Energy Distribution with the Use of Smart Contracts

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-001	**Use Case Type:**	*Vertical*
Submission Date:	October 17, 2018	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Energy distribution with the use of smart contracts	**Domain:**	*Industry*
Status of Case	PoC	**Sub-Domain**	*Energy*
Contact information of person submitting/ managing the use-case	Ioannis Kounelis, ioannis.kounelis@ec.europa.eu Joint Research Centre (JRC), European Commission Via E. Fermi 2749, TP 580 21027 Ispra(VA), Italy Telephone number: +39 0332 78 3653 Social media: https://twitter.com/EU_ScienceHub Web site: https://ec.europa.eu/jrc/en		
Proposing Organization	European Commission		
Short Description	In this use case, taking advantage of the potentialities of blockchain technologies, we propose a solar energy production and distribution architecture using smart contracts, a particular distributed ledger paradigm, to support automatic energy exchanges and auctions, potentially enabling a new, open and more fruitful, under an end-user perspective, energy micro-generation market.		
Long description	In our model, we assume a local grid where energy is produced and consumed in a limited geographical area, such as a local neighbourhood. Energy produced by a prosumer may be saved in the user's local battery for later use or may be immediately injected in the local grid. An additional possibility is to have a common, central to the neighbourhood, battery shared as a temporary energy buffer. The model is divided in three layers: (a) the energy grid, (b) the middleware controller, and (c) the smart contract. When energy is injected in the grid a smart meter linked to each producer continuously measures how much energy has been injected in total. These smart meters, along with the software that handles their output, i.e. a middleware controller, are the input source for our smart contracts. After a predefined amount of energy has been injected to the grid, an Helios Coin (HEC) is awarded to the corresponding prosumer. The middleware controller interconnects the grid with the smart contract since these systems cannot communicate directly with each other. As a result, the controller plays the role of invoking the smart contract on one end, and on the other receiving the readings from the grid, thus facilitating communication between the two entities.		

SDG in Focus (when applicable)	Goal 7: Affordable and clean energy		
Value Transfer:	tokens	**Number of Users:**	
Types of Users:	energy producer, energy consumer, smart meter		
Stakeholders	energy producer, energy consumer, electricity grid		
Data:	*energy data*		
Identification:	energy producer (anonymous), energy consumer (anonymous), smart meter		
Predicted Outcomes:	The main aim of our model is to enable micro-grid prosumers to produce, consume and trade energy. In particular, they would be able to: • Release excess energy to the grid and receive virtual coins in return • Transfer/Exchange the virtual coins • Redeem the virtual coins in exchange with energy • Enable prosumers to access the energy market		

Overview of the Business Problem or Opportunity

Business Problem:

Micro-generation is the capacity for consumers to produce electrical energy in-house or in a local community. The concept of "market" indicates the possibility of trading the electricity that has been micro-generated among producers and consumers, where a user acting both as a producer and consumer is called a "prosumer". Traditionally, this market has been served by pre-defined bilateral agreements between prosumers and retail energy suppliers. This means that until now, electricity-generating prosumers have not had real access to the energy market, which remains a privileged playing field for the institutionalised energy suppliers. This fact has, so far, heavily impacted on the real diffusion at large scale of micro-generation due to the limited economic advantages this energy generation approach would bring to the prosumers.

Opportunity:

The main options considered so far by the technical literature, were completely centralised and their viability (under a prosumer perspective) was in general challenged as they introduce additional management fees and costs and assume the intervention of a trusted third party reducing once again the potential gains of end-users. New approaches should be developed enabling end-users to have free access to the energy market. In this context the advent of distributed ledgers, i.e., blockchains, can be considered beneficial.

Why Distributed Ledger Technology?

Blockchain enable users to access the energy market and exchange energy directly with other entities without trusted centralized third party.

The DLT features required are verifiability, security, resilience, transparency.

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**

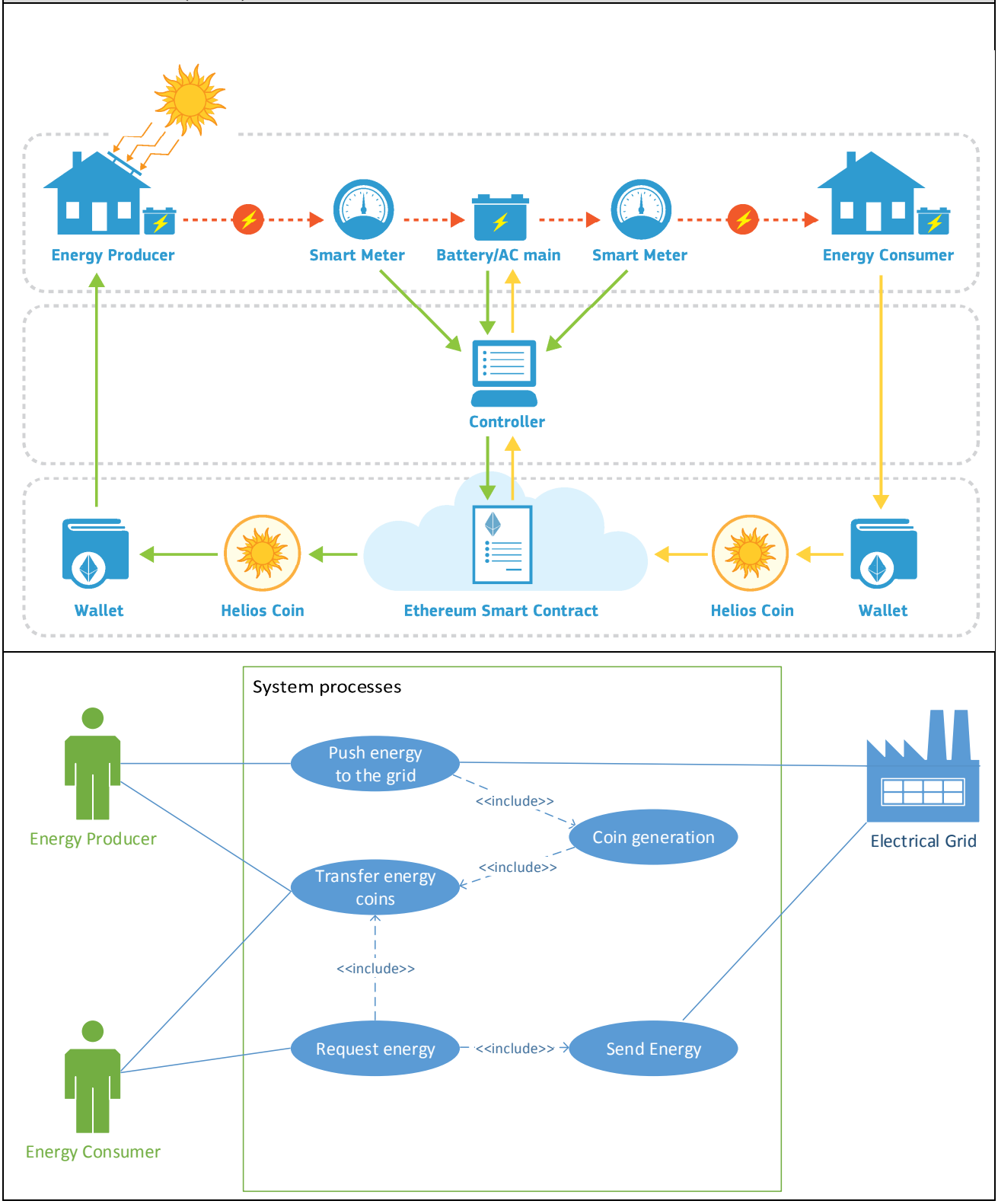
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**

Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	When energy is injected in the grid a smart meter linked to each producer continuously measures how much energy has been injected in total.	
2.	The measurement is sent to the middleware controller which triggers the corresponding smart contract function.	
3	The smart contract function issues the amount of energy coins that correspond to the energy injected. The coins are sent to the energy producer's address	
4	An energy consumer can purchase energy coins from the producer by different means (e.g., Bitcoin, Ether, Euro, etc.)	
5	When a consumer wants to purchase energy, he needs to send energy coins to a predefined smart contract address	
6	Once the coins are received, an event will be broadcasted to the network. Once the controller receives the event it will communicate with the grid and issue a command to release the amount of energy that corresponds to the number of virtual coins received to the consumer.	
7	The smart meter will monitor the energy flow and will stop it once the purchased energy is sent	

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Energy Producer (user)*	The entity that produces energy and pushed it in the grid

Participants and their roles		
Actor	**Type/Role**	**Description**
2	*Energy Consumer (user)*	The entity that buys/consumes energy from the grid
3	*Controller (system)*	Middleware entity that facilitates communication between the user and the smart contract
4	*Smart Contract (system)*	The application logic that enables transactions of virtual energy coins
5	*Electrical Grid (system)*	Physical layer for energy exchange (batteries, smart meters, inverters, etc)

Data and information		
Data	**Type**	**Description**
1	*Helios Coin*	A digital token that can be exchanged for a predefined amount of energy
2	*Energy Measurements*	The energy measurements obtained by the smart meters and transmitted to the smart contract

Security and privacy
The access of energy data should be protected appropriately as they can be used for identifying end users and their activities from their energy consumption. Moreover, as the middleware is a key entity that controls the data input to the smart contract, it should be made sure that it is not manipulated. One way to do so could be to transfer the logic of the middleware to each smart meter, and with the use of a Trusted Platform Module (TPM) or a Trusted Execution Environment (TEE) guarantee that the measurements have not been tampered with.

Main Success Scenario + expected time line

Conditions (pre- or post-)
Pre-conditions We assume the existence of a local grid where energy is produced and consumed in a limited geographical area. The energy producers and consumers should be connected to an blockchain network (e.g., Ethereum). Moreover, the smart meters should be able to communicate with the middleware controller. Post-conditions With the use of the proposed system, energy accountability can be performed and mutual trust on the energy measurements is achieved. The measurements can be audited by any interested party without revealing personal data.

Performance needs

Legal considerations

Risks
The middleware controller needs to be a trusted entity.

Special Requirements

External References and Miscellaneous
Details of this use case can be found in the paper: I. Kounelis, G. Steri, R. Giuliani, D. Geneiatakis, R. Neisse and I. Nai-Fovino, "Fostering consumers' energy market through smart contracts," 2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE), Funchal, Portugal, 2017, pp. 1-6. doi: 10.1109/ES2DE.2017.8015343

Other Notes

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)

P2P Energy Trading

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-002	**Use Case Type:**	*Vertical*
Submission Date:	December 17, 2018	**Is Use Case supporting SDGs**	
Use Case Title:	P2P Energy Trading	**Domain:**	*Industry*
Status of Case	*Proof of Concept (PoC)*	**Sub-Domain**	*Energy*
Contact information of person submitting/ managing the use-case	*Igor Ferreira [FOHAT]* *Chief Executive Officer* *igor.ferreira@fohat.co* *+55 41 9 9101-9222* *https://www.linkedin.com/in/figor*		
Proposing Organization	*FOHAT Corporation*		
Short Description	*Usage of token (NRJ TOKEN) and DLT (EW CHAIN) for energy trading of the Distributed Energy Resources (DERs) inside Blockchain Microgrids.*		
Long description	*By tokenizing the Energy Trading platform (RAPTOR) we will allow Prosumers to trade the energy from their Distributed Energy Resources (DERs) like solar panels, batteries and electrical vehicles in a peer-to-peer transactive network (P2P TE). That will allow people to Bring Your Own Devices (BYOD) into the Microgrids, which promote grid expansion and improves reliability and resilience of the grid network.*		
SDG in Focus (when applicable)	*7-11*		
Value Transfer:	*Tokens*	**Number of Users:**	
Types of Users:	*Energy Traders, Prosumers*		
Stakeholders	*Development Bank, Utility Companies*		
Data:	*=> Shared Data (DLT)* ● *Transaction history for audit purposes;* *=> Use case specific DLT data:* ● *Account;* ● *Token Balance;* ● *Forecasting;* *=> External Data (not stored in DLT):*		

	● *Energy usage inside Microgrid;*
Identification:	*KYC (Know Your Customer) for Energy Traders and Prosumers*
Predicted Outcomes:	The predicted outcomes are: ● Expansion of the Distributed Energy Resources inside Microgrids; ● Transparency of the investments done by Development Bank in the Energy Sector; ● Improved participation of Prosumers in a Free Energy Market;

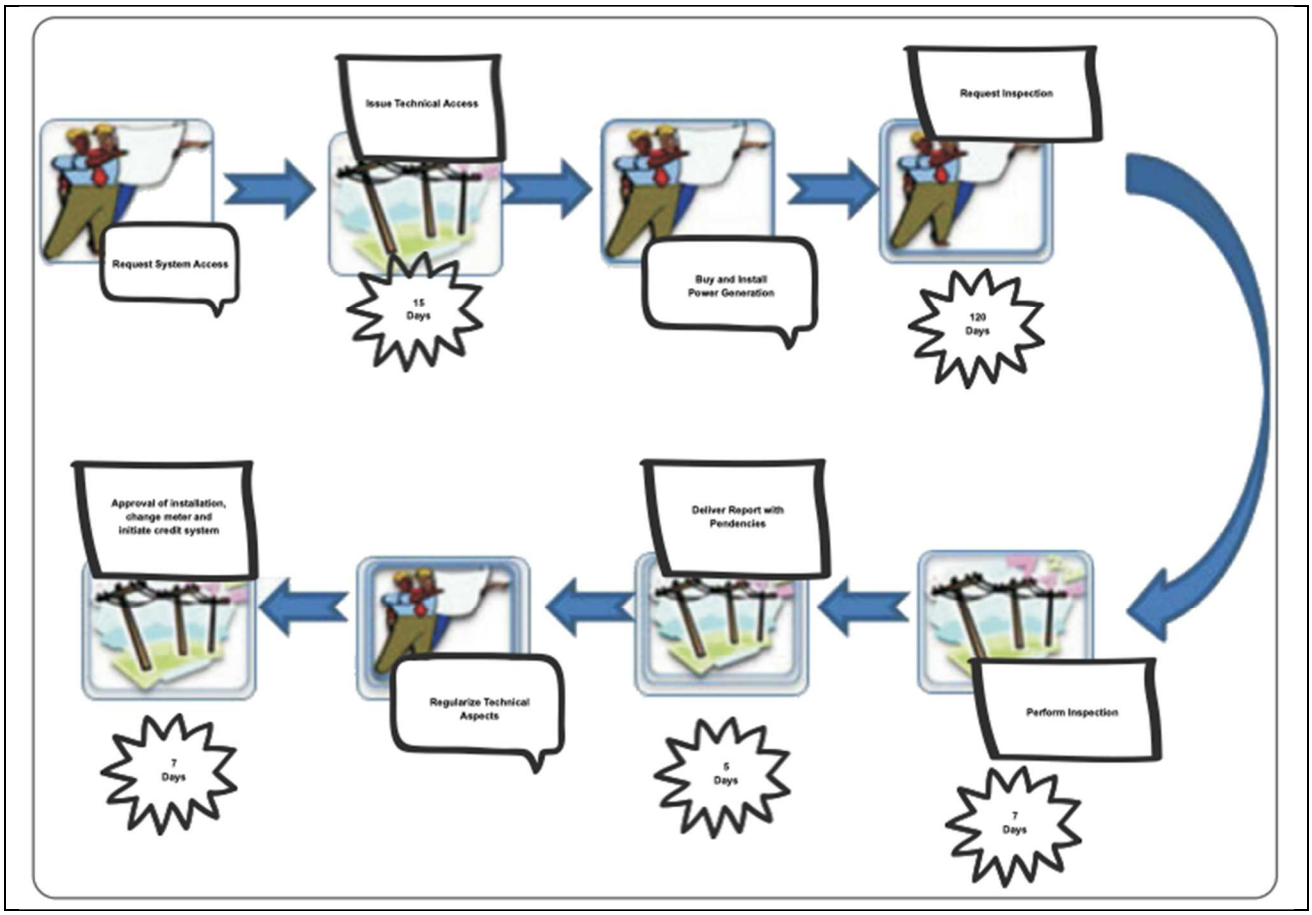
Overview of the Business Problem or Opportunity
The Energy Sector is key for the development of the society and to secure access to a comfortable life for everyone, is a key product/service that support people's life and the country growth. *The world is moving from a Centralized energy generation - based in big power plants - to a more Decentralized energy generation system which improves costs since the energy is produced and consumed closer. A lot of new energy generation is being deployed on solar rooftops, that needs to be integrated in technology arranges called Microgrids, which allows a better way to improve the energy flow and secure a more reliable system that can work both connected or disconnected of the main Grid..*
Why Distributed Ledger Technology?
In the Energy Sector a movement around Decentralization is already happening for power generation, but it's also needed to secure that the Grid is also Distributed when it comes to Operation and Accountability of the energy trading inside over-the-counter (OTC) transactions, DLT technology can scale the energy trading to be performed inside every Microgrid and in between Microgrids, it also allows a new layer of protection against cyber attacks in a infrastructure that is becoming more and more digitized.

