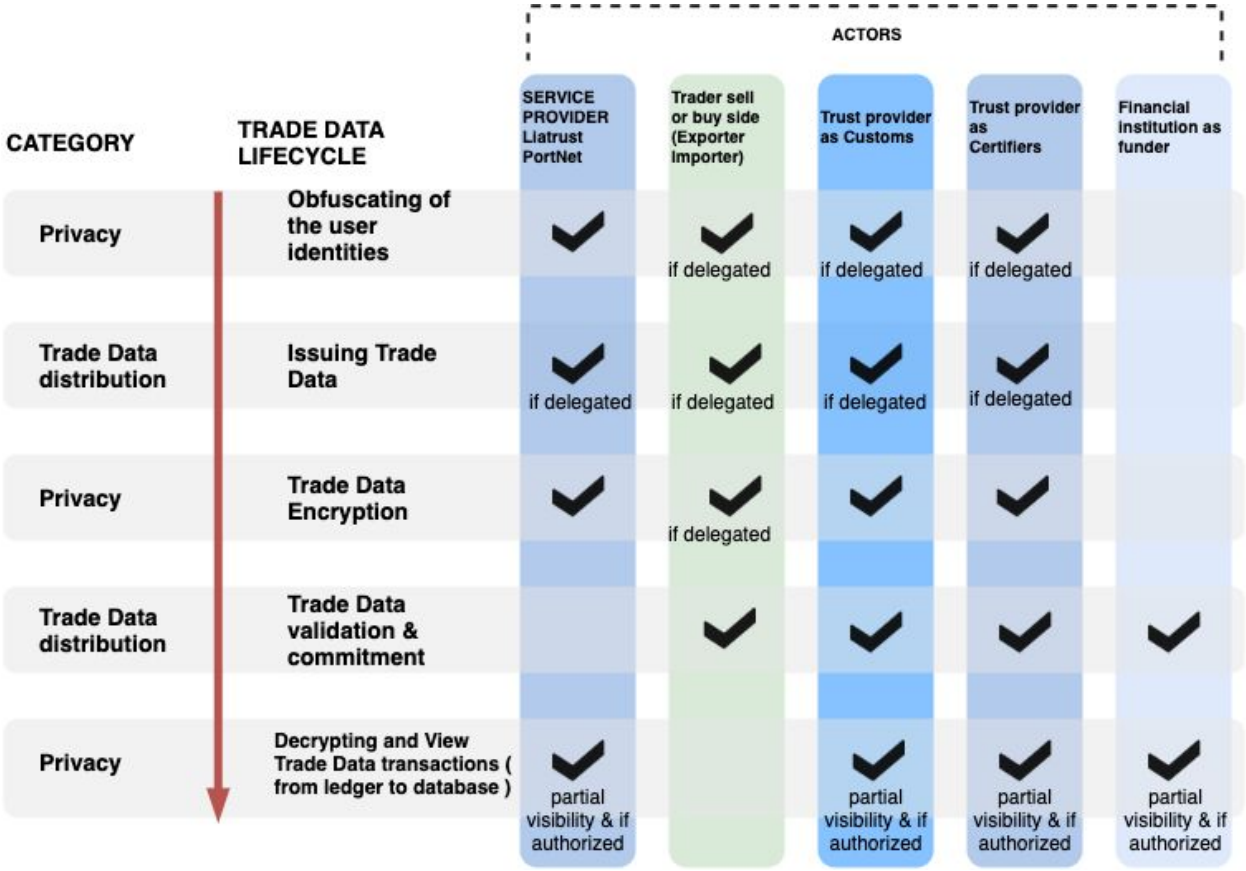

Figure 2. Cycle de vie des Trade Data

Commentaire du schéma :

- Le "Service Provider" est Liatrust, l'opérateur technologique de la plateforme. Il joue le rôle de facilitateur technologique pour les différents acteurs métiers. Nous faisons l'hypothèse que Liatrust est un partenaire des acteurs actuels jouant ce rôle.
- Les "Traders" sell et buy side sont respectivement l'exportateur et l'importateur. Ils interviennent principalement dans l'émission de certaines données initiales et leurs signatures. Ils sont également concernés par le suivi des transactions.
- Les "Trust Providers" sont les acteurs de validation apposant leur approbation sur les données de transaction. Ils enrichissent les données des transactions afin de matérialiser la validation des données. Ils ajoutent également des nouvelles données nécessaires au cycle de vie de la transaction. Nous pouvons citer comme exemple, la validation des données du certificat d'origine par la douane de l'exportateur, la validation des tarifs douaniers par la douane de l'importateur ou dans un autre contexte, l'émission d'un certificat de conformité par un organisme de certification.

- Les organismes de financement concernés par la connaissance de la transaction, interviennent pour authentifier et vérifier l'intégrité des données pour valider, par exemple, un financement dans le cadre d'une lettre de crédit.

3.2. Gouvernance de la donnée et tentative de standardisation

La gouvernance de la donnée dans le cadre d'une transaction du commerce international est complexe. Dans le contexte maroccain, les formats de certificat d'origine par exemple ne sont pas harmonisés. Afin de préparer des accords d'harmonisation, il est important de penser la gouvernance des données d'une manière agile et flexible. La définition du grain des données des transactions et leur identification est un élément crucial dans l'objectif d'harmonisation des informations échangées.

