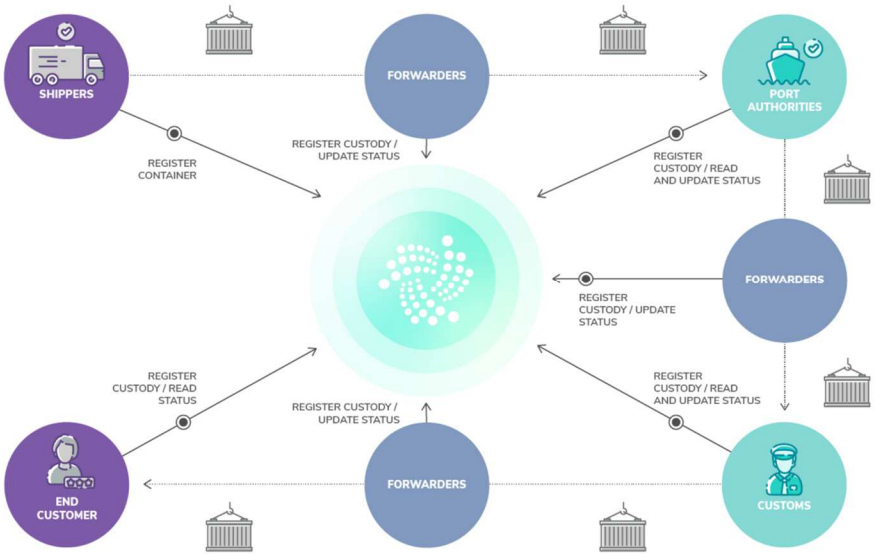
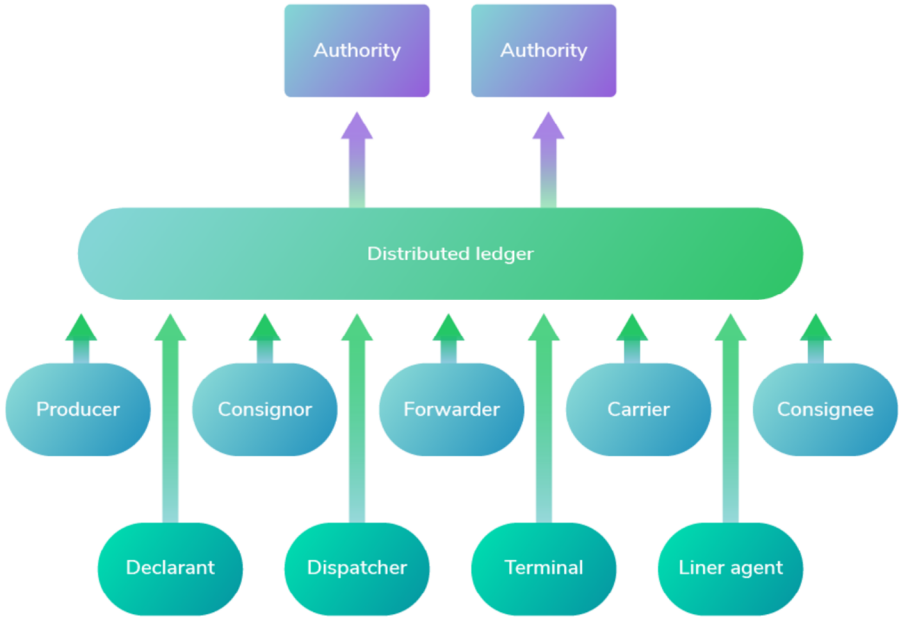
Trade Facilitation and Customs Management