Section 2: Current process

Current Solutions
Utility Companies - Distributed Generation Credit System

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	User wants to produce energy by using their Distributed Energy Resources (like solar panels)	Request Utility Company to approve their project to be connected in the Distribution Grid
2.	User starts to produce energy	Utility provides credits

Process scheme (as-is)



Data and information (as-is)		
Data	**Type**	**Description**
1	*Documentation*	*RN 687/2015*

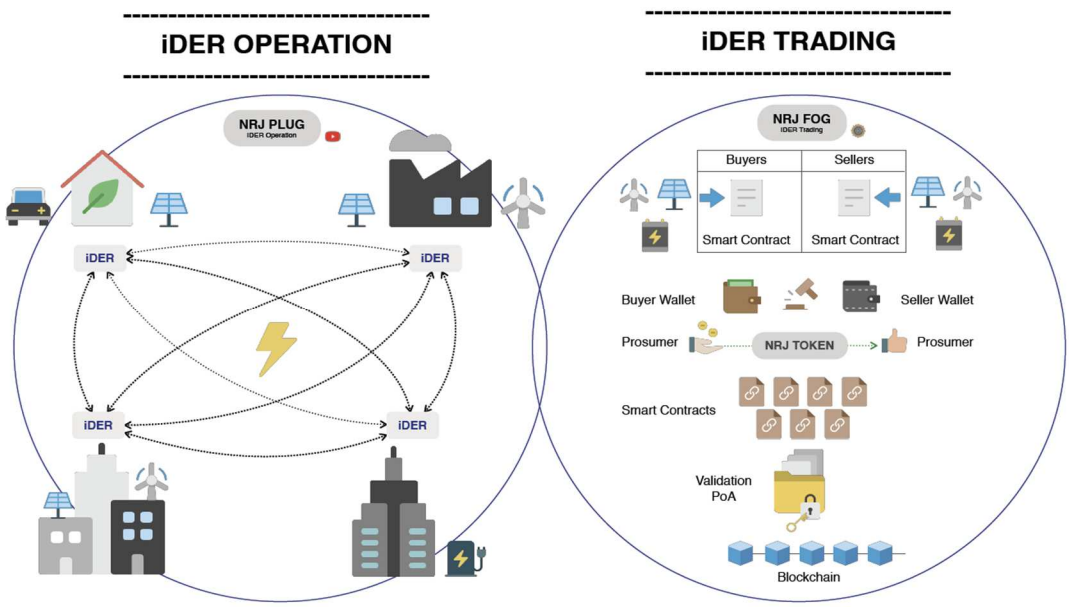
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Users*	*Prosumers (Producer and Consumer)*
2	*Utility*	*Energy distribution and power grant*

Other Notes

Section 3: Expected process

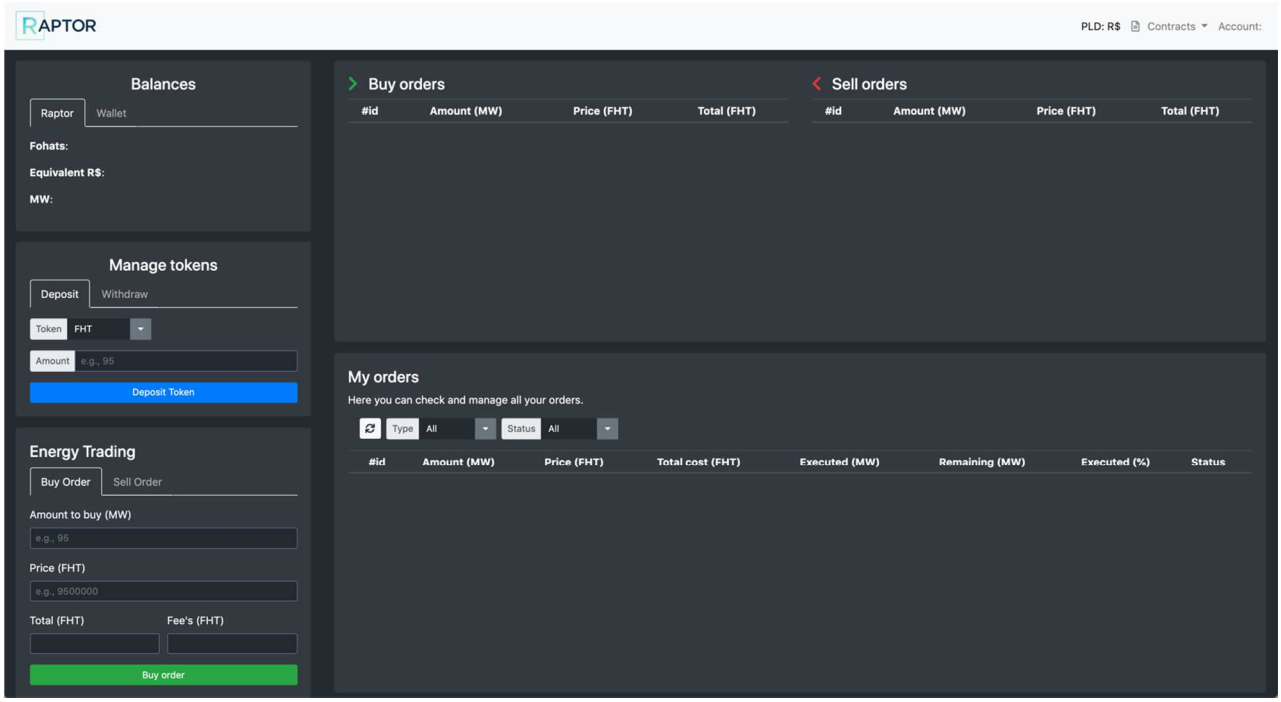
Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	*Prosumers*	*Request access to the Microgrid*
2.	*Utility*	*Provide access to the Microgrid*