L'initiative UCR ("Unique Consignment Reference") du "World Customs Organization" (WCO) n'a pas été concluante car son implémentation est difficile à réaliser. En effet, elle demande une gouvernance inter-pays et donc une coordination accrue entre les participants dans la transaction.

Les dernières avancées permises par l'avènement des technologies des registres distribués permettent une alternative pour partager ce type d'information. La notion d'identifiant décentralisé (DID, Decentralized Identifier) est au cœur de cette alternative. Nous allons y consacrer une section (section DID).

Concernant la granularité de la donnée, une fois une donnée atomique sémantiquement cohérente est définie, il est possible d'agréger les informations pour harmoniser un document donné. Dans le cadre marocain, nous pouvons initier un agrégat générique respectant un standard actuel ou permettant une compatibilité avec les futures harmonisations à moindre effort.

Nous entendons par donnée atomique sémantiquement cohérente, les données de transaction ayant un sens. Par exemple, sans être exhaustif :

- Une adresse
- Un montant
- Un numéro de document
- Une références de marchandise
- Un identifiant du transporteur

Il est d'usage de bien définir cette atomicité. Certaines informations de base peuvent être regroupées au sein du même atome si ceci fait sens. La conception de cette granularité doit être conduite en suivant les potentiels futurs standards.

Aussi, il n'est pas question ici de réinventer de nouveaux identifiants. Les identifiants métiers actuels font sens et permettent probablement une corrélation pendant tout ou partie de la transaction. Les DIDs sont des enveloppes techniques publiquement adressables et cryptographiquement sécurisées permettant un accès à l'information. Les identifiants métiers actuels sont encapsulés dans un DID qui servira de point de publication unique selon la granularité de l'information.
L'agrégation de ces données atomique forme un document (un certificat d'origine par exemple) qui peut être à son tour géré par un DID. Ainsi les données de transaction sont représentables via un arbre de DIDs.

Le propriétaire d'un DID ou d'un arbre de DIDs est également lié cryptographiquement à ces données. Ainsi tous les acteurs de la transaction avec les bonnes autorisations, sont capables d'interagir avec un arbre de DIDs, valider son intégrité, valider son authenticité, l'enrichir et signer cryptographiquement les informations ajoutées.

Cette notion de DID n'est évidemment pas visible par les acteurs de la chaîne. Ces derniers possèdent un Trade Wallet représentant leur identité qui leur permet d'interagir avec les données à l'aide des nomenclatures métiers.
Liatrust fournit les différents composants permettant ce type d'interaction.

Afin d'expliciter l'intégration des DIDs dans l'écosystème Liatrust, voici une projection technique des interactions possibles entre les différentes typologies des acteurs lors de la gestion d'un certificat d'origine. Pour faciliter la compréhension du schéma, voici quelques définitions :

- Le terme **OFF CHAIN** désigne les composants gérant les données et les interactions sécurisées qui sont en dehors du registre distribué. Ils concernent principalement des applications et/ou des APIs permettant l'accessibilité des données des transactions.
- Le terme **ON CHAIN** désigne les composants gérant les empreintes signées des données avec des statuts de suivi ainsi que les interactions internes du registre distribué. Les données concernées sont sous forme de contrat intelligent ou Smart Contract.