Section 1: Summary

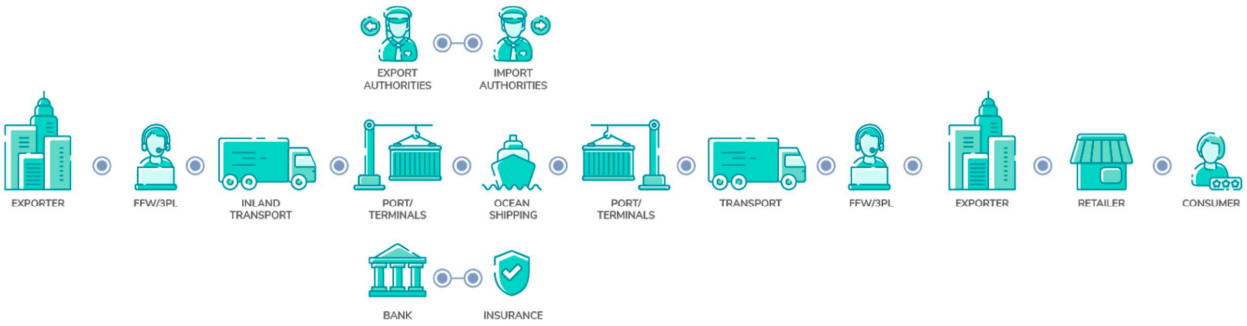
Use Case Summary			
Use Case ID:	IND-008	**Use Case Type:**	*Vertical*
Use Case Title:	Trade facilitation and customs management	**Is Use Case supporting SDGs**	*No*
		Domain:	Industry/Supply Chain
Status of Case	*Proof of Concept*	**Sub-Domain**	
Contact information of person submitting	*Full Name:* ***Lewis Freiberg*** *Job Title:* ***Director of Ecosystem*** *E-mail address:* *lewis@iota.org* *Telephone number:* ***+1 443 693 7730*** *Social media:* *Web site:* ***https://iota.org***		
Proposing Organization	IOTA Foundation, Germany Organisation ID: 3416/1234/2		
Short Description	Distributed ledgers offer a unique platform for stakeholders in international trade facilitation and customs management to interact in meaningful ways. Where digitisation efforts have failed previously, DLTs can enable increases in efficiency that will encourage the spread of the technology in the industry. This Proof of Concept demonstrates the way in which DLT can impact global trade.		
Long description	Cross-border trading involves a selected number of actors, including but not limited to: shippers, forwarders, customs and traders. Such actors are involved in a number of processes dealing with the following challenges: ● how trade certificates can be shared and checked for authenticity even before a shipment is initiated or when it is already on its way; ● how the different actors handling a shipment can report its status (e.g., cleared for export, Gate-in into the port, on-board a vessel etc.); ● how the different actors can share an auditable record of the conditions of the shipped goods (temperature, location, shock, etc). Due to the multi-stakeholder nature of these processes, simplifying them requires the creation of a data exchange layer which uses the IOTA Tangle and other IOTA technologies. IOTA DLT helps to ensure the integrity of data and to maintain trust among the parties involved in the international shipment of containers goods.		
SDG in Focus (when applicable)	*None as of yet*		
Value Transfer:	This use case **does not** use tokens to transfer value.	**Number of Users:**	
Types of Users:	Governments, Corporations, NGOs, SMEs & Consumers		
Stakeholders	Figure below shows a stakeholders' map, highlighting a container journey, its different chains of custody (dotted arrows) and those		

	stakeholders (namely custodians) eventually responsible of updating the container status and the associated shipment documents (plain arrows). In the case of international trading of goods, a container is first sent by a shipper. Subsequently, the container is handled by a forwarders until it reaches a port operator and later a custom clearance agent. 
Data:	The data for this use case is stored on the permissionless IOTA ledger so each actor can access and verify the information. The PoC utilizes encrypted messaging streams to publish records about the shipment from each actor. This ensures a level of privacy that ensures that others using the network aren't able to decrypt the information even if they were able to capture it. The data is published in a machine readable format to ensure that companion applications accessing the ledger are able to interpret the information efficiently. The structure of this information is discussed below in the process discussion. In some solutions requiring real-time data sharing, supply chains actors store on the ledger hashes of information while original information is shared via another communication channel. Received information and its hashes are compared to ensure that the received data has not been tampered.
Identification:	The trade facilitation proof of concept primarily deals with the flow of information between actors through the various interactions with the shipment. Given that these data records are important ensuring the integrity of the data is high priority. This is enabled via the use of DLT given its properties of immutability. However, above tamper resistance is the requirement that the information be correct when it is entered. In order to track provenance of information and identify responsibility, it is required to bind information to the actor unique identity. This requires to create an non-repudiable identification system for the different actors. This allows auditors to correct identify owners of stored information. Within the Trade Facilitation proof of concept we do not directly address the identification problem neither the KYC verification of all parties.