Process scheme (to-be)

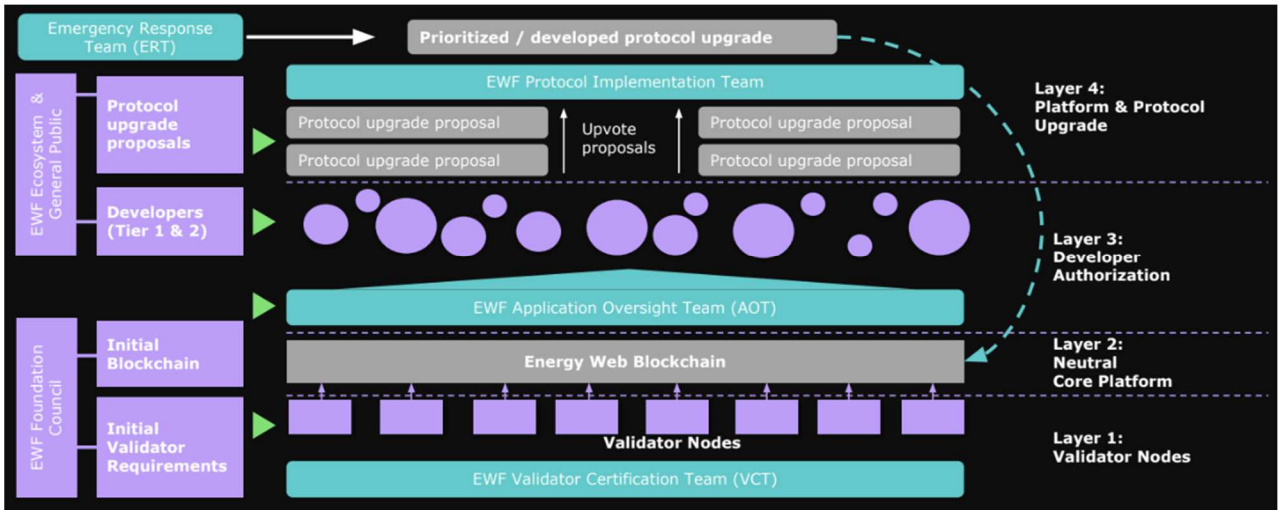


iDER OPERATION (I-GRID)

iDER TRADING (RAPTOR)



EWF Solution

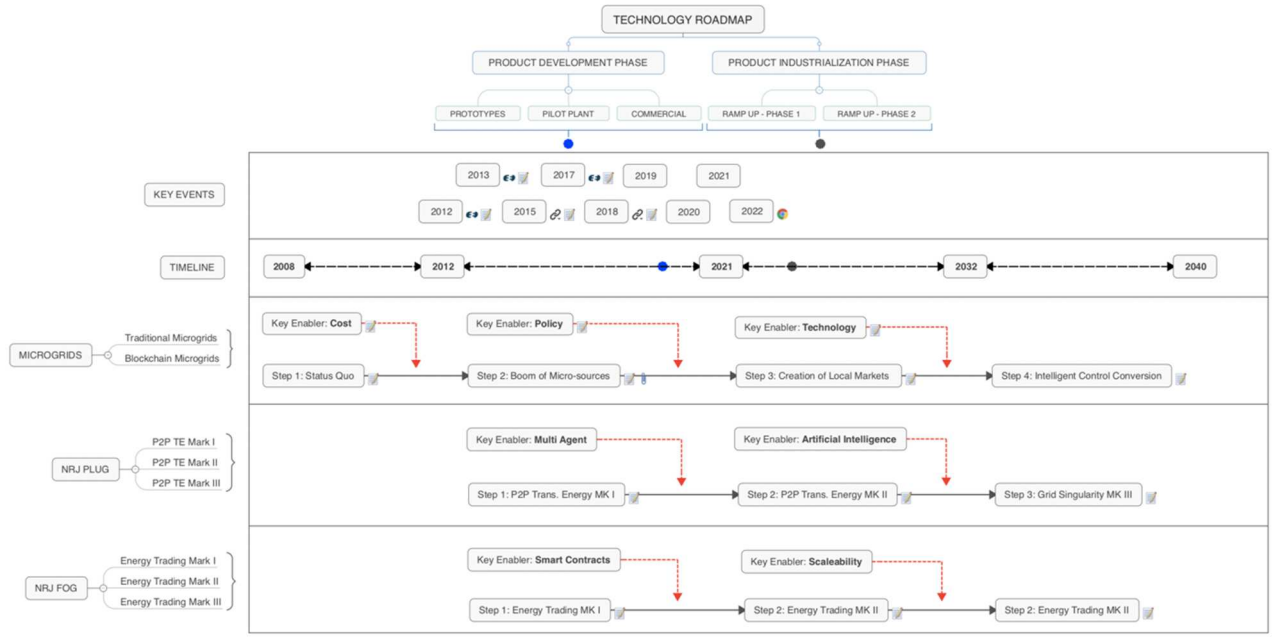


Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Prosumers*	*DER owners*
2	*Energy Retailers*	*Sell excess energy from DER Owners.*

Data and information		
Data	**Type**	**Description**
1	*Documents*	*RN 687/2015*

2	*Smart Contract*	*P2P Energy Trading*

Security and privacy
1.According to EWF Chain solution

Main Success Scenario + expected time line


Conditions (pre- or post-)
1. EWF Chain solution deployed
2. FOHAT I-GRID and RAPTOR solution deployed

Performance needs
1.According to EWF Chain solution

Legal considerations
Different Regulation between countries can offer legal restrictions for operation of a free market

Risks
Regulation

Special Requirements
Standards for communications between different DERs (Distributed Energy Resources) like Open Protocols.

External References and Miscellaneous

https://www.youtube.com/watch?v=PFKMwJL8-RI

Blockchain Solutions for the 3Ds of the Energy Industry

Presented by Jorge Alvarado
Blockchain Architect/Manager at Swisscom Blockchain
20.04.2018

UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE

UNITED NATIONS UNCTAD

Swisscom | Blockchain

Other Notes

N/A

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)

Reverse Logistics Credits

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-003	**Use Case Type:**	*Vertical*
Submission Date:	January 4, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Reverse Logistics Credits	**Domain:**	*3*
Status of Case	*Pilot*	**Sub-Domain**	*g*
Contact information of person submitting/ managing the use-case	*Full Name: Lucas Farias de Moraes Sarmento* *Job Title: COO* *E-mail address: lucas.sarmento@brpolen.com.br* *Telephone number:+55 21 991686899* *Social media: https://www.linkedin.com/in/lucas-farias-de-moraes-sarmento-82206490/* *Web site:* ***www.brpolen.com.br***		
Proposing Organization	*Legal Name: POLEN CONSULTORIA E INTERMEDIACAO DE NEGOCIOS EM SUSTENTABILIDADE LTDA - EPP* Country: Brazil CNPJ: 28.038.406/0001-82		
Short Description	*Post-consumption waste Reverse logistics compensation scheme using DLT as infrastructure to issue Reverse Logistics Credits, which can be used by companies wishing to offset and incentivise the recycling of the waste generated by the consumption of the products they sell to the public.*		
Long description	Companies in Brazil that manufacture packaged goods are required by law to provide proof that a percentage of said packaging is recycled, post-consumption. Also, in Brazil, a crucial part of the reverse logistics chain lies on street waste pickers associations, they collect, sort and sell post-consumption urban solid waste to the recycling industry. In short, waste pickers do the job that these manufacturers were supposed to do. Regulators, auditors and legislators are aware of this scheme and allow for companies to finance the operations of waste pickers associations (proportionally to the amount of waste the association collects and sell) as a way to prove that the packaging of the products they sell to the public is returned to recycling industry, what constitutes basically a credit or offsetting scheme. Currently the scheme works as follows: - Waste Pickers collect, sort and sell post-consumption waste to recycling industry - Packaged goods manufacturers 'buy' the invoices from the		

<table>
<tr><td></td><td>transactions described above from the association paying in the form of improvements in the association's infrastructure and machinery.
- Packaged goods manufacturers use these invoices to prove to authorities that they were financially responsible for the recycling of the post-consumption waste.