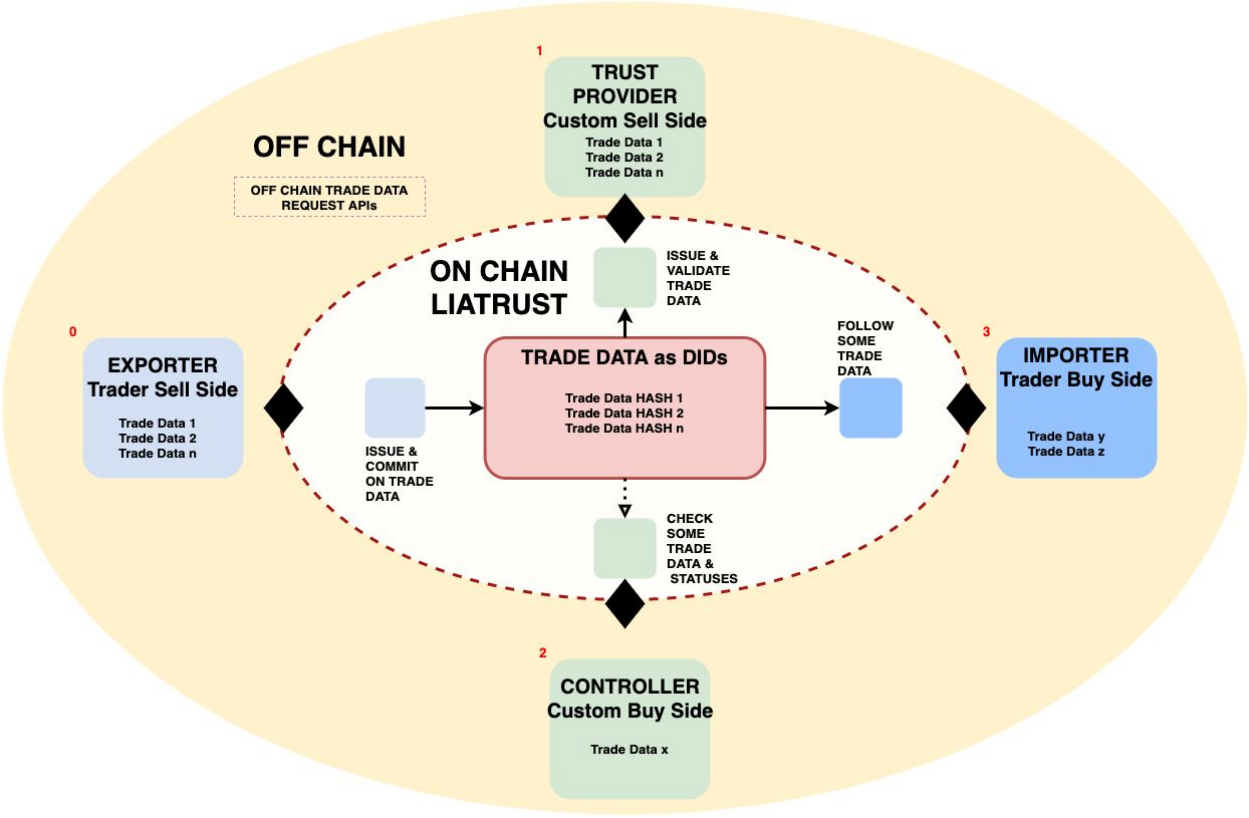

Figure 3. Interaction entre le registre et les acteurs d'un certificat d'origine

3.2.1. Decentralized Identifier pour les données

Les identifiants décentralisés (DIDs) représentent une nouvelle manière de gestion universelle d'un identifiant unique. Ils tirent parti des avantages de l'architecture décentralisée et des systèmes cryptographiques pour fournir des identifiants vérifiables et dont le contrôle subsiste dans les mains de ses propriétaires. Ainsi, les DIDs permettent aux acteurs d'un processus de connaître avec qui leurs données sont partagées. Ils permettent aussi une traçabilité des données d'une manière décentralisée.

Dans notre contexte, les DIDs nous servent de point de publication décentralisé et sécurisé de la donnée. Ainsi, un certificat d'origine représenté techniquement par un DID ou par un arbre de DIDs, fournit nativement le matériel cryptographique qui permet de vérifier son authenticité et son intégrité.

Les DIDs identifient non seulement les données d'un acteur, mais aussi toute entité cohérente concrète ou abstraite (une organisation, un objet ou une chose, un modèle de donnée). L'identité des acteurs Liatrust est aussi représentée via un DID qui est un représentant du Trade Wallet Liatrust.

Les DIDs suivent le même modèle de base que la spécification URN (Uniform Resource Name: https://tools.ietf.org/html/rfc8141).

En voici le fonctionnement tel qu'il est décrit dans les standards W3C.

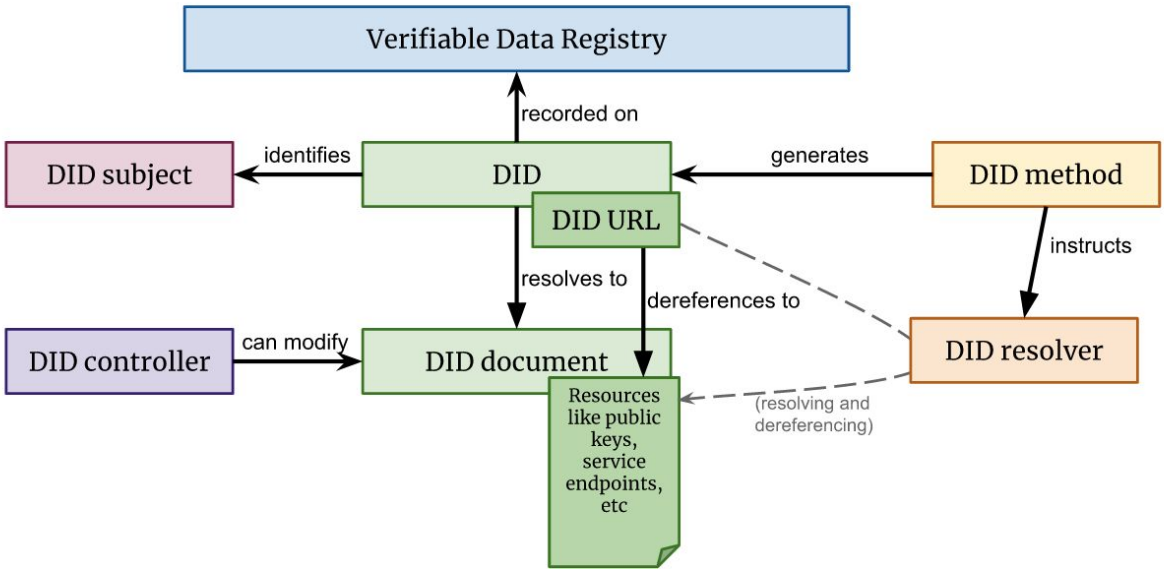

Figure 4. Spécification d'un DID

Commentaire du schéma :

- Le registre de DIDs peut être implémenté par un ensemble de contrats intelligents contenant des attributs dans un document DID.
- Les attributs sont sous forme d'empreinte numérique jumelée avec les Trade data dans notre contexte.
- Il est possible de réaliser également une implémentation permettant de représenter des données liées et ainsi construire tout un arbre de Trade data vérifiable cryptographiquement.