	Given the large complexity of this, identity verification is out of scope for the proof of concept at this point. What the PoC does do is ensure once an actor engages with the shipment, all subsequent transactions that are related can be verified as coming from the same entity. However at the moment there is no way to bind this entity identity to an organization identity. This is achieved by using a 2nd layer library called Masked Authenticated Messaging which will be discussed below. Weak identities are bind MAM Channel root keys.
Predicted Outcomes:	An IOTA powered data exchange layer for trade can deliver the following benefits for each stakeholder category. **For shippers:** ● It simplifies paperwork, enables easy way to provide documents and certificates, even when container is already on its way to the destination; ● It enables container position updates and status monitoring; ● It provides overview of chain of custody, handling of goods during shipment; ● It creates an immutable audit trail accessible to refine shipper risk profile and to facilitate their access to services such as trade finance and trade insurance. **For customs clearance :** ● It simplifies access to container load information and all related documents and certificates; ● It provides access to shipment information and simplifies direct contact if required; ● It enables government agencies to shift to a Riskbased approach of assessing consignments by enhancing ● the accuracy and reliability of their risk profiling techniques and tools. **For port authorities and freight forwarders:** ● It simplifies access to container route information and estimated time of arrival; ● It provides access to temperature sensor information with optional alerting functionality in case of ● temperature value rise or power outages; ● It simplifies documentation handling and prevent loss of documents and associated costs. The bullets above shows the complexity of the involved ecosystem and the associate number of systems that would require integration in order to allow seamless sharing of the required information. Instead, this system describes a proof of concept platform that allows to share shipment information across any number and type of stakeholders. Such information includes transport conditions of a given container, its location and other monitoring data (e.g., temperature), its chain of custody and other handling events as well as a digital authenticated versions of the associated trade documents, such as Certificate of Origin,

	Phytosanitary Certificate, packing list etc.  Through the use of the IOTA Tangle the information associated to the container is shared across all the above actors without requiring any direct integration of proprietary systems. With the use of a distributed ledger, like IOTA, integrity of the shared information is guaranteed, whether this being data or digital documents. This way all the actors handling the container can read and update relevant information without any delay, and so speeding up all the associated operations.

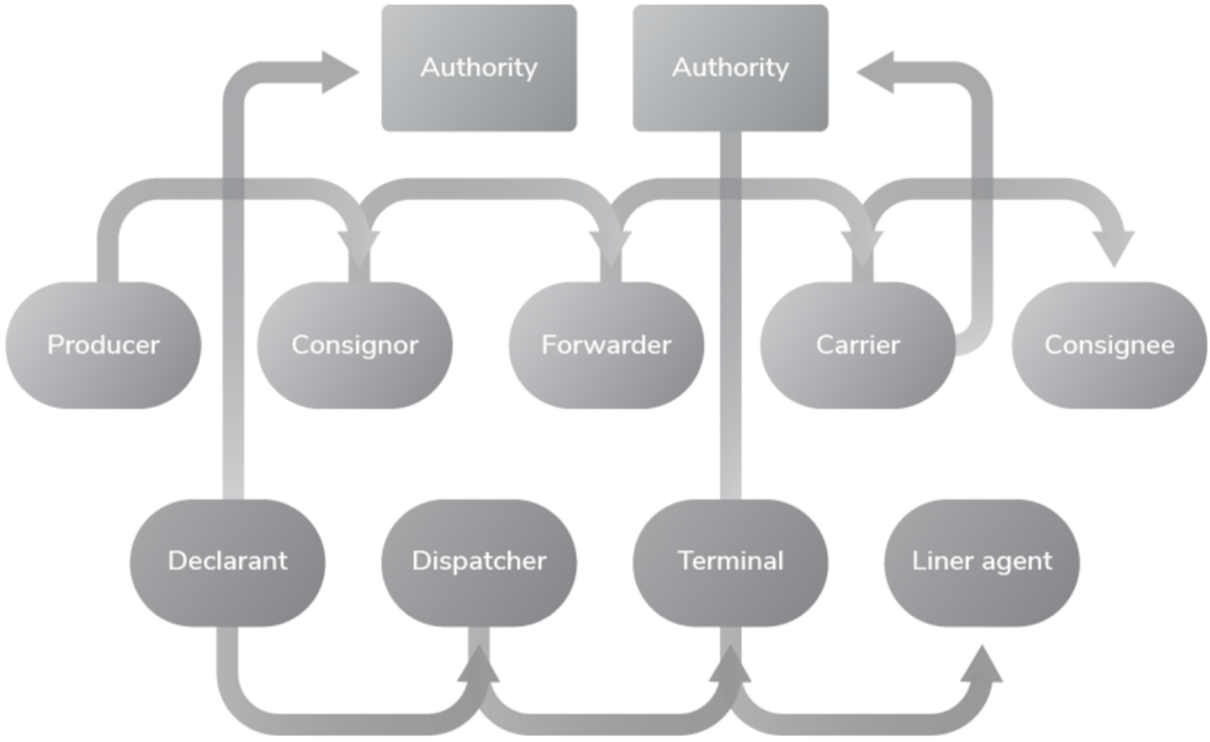
Overview of the Business Problem or Opportunity
International trade is a complex system facing a number of inefficiencies. Figure 4 below shows how international containers shipment of goods is mainly composed of many actors and three flows: ● the physical movement of containers; ● the exchange of data and documents associated to the traded and the transported goods; ● the transfer of any monetary flow associated to the container and the transported goods.