The main concern about the current process is that companies are paying for duplicate credits, Reverse Logistics Operators (waste pickers associations and similar organizations) have been selling invoices of the same commercial transaction for more than one packaged goods manufacturer, effectively incurring in 'double-spending' of the Reverse Logistic Credit they generated.

Another concern about the current process is that to rule out any chance of an employment bond between the associations and the manufacturers the waste pickers associations can only receive the payments from the manufacturers in the form of improvements in the association's infrastructure and machinery. Being that most of these waste pickers live in extreme conditions of poverty, their, totally fair, claim is to be able to receive these payments in actual sound money instead of improvements and machinery.

Using a DLT to record, issue and transact those credits solve both above mentioned problems. Double spending is made impossible by the very characteristics of the system and employment bonds between associations and manufacturers will be never be formed because manufacturers will only buy the fungible tokens issued by the smart contract not knowing which association was responsible for the actual process of returning the post-consumption waste to the recycling industry.</td></tr>
<tr><td>SDG in Focus (when applicable)</td><td>GOAL 8: DECENT WORK AND ECONOMIC GROWTH

GOAL 9: INDUSTRY, INNOVATION AND INFRASTRUCTURE

GOAL 12: RESPONSIBLE PRODUCTION AND CONSUMPTION

GOAL 14: LIFE BELOW WATER</td></tr>
<tr><td>Value Transfer:</td><td>Users transact tokens that represent the collection and recycling of 1 ton of post-consumption packaging waste</td><td>Number of Users:</td><td>TBA</td></tr>
<tr><td>Types of Users:</td><td colspan="3">Reverse Logistics Operator (company or association that is responsible for collecting and selling post-consumption packaging waste to the recycling</td></tr>
</table>

	industry) ***Packaged Goods Manufacturers*** *(company that sells packaged goods to the general public and is required by law to provide proof that a percentage of said packaging was recycled)* ***Auditors*** *(Brazilian Government body that is responsible for overseeing the compliance of such legislation)* ***System Operator*** *(company that develops and maintain the online platform and infrastructure where tokens are issued, bought and sold)*
Stakeholders	***General society****: is benefited by the increase in recycling rates and the environmental consequences that come from said increase.* ***Waste Pickers Associations:*** *is benefited by the extra income earned due to the selling of the Reverse Logistics Credits.* ***Packaged Goods Manufacturers:*** *are provided with a simple and secure mechanism to comply with legislation and offset environmental impact of their activities.* ***Government bodies responsible for overseeing compliance of such legislations:*** *are provided with an easy and secure way to audit the compliance of such legislation*
Data:	The DLT will store data about commercial transactions that complete the reverse logistics process (Reverse Logistics Operator selling post-consumption waste to Recycling Industry). Invoices of such transactions officially issued by the Brazilian fiscal authorities will be parsed and tokenized if adherent to the requisites above. The information to be stored is: Seller's CNPJ, Buyer's CNPJ, NCM Code (MERCOSUL common denomination code), amount, type of material transacted, date of issuance.
Identification:	*Identity of participants will be available only for the marketplace provider and government authorities*
Predicted Outcomes:	Increase in packaging recycling rates; increase in Waste Pickers income and overall work conditions; increase in compliance by packaged goods

	manufacturers; decrease in the amount of landfilled recyclable material; decrease in the amount of waste mishandled and wrongly disposed in the environment.

Overview of the Business Problem or Opportunity
Business opportunities lies on the intermediation of the buying and selling of the token, collecting transaction fees for every transaction made on the platform.
Why Distributed Ledger Technology?
Using a DLT to record, issue and transact Reverse Logistics solve the two more sensible problems of this compensation scheme. Double spending is made impossible by the very characteristics of the system and employment bonds between associations and manufacturers will be never be formed because manufacturers will only buy the fungible tokens issued by the smart contract not knowing which association was responsible for the actual process of returning the post-consumption waste to the recycling industry. Also, auditing the system becomes extremely easy due to the immutability and traceability of the transactions recorded on the ledger.

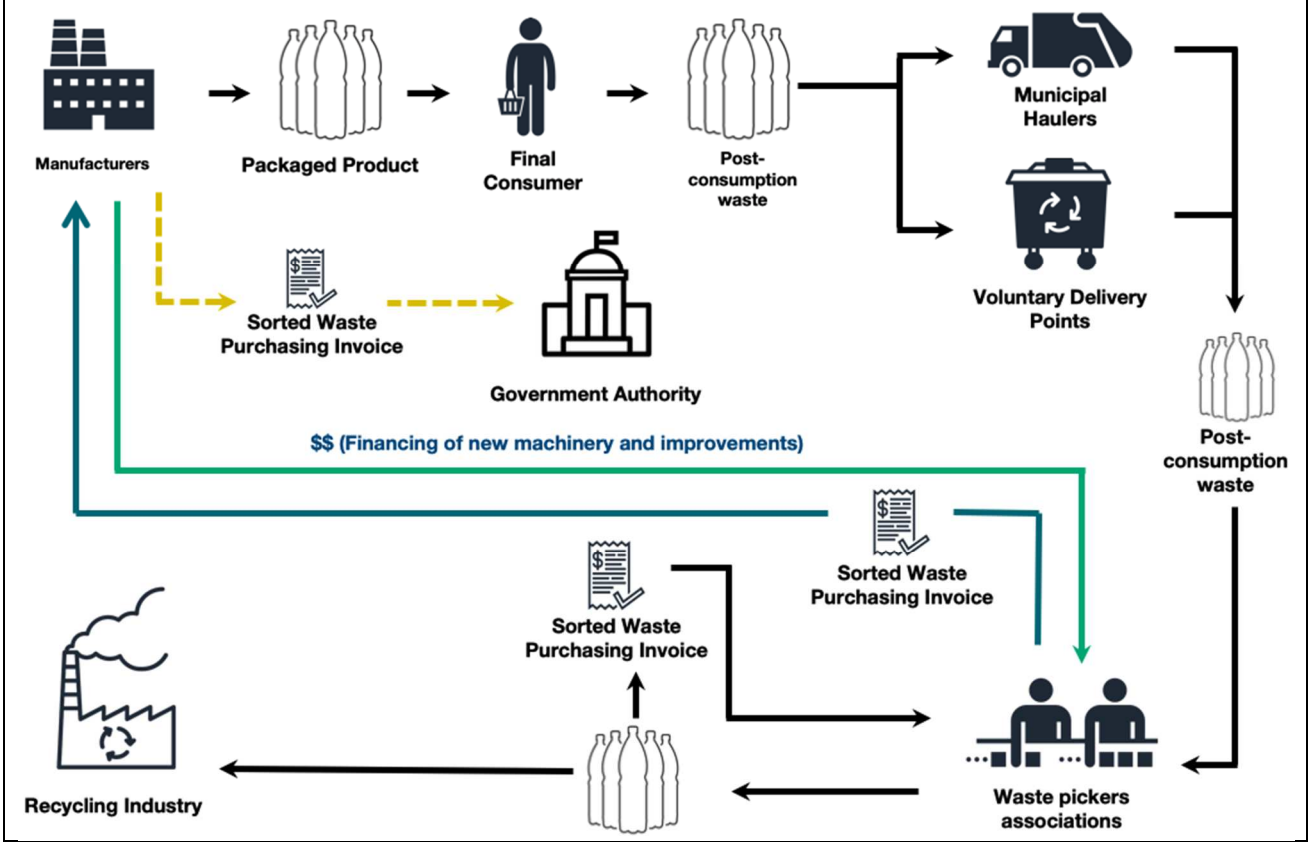
Section 2: Current process

Current Solutions
Current solutions are based on the model mentioned above, with the vulnerabilities mentioned above, on the 'long description' section.