Voici par ailleurs un schéma représentant le flux des identifiants décentralisés :

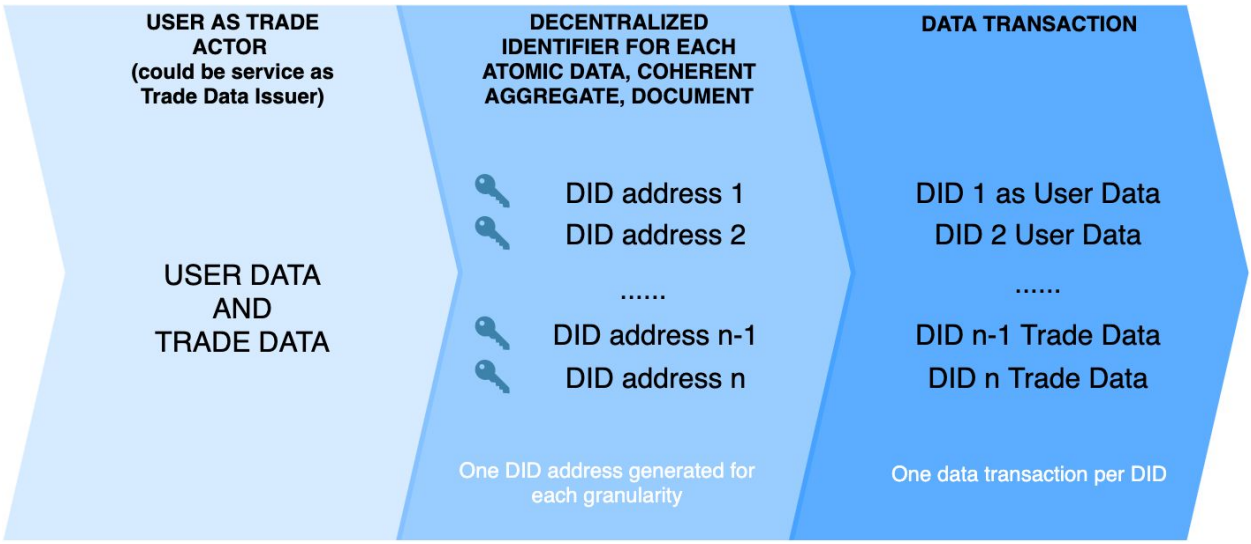

Figure 5. Flux des identifiants décentralisés

3.2.2. Complexité linguistique

Comme mentionné en introduction, le contexte du commerce international est intrinsèquement multi-langue. La diversité linguistique et l'hétérogénéité des formats de la documentation autour d'une transaction ajoute une couche de complexité certaine.

Liatrust choisit de traiter les informations d'une manière atomique et repose sa stratégie linguistique sur le standard i18n permettant ainsi d'avoir une gestion très fine sur la donnée. Chaque agrégat pertinent de données atomiques métier possède une métadonnée permettant la gestion linguistique reposant sur le standard i18n.
Ces métadonnées sont traitées avec le même niveau d'intégrité et d'authenticité que les Trade Data métier dont ils font partie.

3.3. Gestion de l'identité des acteurs et de leurs autorisations

3.3.1. Trade Wallet management

Le Trade Wallet de Liatrust est l'outil principal qui permet l'identification des acteurs et une interaction avec les APIs. Sa gouvernance se fait avec une attention particulière car il est l'unique propriété de l'acteur qui effectue une action sur les données d'une transaction. Pour assurer un niveau de sécurité et de confiance entre les différents acteurs, le Trade Wallet de Liatrust est basé sur des processus cryptographiques distribués permettant une signature de l'information sans matérialiser la clé privée en mémoire. Ceci rend très peu probable le vol d'identité qui est possible avec les infrastructures de gestion de clé privé actuelle où une seule autorité détient les clefs d'une manière centralisée. Cette innovation repose sur les dernières recherches cryptographiques sur les algorithmes distribués de signature et de chiffrement/déchiffrement. Nous consacrerons une section à cette notion.

Voici un aperçu du processus générique mettant en jeu le Trade Wallet :

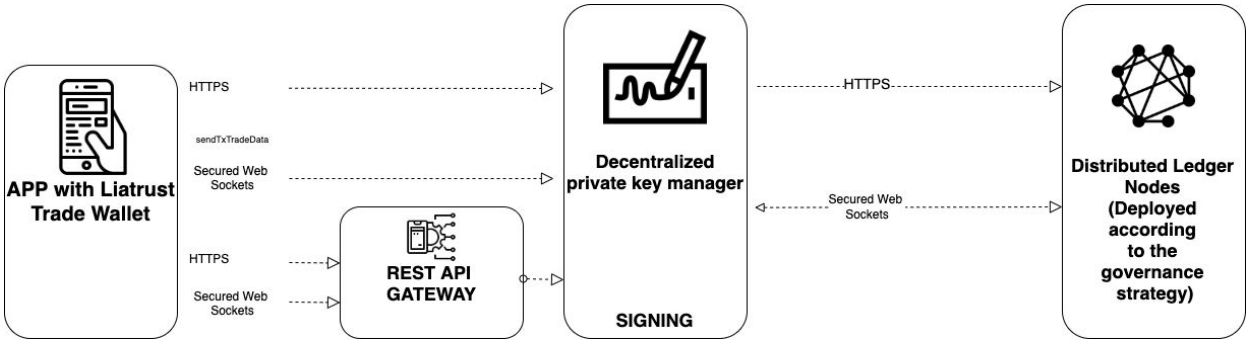

Figure 6. Interaction avec le Trade Wallet de Liatrust

Commentaire du schéma :

- Liatrust Trade Wallet est la seule propriété de l'acteur d'une transaction.
- L'acteur en tant que personne physique et agissant au nom de son entité légale ne peut interagir (signer) sur l'écosystème sans un lien cryptographique avec son entité légale.