Without considering the third flow, the first two already pose a number of challenges the effect of which is slowing down the speed of international trading. Some of these challenges include:

- Information about transport conditions are collected and stored in siloed systems;
- Full tracking of containers position and chain of custody is not seamlessly visible and in real-time to all the parties handling the container;
- The trading documents and certificates (often paper-based) travel separately from the container and its goods thus many times leading to delay in the clearance procedures, as consequence of document being missing, lost or not timely delivered.

Today's supply chains are driven by actors pushing information to the next actor in the chain and requesting updates on containers and their content status, approval of shipping documents and payment of required taxes.



Innovation in the international trading has been so far unsuccessful due to the following too established practices:

- Emails, phone calls and paper documents are the daily details of moving goods;
- Information is delivered bilaterally and retyped into new systems with introduction of errors and loss of data integrity and authenticity;
- Multiple data formats are used and often not compatible one with the other.

As result, actors are unable to automatically broadcast/receive notification of events to relevant parties. This generates delay, inefficiencies and loss.

It is calculated that improving all countries' trade facilitation halfway to global best practice would increase global trade with 15% and global GDP with 4.7 % - before even introducing DLT and Trade Policy 3.01.

Why Distributed Ledger Technology?

Use of distributed ledger technologies, and IOTA in particular, can help to mitigate these risks. The permissionless nature of IOTA Tangle allows for any party to start sharing the required information, with guaranteed integrity.

In addition, the use of the 2nd layer MAM protocol allows for fine grain control of information access, despite the distributed nature of the IOTA Tangle. Moreover, using IOTA as trusted data exchange layer, in future scenarios, the use of Token (and IOTA Qubic) could allow to create automated verification of documents and transport conditions and consequently automate moving of associated monetary flows (trade finance) .

Section 2: Current process

Current Solutions

If there are existing systems which automate the above business problem/opportunity.

Existing Flow (as-is)

Step	User Actions	System Actions
1.		
2.		

Process scheme (as-is)

Data and information (as-is)