	Existing Flow (as-is)		
	Step	**User Actions**	**System Actions**
	1.	Reverse logistic operator collects, sort and sell post-consumption packaging waste to the recycling industry.	Brazilian fiscal authority keeps a digital version of every invoice issued.
2.		Packaged goods manufacturer contacts Reverse Logistics Operator and buy the invoices of those transactions from them.	System has currently no way of keeping track of these transactions.
3.		Packaged goods manufacturer compensate associations via improvements in infrastructure and machinery.	System has currently no way of keeping track of these transactions.
4.		Packaged goods manufacturers use the bought invoices to prove to the responsible government body	Invoices are handed to the responsible government body in physical form, making it very hard for the auditors to validate the information.

	that they have met the recycling requirements	

Process scheme (as-is)



Data and information (as-is)		
Data	**Type**	**Description**
1	*Invoices*	Invoices issued by the official Brazilian fiscal authority.

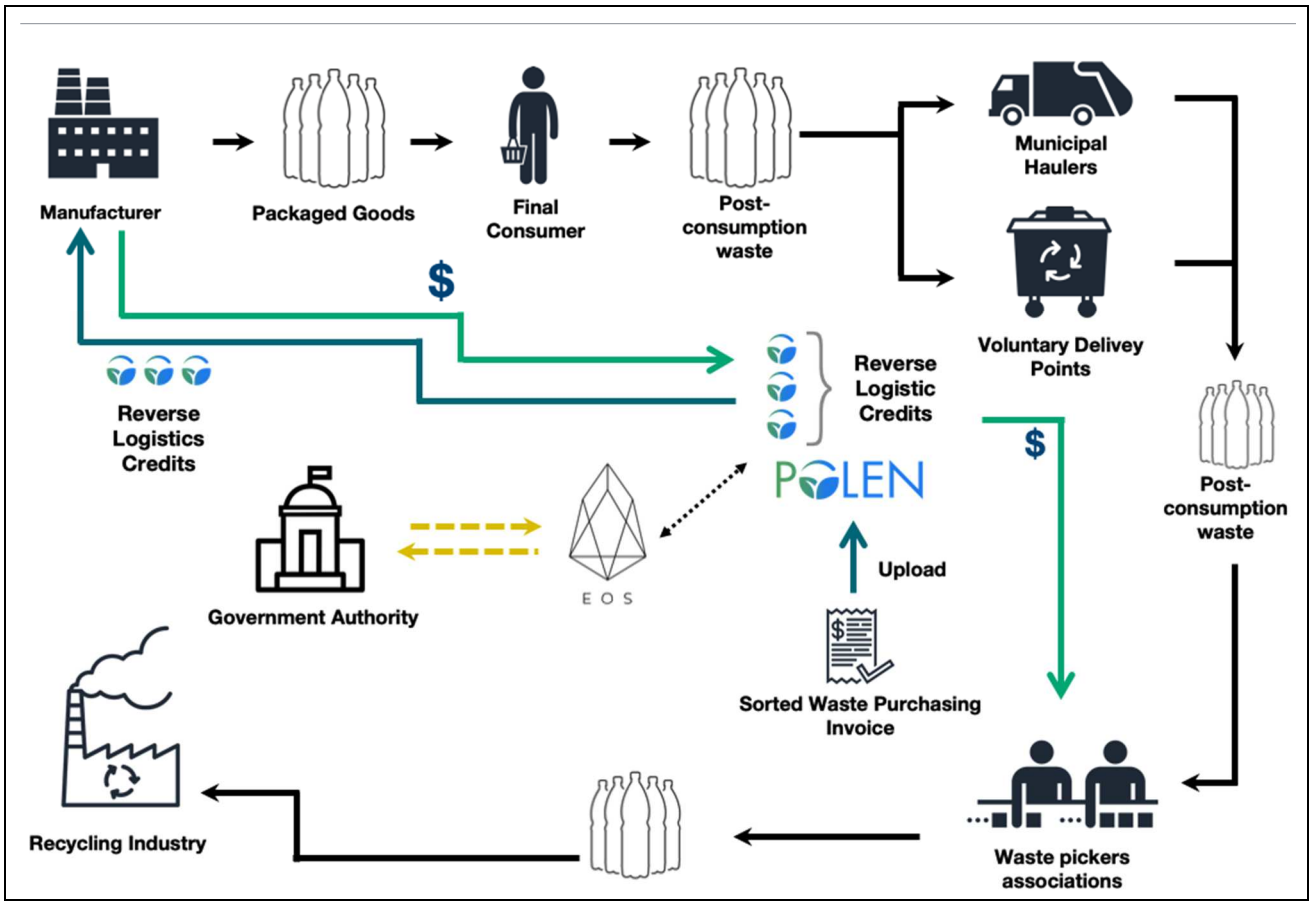
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Packaged good manufacturers*	Buys invoices (representation of a commercial transacation) from waste pickers associations to provide evidence that they have funded the recycling of a certain amount of post-consumption packaging waste.
2	*Reverse Logistic Operators/Waste Pickers Association*	Collect, sort and sell post-consumption packaging waste to the recycling industry & Sell the invoices (representation of the process of returning a certain amount of waste to the recycling industry.
3	*Auditors*	Brazilian Government body that is responsible for overseeing the compliance of such legislation.

Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	**Reverse logistic operator** collects, sort and sell post-consumption packaging waste to the recycling industry.	Brazilian fiscal authority issues and keeps a digital version of every invoice issued.
2.	**Reverse Logistic Operator** and **Packaged Goods Manufacturer** creates an account in the platform providing legal and official information.	System Generates keys pair an assign to user accounts.
3.	**Reverse Logistic Operator** uploads the electronic invoice to the platform	System parse the electronic invoice and feeds a smart contract running on the EOS blockchain with the information of which kinds and how many tokens (Reverse Logistics Credits) are to be issued and transferred to user account.
4.	**Users** transact the tokens between each other accounts in exchange for payments made online.	System records this transactions between users.
5.	**Packaged Goods Manufacturer** 'burn' the tokens under their possession	System records the burning of the tokens and the accounts that did it
6.	**Government Authority**	Audits the system by checking the amount of 'burnt' tokens under each participants accounts and the provenance of these tokens.

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Packaged goods manufacturers*	Buys invoices (representation of a commercial transacation) from waste pickers associations to provide evidence that they have funded the recycling of a certain amount of post-consumption packaging waste.
2	*Reverse Logistic Operators/Waste Pickers Association*	Collect, sort and sell post-consumption packaging waste to the recycling industry & Sell the invoices (representation of the process of returning a certain amount of waste to the recycling industry.
3	*Auditors*	Brazilian Government body that is responsible for overseeing the compliance of such legislation.
4	*System Operator*	Company that builds and operates the online platform where tokens are issued, bought and sold.
5	*Multi-purpose blockchain*	Computer network in charge of maintaining the DLT.