- Un système de backup géré par son entité légale lui permet de récupérer son Trade Wallet.
- Liatrust fournit des services cryptographiques permettant d'assurer ce haut niveau de sécurité.
- La notion de décentralisation dans ce contexte précis, doit être entendue en tant que multi-device ou multi-server.

Liatrust porte une attention particulière à la gestion des clés privées des acteurs de la transaction. Ainsi nous avons choisi d'utiliser une technologie permettant un très haut niveau de sécurité. La section suivante en parle d'avantage.

3.3.2. Système cryptographique utilisé

Les acteurs de l'écosystème Liatrust sont amenés à signer cryptographiquement l'empreinte de leurs données pour matérialiser leur statut d'émetteur ou de possesseur des données. Ceci permet aux autres acteurs mandatés de vérifier cette signature. Ce procédé est basé sur un système dit asymétrique de clefs publiques/privées. Les clefs privées sont associées à une identité représentée par une adresse qui est l'équivalent de la clef publique. Le Trade Wallet est l'objet encapsulant cette adresse.

Le stockage de ces clefs d'une manière fortement sécurisée tout en évitant les tentatives de violation est primordial pour un système sain capable de digitaliser la confiance entre des acteurs du commerce international. Vu leur importance, les clés privées demeurent une cible attractive pour les utilisateurs malicieux. C'est le talon d'Achille d'un système de gestion de clefs centralisés. Ainsi, il est nécessaire de proposer des solutions avec un niveau de sécurité aussi sûr que du hardware cryptographique dédié qui est très coûteux.

Par ailleurs, le procédé même de signature expose une surface d'attaque non négligeable. Les algorithmes de signature proposent un vrai défi; ces algorithmes doivent être effectués à l'abri et en toute confidentialité et authenticité pour éviter leur exposition.

La solution proposée par Liatrust est de traiter le problème en amont. Ce qui est possible en tenant compte des étapes suivantes:

- L'adoption d'un système de gestion de clefs distribuées sans surface centrale d'attaque
- Une abstraction de la clé privée rendant toute tentative de violation très difficile qui demande la prise en otage de plusieurs serveurs simultanément.

Nous offrons une panoplie de fonctionnalités pour répondre à ce défi :

1. GENERATE_GENERIC_SECRET: Création de la clé initiale qui sera utilisée dans la procédure d'abstraction de clé.

2. ABSTRACT_SECRET: En se basant sur le secret initial, cette méthode nous permet de décentraliser les clés qui seront utilisées dans les opérations initiées par le Trade Wallet.
3. KEY_GENERATION: Cette opération permet de créer une clé publique et une clé privée abstraite décentralisée. Comme les parties prenantes collaborent par le biais d'algorithmes distribués, la clé privée demeure inconnue.
4. SIGN_DATA: Utilise la clé précédente avec un algorithme distribué pour signer une empreinte de la donnée en jeu dans le cadre du certificat d'origine. Ceci peut être une donnée atomique ou un flux de document.
5. KEY_REFRESH: Mise à jour de la procédure d'abstraction et de décentralisation de clés.

En adoptant cette stratégie de sécurité, Liatrust arrive à proposer un haut niveau de sécurité même dans le cas d'intrusion malveillante dans l'écosystème. Un utilisateur malicieux ne pourra pas falsifier des données comme il n'a pas le consentement d'autres parties. S'il tente d'aller à la conquête des clés privées, comme dit précédemment, il lui faudra avoir la main sur tout l'écosystème en même temps. Une tentative qui est pratiquement très difficile, de plus, avec la mise à jour automatique et périodique de la procédure d'abstraction et de décentralisation de ces clés, elle est quasi inviolable.

3.3.3. Gestion des autorisations

Toutes les autorisations de la plateforme Liatrust reposent sur un système de contrôle d'accès par rôles jumelés avec des autorisations natives associées à chaque Trade data dans le registre. Par cette granularité, les différents acteurs n'ont accès qu'aux informations nécessaires à leur tâches pendant le cycle de vie de la transaction. Nous assurons aussi des preuves immuables à chaque accès afin d'avoir une traçabilité complète du cycle de vie de la donnée.

4. Gouvernance des services Liatrust

4.1. Gouvernance des services applicatifs

L'une des difficultés majeures de la digitalisation de la documentation d'une transaction du commerce international en générale et du certificat d'origine en particulier est d'assurer l'accessibilité des données d'une manière intègre et authentique au-delà des frontières nationales. Ceci implique des accords internationaux avec une infrastructure interconnectée. Il est donc important de mettre en place une gouvernance technologique qui demande une volonté commune. Ainsi l'identification des partenaires du Maroc qui sont "technology friendly" et près à s'investir dans ce type de projet est un préalable pour la réalisation de notre ambition.