Data	Type	Description
1	*Documents*	

2	*Payment transactions*	

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Lawyers*	
2	*Bank*	

Other Notes
Any assumptions, issues

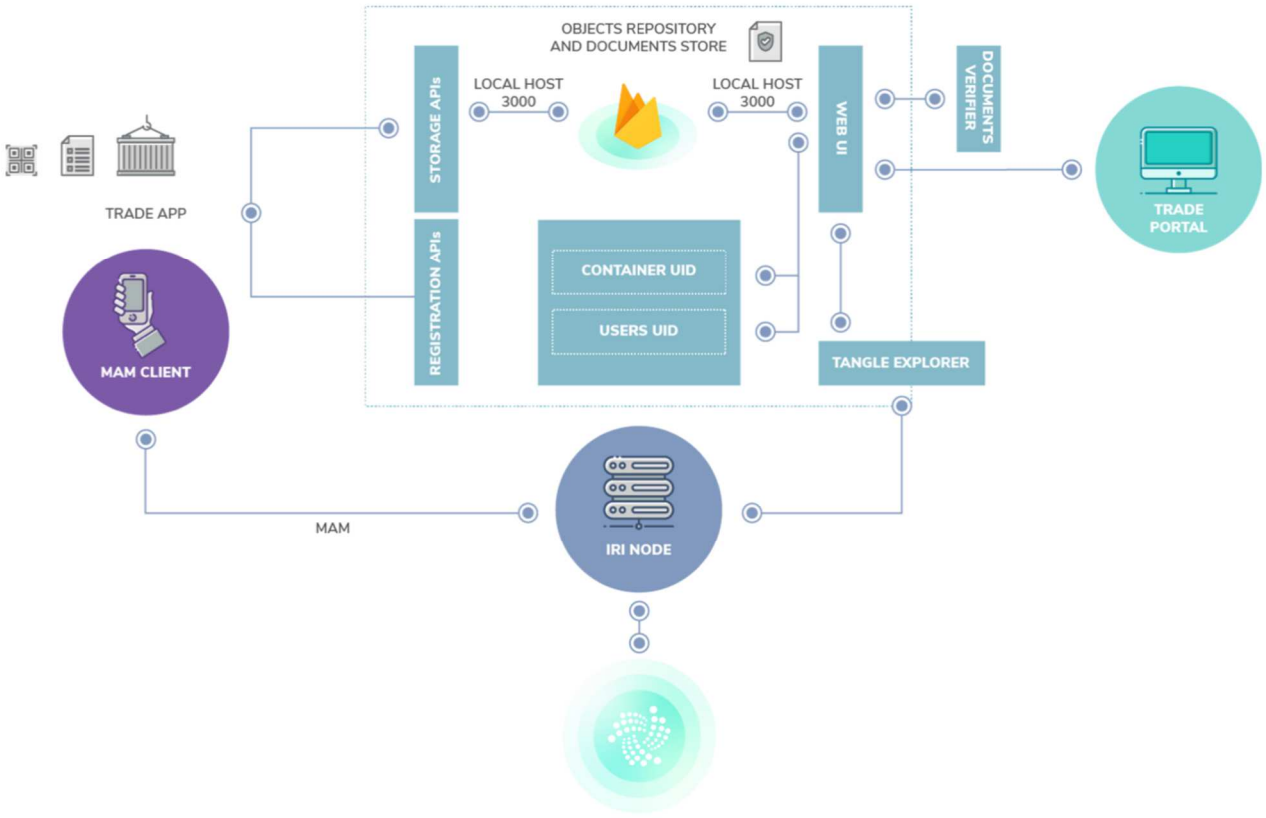
Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Through a web portal or mobile app a shipper acquires the given container SSCC number, e.g., by scanning a Barcode,	The application creates a digital representation of the container, the so called **digital twin**, which includes container id and additional information (e.g., container status, load type, temperature, route, position). A digital copy of the shipping documents is also uploaded and a hash of them referenced into the container's digital twin. The updated digital twin is then recorded in an immutable way onto the IOTA Tangle together with the identity of its shipper;
2.	When the container is handed over to a forwarder, through the same portal and QR-code, the new custodian attaches to the container digital twin its identity as well as its location (when available) and updates other relevant information, including specific supply chain handling events.	Updated information is recorded onto the Tangle in order to further trace the container journey;
3	When the container reaches a port authority or a custom clarence point, an agent can use the portal or the mobile app to acquire the container identity and, if authorised, to access in real-time all relevant	This information is fetched directly from the IOTA Distributed Ledger.

	information needed to support her operation,	
4	Following that, an agent can finally issue new events about the container (e.g. Cleared for export) by updating its digital twin.	This become immediately visible to all authorised parties. After that, the container is finally delivered to its end-customer, who can verify its whole journey, by retrieving the full digital twin from the IOTA DLT (from everywhere and at any time).