Data and information		
Data	**Type**	**Description**

1	*Electronic Invoices*	Electronic invoices issued by the official Brazilian fiscal authority. Tells the system the amount of each kind of post-consumption waste (plastic, metal, glass or paper) was sold to the recycling industry
2	*User Profile*	User profile on Polen's database for public-key and CNPJ syncing.
3	*Reverse Logistics Credits (cryptographic tokens)*	Digital and unique representation of the process of returning of 1T of packaging material to the recycling industry. Four different kinds of tokens can be issued, one for each category of packaging material (plastic, metal, glass or paper)
4	*'Burnt' tokens balance*	Balance of consumed tokens under each account. This means the token was used by the Packaged Goods Manufacturer as evidence of the reverse logistics process and can no longer be transacted.

Security and privacy
1. *All information on the blockchain is public*

Main Success Scenario + expected time line
The DApp functions are basically: *Register Invoice and mint tokens - The contract owner (can evolve to registered auditors) register a given invoice, for a recyclable waste sold to a registered recycler, generating Reverse Logistics Credit to the seller, and also tokens to buyer and seller for the transaction.* *Trade tokens - Polen tokens are free tradable.* *Certify - tokens can only be certified for a period of time defined according to the legislation. Any wallet is able to certify tokens, this means the token will be foverer frozen on beahalf of a given CNPJ (brazilian company registry)*

Conditions (pre- or post-)
1.

Performance needs
The application will perform according to the Jungle EOS Testnet, and later on to the EOS Main Net, that have proved to be able to process more than 4.000 transactions per second. This will depend on network capacity, usage and staked resources (CPU and bandwidht). The irrevesibility happens when 15/21 BPs build on top of a block, which happens in up to 90 seconds.

Legal considerations
There's no legal barriers to the implementation of such system

Risks
Legal, business and technical risks related to use case

Special Requirements
Business and technical requirements of use case

External References and Miscellaneous
National Solid Waste Policy (Brazil) - http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm Federal Reverse Logistics Obligation Decree - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9177.htm State Level Reverse Logistics Obligation Decree - https://www.legisweb.com.br/legislacao/?id=368998

Other Notes
Any assumptions, issues

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)

Nori Carbon Removal Marketplace

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-004	**Use Case Type:**	Agriculture, Finance, Data Validation
Submission Date:	March 19, 2019	**Is Use Case supporting SDGs**	Yes
Use Case Title:	Nori carbon removal marketplace	**Domain:**	Finance
Status of Case	Pilot	**Sub-Domain**	P2P transactions
Contact information of person submitting/ managing the use-case	Ross Kenyon Lead Strategist ross@nori.com https://nori.com		
Proposing Organization	Nori LLC, Washington, United States		
Short Description	Nori is building a new marketplace to incentivize the removal of carbon dioxide from the atmosphere.		

Long description	Nori is a carbon removal marketplace. We focus exclusively on helping carbon removal practitioners get paid for removing CO_2 from the atmosphere. Existing carbon markets primarily focus on avoided emissions. We have learned a lot from their experience but have made a number of design choices that we believe improves credibility, efficiency, and deservedly treats carbon removal as a discrete activity. Our technology and carbon removal methodologies are open source, and we have open our first pilot project for farmers engaging in regenerative agriculture. As a result of carbon removal's mechanics and the transparency of blockchain accounting, we can far more credibly guarantee that a tonne of carbon dioxide removed and represented by a Carbon Removal Certificate is actually removed. Our NORI token trades at a ratio of 1:1 against the CRC, which will create a market-driven price on carbon for the first time in history, something akin to the Brent Crude or West Texas Intermediate prices used for forecasting in petroleum. A simple and scalable system that allows even small carbon removers to monetize their activity could see the emergence of a trillion dollar carbon removal industry.		
SDG in Focus (when applicable)	#13.1, 13.2, 13.3, 13.A, 13.B		
Value Transfer:	NORI is a token acting as a medium of exchange that will be traded representing the global price for a metric tonne of carbon dioxide removed from the atmosphere. It is traded 1-to-1 for a non-fungible token called a Carbon Removal Certificate (CRC) that is immediately retired upon purchase.	**Number of Users:**	Including employees, those in the pilot, and those at companies we collaborate with, <100. Our ultimate goal is to be "The API for reversing climate change" with billions of users interacting with the system in the backend of everyday transactions.
Types of Users:	Supplier, Buyer, Verifier, Baseline generator, Peer reviewer, Data platform provider, Data manager, CRC aggregator.		

Stakeholders	There are two broad groups of stakeholders: those benefitting from less climate change (or a fully pre-Industrial Revolution climate), and those being paid for carbon removal behaviors. As a result of there being a single market-driven price for carbon removal, this could proportionally benefit the Global South more than those more-developed countries.
Data:	Carbon Removal Certificates will include metadata about who removed the CO2, where it was removed, how it was removed, who verified it, what standards it was verified against, who purchased the CRC, how much they paid.
Identification:	CRCs will be transparent, so the sellers and buyers will be public. Certain data about the carbon removal, such as farming practice data, will be kept confidential.
Predicted Outcomes:	Our goal is to provide the market mechanism for the future trillion dollar carbon removal industry. With a market-driven price on carbon dioxide, and a credible marketplace that is software-driven and scalable, we think this could cause a gold rush into carbon removal technology. At a more basic level, an outcome we expect is that carbon removal will be treated as discrete from offsets, which is crucial for carbon removal to grow into its own dedicated financial infrastructure.

Overview of the Business Problem or Opportunity
There is no marketplace that treats carbon removal as discrete from avoided emissions credit. But they are not the same and should not be treated as such. Additionally, we are past the point where emissions reductions, cap and trade allocations, avoided deforestation credits, and RECs can prevent climate change. With the trajectory we are currently on, we need carbon removal and we need it immediately. By building financial infrastructure that is simple and scalable, and assets that are trustworthy and make a credible impact on climate change, there is a huge opportunity to defuse political fighting over the environment vs. the economy. If people can become wealthy by practicing carbon removal, then we can grow the economy while also reversing climate change. Our approach to this financial infrastructure is software-driven and should be as easy to use as we have come to expect from ecommerce giants like Amazon. Our technology cuts out the large number of middlemen in legacy carbon markets, and can plug into the backend of many other applications through an API.
Why Distributed Ledger Technology?

Trust: The main reason blockchain is needed is for verification of who owns the Carbon Removal Certificate at what time. Public databases can provide transparency, but when you combine the transparency of the public ledger with the verifiability of records that cannot be tampered, corrupted, or bribed via the blockchain, you have something truly unique and valuable.

Provenance:
In carbon markets today, there is rampant double-counting and fraud. Companies routinely count emissions reductions against their carbon emissions after someone in their supply chain has done the same thing.
In the Nori market, there can only ever be one owner at a time of a Carbon Removal Certificate (CRC). Once the supplier sells it to a buyer, it becomes non-transferable, and can never be sold again. No longer can buyers of these certificates claim emissions reductions that were paid for by someone else. Whoever owns the CRC is the entity who can claim publicly that they've been responsible for removing a tonne of CO2.
The same goes for suppliers. It is often the case that suppliers count their projects that reduced carbon emissions for themselves, and then sell offset credit to a buyer who also counts the emissions. In the Nori market, after a supplier sells a CRC, they no longer own it, and cannot claim that they have removed CO2 in their own emissions report.
It would be possible to do this in a centralized database. But that's exactly what the current carbon registries use, and yet somehow the double-counting continues. By building this application on a blockchain, everyone involved can completely trust that there is only one owner of the CRC.