Afin de préparer les argumentaires qui permettront de bouger les lignes avec les partenaires internationaux et permettre une digitalisation efficace en toute confiance, il est important de réaliser un produit permettant une institutionnalisation des processus entre pays.

Pour permettre une gouvernance efficace, il est important que la conception du système soit ouverte et interopérable basé sur des APIs et des applications clés en main.

Commençons par expliciter ces notions.

Tout d'abord, afin de faciliter au maximum l'adoption d'un produit IT par une organisation, il est essentiel de fournir une expérience développeur ergonomique permettant une intégration rapide, efficace et sécurisée. La notion d'API (Application Programming Interface) est un paradigme qui permet d'exposer des contrats d'interface minutieusement documentés et prêts à l'emploi. Pour avoir une expérience développeur ludique et fluide, il est d'usage de fournir également une sandbox de test et simulation sous forme de machine virtuelle. Dans le cas par exemple d'un consortium porté par divers acteurs portuaires internationaux, Liatrust fournit les APIs qui permettent d'interagir avec l'écosystème. Comme exemple, voici un certain nombre d'APIs applicatives nécessaire à l'écosystème :

- Service de création du Trade Wallet représentant l'identité d'un acteur (cette API demande l'utilisation de système cryptographique distribué sur plusieurs nœuds).
- Service de récupération des données associées à une transaction sous diverses granularités selon les autorisations pertinentes. Exemple un certificat d'origine numérique.
- Service de recalcul des empreintes des données et de vérification des signatures.

Par ailleurs, les APIs peuvent ne pas suffir pour atteindre les niveaux d'adoption souhaités. Il est donc important de fournir des kits clés en main (Software Development Kit ou SDK) afin de rendre l'intégration quasi-transparente.

Voici quelques points d'attention à apporter :

- Les Traders nationaux peuvent éprouver des difficultés d'adoption. Ces acteurs peuvent interagir avec l'écosystème Liatrust via une application clef en main permettant d'avoir un Trade Wallet.
- Pour les Trader internationaux, la situation est plus compliquée. Il est donc crucial de leur fournir un accès clefs en main et autonome leur permettant d'interagir avec l'écosystème sous forme d'application. Selon leur maturité technologique et leur degré d'intérêt d'intégrer ce type de solution à leur système local, nous pouvons proposer d'autres fonctionnalités. L'application Liatrust avec son Trade Wallet reste la première option.
- Concernant les acteurs institutionnels locaux, la solution proposée permet d'avoir plusieurs niveaux d'intégration. Les institutions faisant partie intégrante du consortium, auront la possibilité de gérer un nœud du registre distribué et prendre part au processus de validation des signatures des données de la transaction. Liatrust peut leur faciliter l'intégration de ce nœud dans leur système en fournissant des APIs Cloud intégrables avec leur système IT. Il y a aussi la possibilité d'intégrer localement tous les composants nécessaires pour participer au consortium.
- Concernant les acteurs institutionnels internationaux, selon les accords établis et le niveau de maturité technologique. Nous pouvons proposer divers scénarios :
    - Le premier niveau d'intégration permet de souscrire au Trade Wallet Liatrust représentant leur compte et leur identité. Ce wallet leur permet d'interagir avec le système en toute autonomie, avec confidentialité, intégrité et authenticité.
    - Le deuxième niveau d'intégration permet d'opérer un nœud du registre en local en tant que membre du consortium comme certains acteurs nationaux. Liatrust pourra fournir les outils permettant cette intégration.
    - Le troisième niveau d'intégration concerne les pays qui prévoient l'adoption d'une autre technologie ou d'un registre distribué indépendant, en consortium avec d'autres acteurs correspondant à leur enjeu économique. Ce registre peut être conçu avec des technologies différentes et variables selon les pays. Dans ce cas, Liatrust prévoit des composants d'intégration hautement sécurisés permettant de créer des ponts entre registre. L'idée étant de fournir des APIs permettant de rendre accessible avec des procédés cryptographiques les données des transactions inter-registres. Le Trade Wallet Liatrust est conçu pour encapsuler d'autres types de wallet afin d'interagir avec différents registres.

- Dans le cadre de l'intégration de toutes les données d'une transaction nécessitant une lettre de crédit ou un crédit documentaire, des organismes financeurs peuvent participer au consortium et avoir une intégration permettant d'accélérer d'une manière drastique les financements et la clôture de la transaction.
- L'une des manières de créer l'adoption est aussi l'incitation financière. Ce sujet sera traité dans la partie consacrée au modèle économique de la plateforme.