Process scheme (to-be)

Note: The international shipment of containers consists of a chain of events, information and actors involved in the handling of a given asset (the container and its goods). Because of this, associating each given container shipment to a dedicated Masked Authenticated Messaging (MAM) channel makes easy to store the different generated information onto the IOTA Tangle as a sequence of MAM messages in the same channel. Using MAM allows for encryption and protection of the shared information. Without using MAM, this could alternatively be done by issuing to the IOTA Tangle independent transactions that store the information generated by each handling procedure of a given container. However, the architecture complexity of reconciling and linking all the information associated to a given container shipment would increase. Hence MAM was chosen as preferred design solution.



Once a new container is first registered by its shipper a new IOTA MAM channel is created. A digital twin for the container is created with the following information: <containerUniqueID, containerOwnerID, containerCustodianID, cargoType, origin, destination, location, temperature, time, status, documents list>.

Required information is captured through the Trade PoC app:

- containerUniqueID is captured through Barcode scanning. In future implementation it can be matched against a containerUniqueID server (e.g., GS1 SSCC) for verification purpose;
- information about the containerOwnerID is inserted through the portal. In future implementation it could be fetched from an external source (e.g., a registration server for the use of the app or a self-provided KYC);
- containerCustodianID initially coincide with containerOwnerID;
- location (and temperature) are not implemented but they can optionally be acquired by a dedicated beacon5 installed into the container;
- time is acquired by the mobile phone or an installed beacon;
- status could corresponds to standard EPCIS Supply Chains events. For this PoC we use a set of predefined standard statuses. Initial status it set to Container Announced;
- documents list contains external URLs to relevant shipping documents alongside with their computed hash.

The information is stored to the IOTA Tangle using the javascript MAM client library. This can either be embedded into the app or be implemented through an external server (MAM Server, not shown here), to which the app exchange information using secure HTTPS REST APIs.

After creation of each MAM channel, a central back-end Object Repository is populated. The Object Repository is implemented as Firebase NoSQL database and deployed using port 3000. Storage REST APIs are provided to populate and update the Firebase DB with information related to the MAM channel associated to a given containerUniqueID. Information stored in the Object Repository includes the root address of the channel, e.g., where this can be accessed on the IOTA Tangle and the cryptographic key needed for decrypting the information stored in the channel (named side keys) , in case restricted MAM channels are used. The following tuple is created and stored in the Object Repository: *<containerUniqueID, channelRoot, channelSideKey>*.

The Object repository is either populated by the app or the MAM Server, according to the implemented architecture. Access to the Object Repository is managed by the given container shipper, thus guaranteeing control on who can access and modify the information chain associated to a given container shipment (e.g. by adding new MAM messages).

For a given shipment, when the container changes custodian, information about the new custodian is appended to the existing MAM channel. Additionally location and temperature of the container can also be updated, by the new custodian (or automatically by any beacon installed in the container). For that, a new MAM message, with updated digital twin information, is attached to the existing channel. The following information is updated and stored onto the Tangle: *<containerCustodianID, location, temperature, time, status>*.

In order to achieve this the mobile app (or the beacon) needs to access, either directly or through the MAM Server the information related to the root of the MAM channel associated to the given container (e.g. where the given channel is stored onto the Tangle). This information is fetched from the Object Repository, by using as primary key the containerUniqueID, which is obtained from the Barcode scanning, manually inserted (or preloaded into the beacon). The following two functions:

createItem(eventBody, channel, secretKey, userId);

updateItem(eventBody, mam, newItemData, user);