4.2. Gouvernance de l'infrastructure

En parallèle des services applicatifs, la facilitation de la mise en place d'un registre distribué est cruciale pour l'adoption de l'écosystème. Liatrust propose des APIs techniques permettant d'opérer un registre distribué en mode service. La solution proposée permet d'avoir différentes configuration dont l'une est schématisée dans le diagramme suivant :

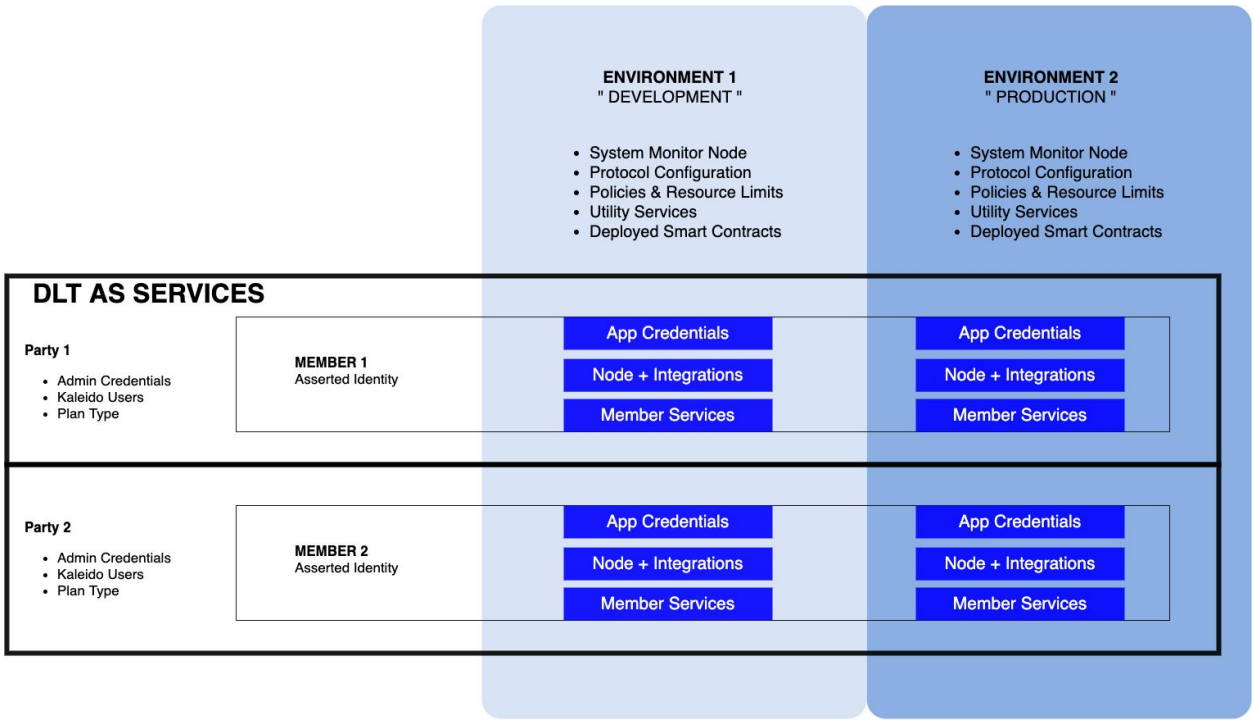

Figure 7. Membres du consortium

Liatrust met à disposition aux différents membres du consortium les outils nécessaires pour participer à l'écosystème.

4.3. Outils et technologies

Les technologies associées aux registres distribués sont en phase de maturation. Il existe une hétérogénéité et des spécificités techniques qui rendent les choix difficiles. Dans le contexte B2B et B2G du certificat d'origine et des transactions internationales en générales, les infrastructures de registres distribués devront être adoptées par plusieurs organisations. L'écosystème technique est le socle de la confiance entre les organisations qui permet de faciliter des accords juridiques pour fluidifier le commerce international. Ainsi, les choix

technologiques engageant dans cette ambition doivent être pris en tenant compte de cette problématique.

Voici les critères et les choix fait par l'équipe Liatrust :

Critère	Descriptions	Technologies
Registre privé en consortium (avec permissions)	Le cadre B2B et B2G impose un registre avec plusieurs autorités de validation des blocs de données. En annexe, vous pouvez consulter l'arbre de décision conduisant à ce choix (Voir *Figure 8*).	• **Hyperledger Fabric** • **Hyperledger Sawtooth** Le choix doit être guidé par le nombre de noeuds à opérer et le choix du consensus (CFT vs BFT[1])
Scalabilité	Assurer une montée en charge pour pouvoir absorber toutes les données des transactions du commerce international marocain	Les deux choix du consensus précédents doivent être arbitré selon le type de scalabilité voulu. Sawtooth permet la parallélisation des écritures et donc une meilleure scalabilité
Facilitation à l'adoption **Facilitation technologique** **"Register as a Service"**	La stack technique doit être "Entreprise Ready" afin de faciliter la réalisation du produit et réduire le "time to market".	**"Blockchain as Services"**. Infrastructure **conteneurisée**. **Sextant for Sawtooth** est un choix cloud pertinent (sous AWS). IBM cloud ou AWS permet le déploiement de Hyperledger Fabric
Convergence de modèle métiers pour une meilleure interopérabilité.	Le modèle à l'intérieur du registre (les "Smart Contracts") et en dehors doivent converger nativement.	**DAML** est un standard en bonne voie de généralisation. Il s'intègre à Fabric et Sawtooth. D'autres langages sont possibles selon le registre.
Facilitation du prototypage	Pour accélérer le "time to market"	**DAML** permet un prototypage rapide au-dessus de divers types de couches de persistance sous forme de registre.

Table 2. Matrice des technologies

[1] Protocol de consensus pour le stockage dans le registre distribué

5. Modèle économique

Dans cette section nous allons aborder le modèle économique du consortium qui permet une adoption de l'écosystème. Puis nous allons décrire le modèle économique de Liatrust.

5.1. Incitation et motivation à l'adoption

L'incitation économique pour l'adoption est un levier pertinent pour pousser certains acteurs hors du maroc à interagir avec l'écosystème. La digitalisation End to End de la confiance dans les processus de gestion du certificat d'origine et de gestion des informations d'une transaction d'import/export permet des économies de temps et donc d'argent. Ceci est un argument en soi pour l'adoption. Cependant, vu le contexte concurrentiel, il est important d'identifier d'autres leviers d'adoption.

L'adoption de l'écosystème Liatrust devrait s'accompagner d'une réduction sur les frais associés à l'émission des certificats d'origine par exemple. Et donc il serait pertinent d'imputer cette réduction sur l'ensemble des acteurs via des remises sur factures.

Les détails de ce système doivent être conçus en tenant compte des systèmes actuellement en place permettant de régler les divers frais liés à une opération d'import/export.

5.2. Modèle économique de Liatrust

Le modèle de la plateforme Liatrust est un **modèle SAAS** sous forme d'abonnement par nombre d'enveloppes de signature.

Dans le cadre du certificat d'origine, une enveloppe de signature correspond à la gestion d'un certificat d'origine End to End. Les détails de ces abonnements seront fixés après le chiffrage financier lié à l'infrastructure et à l'organisation que mettra en place Liatrust pour réaliser ce projet avec ces partenaires.

6. Conclusion

Chez Liatrust, nous avons l'ambition de mettre les nouvelles technologies au service de la confiance dans les échanges des données dans une transaction d'import/export. La dématérialisation de la confiance dans la gestion du certificat d'origine est un challenge conséquent permettant de prouver la valeur ajoutée de nos choix et notre écosystème.

Cependant, notre ambition dépasse le cadre du certificat d'origine. En effet, pour arriver à simplifier l'émission de ce dernier, il serait aussi pertinent de dématérialiser la confiance d'autres procédures en amont permettant de consolider avec un niveau de trust jamais égalé toutes les données d'une transaction à l'international. C'est un projet faramineux et nous en avons l'ambition et les compétences techniques.

Liatrust propose des applications web et mobiles décentralisées qui reposent sur un registre distribué permettant d'échanger des informations avec intégrité et authenticité. Nos choix technologiques permettent une réduction du "Time to Market" et nos compétences nous permettent de proposer des architectures cloud natif avec une organisation de génie logiciel agile suivant les principes de DevSecOps[2] et de l'Hexagonal Architecture[3] pour construire un écosystème robuste et continuellement améliorable.

L'équipe Liatrust a été ravie de travailler sur le processus de gestion du certificat d'origine pour ce challenge et nous serons heureux de construire le monde de demain du commerce international marocain avec nos futurs partenaires.

[2] Équipe multidisciplinaire de développement, de sécurité, d'intégration et de production

[3] Architecture modulaire évolutive

7. Annexes

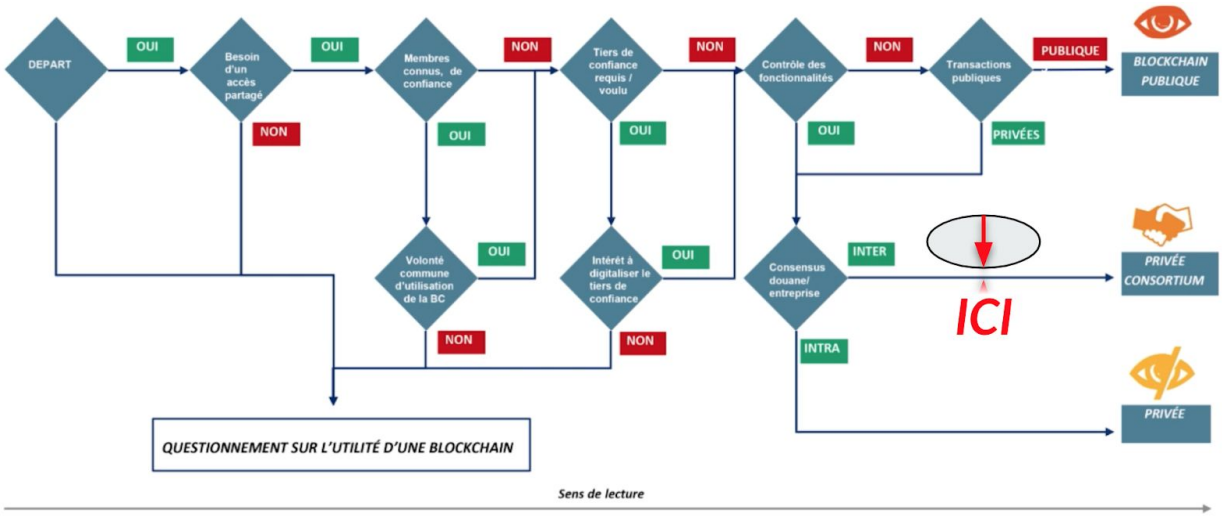

Figure 8. Décisions technologiques

Quelques liens utiles

- Cartographie des règles d'origine pour une construction d'une base référentielle.
- Hyperledger Fabric
- Hyperledger Sawtooth
- Sextant Cloud for DAML
- DAML docs