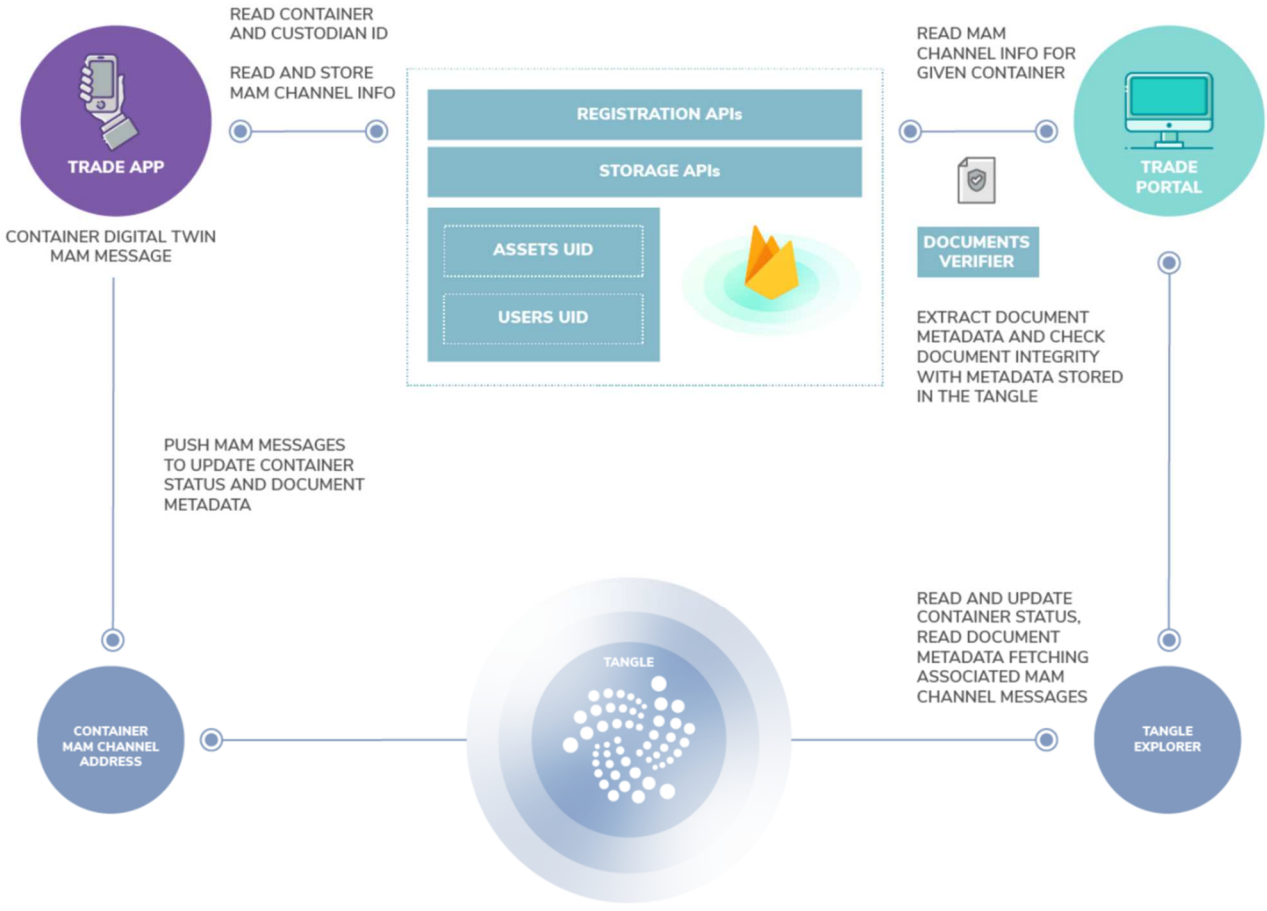
have been implemented in order to respectively access and update existing MAM channel information (e.g. adding new messages to update the stored digital twin). Information is then attached to the correct MAM channel and stored immutably onto the IOTA Tangle.

In case of new documents upload or update of existing ones, every time a document is saved by one of the actors in any Document Storage (Figure 6 shows only one for simplicity), its metadata including size, last change date and calculated hash checksum are stored in the IOTA Tangle as part of the digital twin associated to the container. In case of update of existing documents, the original copy hash checksum is retrieved and a new one calculated in real time. If there are differences with the stored values, a Documents Verifier (implemented in the web or mobile app) will send an alarm to the current actor and indicate that documents' content is no longer integral and has been changed.

A Web UI (WUI) written in React implements APIs to access to the MAM explorer and to retrieve information, e.g. container custodian, location, temperature and lists of associated documents and events. Information on the Tangle is retrieved by accessing the required channel root address obtained from the Object Repository.

With the same GUI a list of document hashes associated to a given container can also be retrieved. Documents that have been altered from their initial version are flagged red.

The communication diagram below shows the different messages exchanged across the architecture components presented above.



Participants and their roles		
Actor	**Type/Role**	**Description**
1	**Shippers/Exporters**	The shippers are often also the exporter/producer of goods. They load the container with goods and initiate a number of the needed shipping documents for export; then they handover the

		container and shipping documents to forwarders. Container and shipping documents might be handled by different sets of forwarders.
2	**Forwarders**	Forwarders are agents who coordinate with the other participants in the shipping process on behalf of the importer/exporter. They will coordinate pick-up of container, manage part of the shipping documents including transfer to port authorities, customs, shipping liners etc., update container routes.
3	**Port Authorities**	Port authorities of at least two countries are involved in the shipping process. The port authorities receive the container and documents from the forwarders. They will handle logistics within the port area including moving container to Customs for inspection and loading it onto the vessel.
4	**Custom authorities**	In any international trade, custom authorities of at least two countries - country of export and country of import - are involved. The customs authorities provide clearance for the goods to leave the country of export and enter the country of import. They need access to shipping documents.
5	**End-customers/Importers**	They receive container and documents from Forwarders and check container status and transport conditions.

Data and information		
Data	**Type**	**Description**
1	*Digital Twin*	This is the data representation of the Digital Twin used in the trade facilitation PoC:: "data": [{ "containerUniqueID": "number", "containerOwnerID": "string", "containerUserID": "number", "location": "string", "temperature": "number", "time": "date", "documents": [{ "link": "string", "hash": "string"}], "status": "string" }]

Security and privacy
1. **Data Tampering:** This is a primary concern when dealing with sensitive data. This issue is mitigated through the use of the distributed ledger as this is one of the core properties of the technology. 2. **Access control:** When dealing with a public ledger like IOTA, anyone has the ability to write & read transactions. This is a core freedom of the protocol. However, given this right there needs to be considerations about how to protect access to the information and disruption of the records. To mitigate this the use of encrypted messaging renders the information unaccessible to those without

the proper authorisation. Similarly those without the means to correctly encrypt new information will be unable to add new information into the application and disrupt it.

Main Success Scenario + expected time line

Conditions (pre- or post-)

Performance needs

Using the IOTA ledger as the basis for this application allows for a near real time performance of the proof of concept. IOTA is a unique technology in a number of respects, but the relevant features for this use case are: a) feeless transactions b) a lack of blocktime.

These two features enable entities to publish data transactions to the network in exchange for a small amount non-competitive PoW and validation. Additionally, due to a lack of blocks, transactions are immediately readable back from the network. Given the transactions is only data and doesn't need to be confirmed there is no need to wait for the transaction to be included in the next block. This means that the network is able to run at speeds that can accommodate the sheer volume of reads and writes that would be seen in a real world applications.

Furthermore given the network is permissionless, any entity wishing to partake in this process is able to create a node on the network and start transacting as well as reading data from it. This ensures an equality of actors whether they are a Government, NGO, Corporation or the end consumer.

Legal considerations

Value:

The trade facilitation use case doesn't utilise the native IOTA token. This means that those wishing to use the system do not have to purchase tokens to participate. This is extremely advantageous as most governments have sparse or non-existent regulations surrounding cryptocurrencies which would prohibit participation from government ministries or even companies residing in certain jurisdictions.

Furthermore at the time of submission IOTA is the only operating permissionless distributed ledger that does not require the ownership of tokens to send transactions. So in Ethereum must use previously purchased Ether to pay the `Gas` fee for a transaction, in IOTA you exchange a small amount of computing power to help validate and secure the network when sending a transaction.

Data:

When building any system on a distributed ledger the data is being stored in an immutable database. There is no way to remove information from the system once it has been published. This poses interesting challenges when complying with data protection regulations in various countries, especially when the information must interact with a number of different nations during its regular operation.

This requires the organisations interacting and storing data on the ledger to adhere to the relevant regulations in their countries. Failure to do so could create a breach of data protection laws and may incur fines.

Risks

Special Requirements

External References and Miscellaneous

For information on IOTA and how it operates, please read here: https://docs.iota.org/docs/iota-basics/0.1/introduction/overview
For how-to deploy a Firebase server for the required PoC backend functionalities, please read here: https://firebase.google.com/

For how-to connect to an IOTA node, and sending transaction to the IOTA network using IRI, please read here: https://docs.iota.org/iri

For how-to to create MAM Channel and messages, using the IOTA MAM JS library, please read here: https://github.com/iotaledger/mam.client.js

Other Notes