Insurance pooling: Of the 500 million NORI tokens which we plan to mint, they will belong to different categories of stakeholders. The most relevant category here is the insurance pool. In legacy carbon markets, if someone buys certificates that turn out to have released the carbon they attempted to remove or avoid emitting, the buyer would be on the hook for replacing those. We take that risk ourselves. We have an insurance pool set aside of 100 million tokens to replace any invalid CRCs for the benefit of buyers. We are able to build this mechanism into our market because of our control over token supply and its mechanics for the benefit of our users.

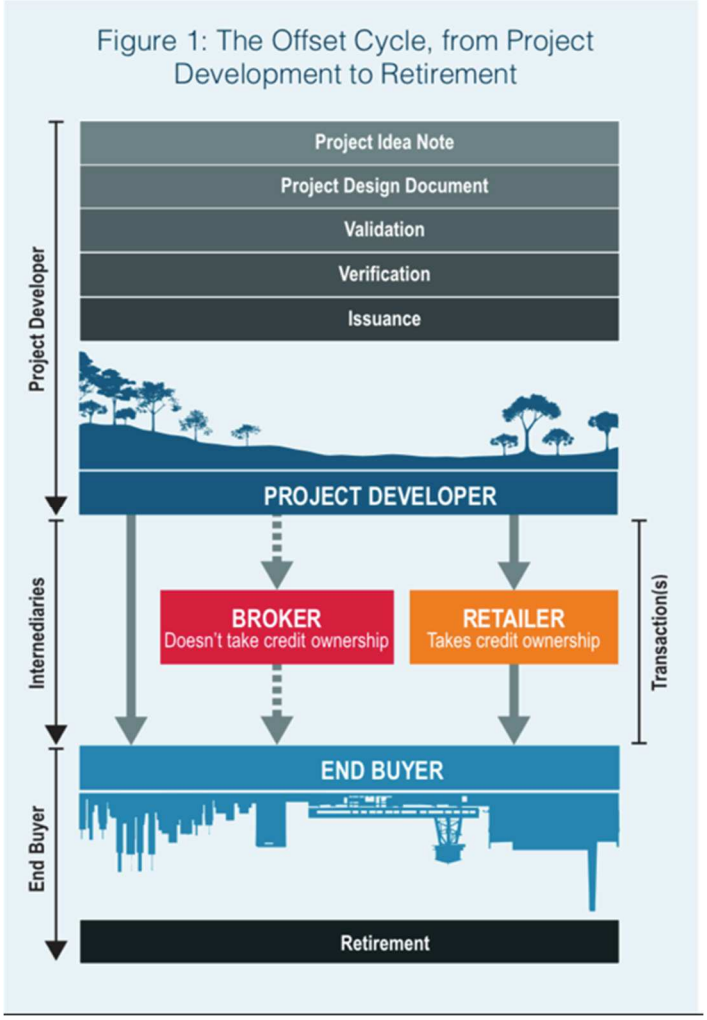
Operating, not Brokering: By using smart contracts, Nori is able to take a role whereby we never actually take ownership of the CRCs. We have developed our own open-source framework for an atomic swap marketplace. This enables the seamless transfer of the CRC for a NORI token between buyer and seller. All without Nori ever touching either asset.
This is partially useful to Nori so that we avoid any regulatory requirements that exist for brokering in a commodity like the CRC. But this is also a benefit to the users of the platform. They can trust—because of the open-source nature of the smart contract—that the exchange of NORI for CRC is truly a bilateral agreement solely between the buyer and supplier.

Immutability, verifiability, and transparency are cornerstone values of what Nori is building.

Section 2: Current process

Current Solutions
There is no focus by legacy carbon markets on carbon removal, nor by other DLT projects, at least that are operational. There is the Ecosystem Services Market Consortium, and Indigo Ag's The Terraton Initiative, that are in development of various approaches to soil carbon sequestration. It probably makes the most sense here to detail the working of legacy offset markets.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**

Process scheme (as-is)


Data and information (as-is)		
Data	**Type**	**Description**
1	Offset protocol	A set of rules and descriptions of what constitutes a specific carbon offset project as well as how it is to be measured and verified.
2	Carbon offset credit	A certificate that purports to represent 1 tonne of CO2-equivalent avoided emissions

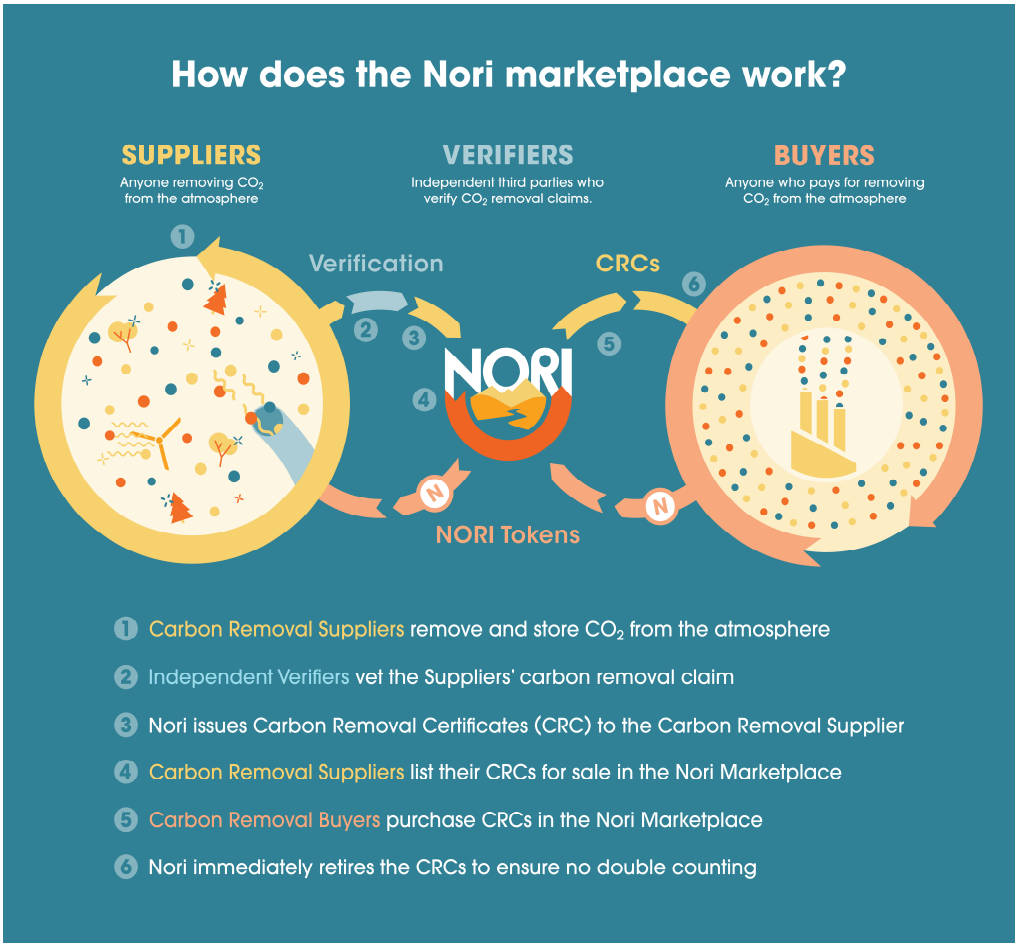
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	Corporate offset buyers	Typically sustainability officers at companies who purchase offset credits to meet voluntary or regulatory offsetting commitments.
2	Project developers	Developers of projects that avoid future GHG emissions.
3	Verifiers	Accredited people/companies who often co-develop a protocol for measuring avoided emissions.
4	Carbon registries	A group that maintains protocols for carbon offsets and lists of issued and sold offset credits.

Other Notes
It can be incredibly expensive for project developers to meet the requirements legacy carbon markets place on them for developing a protocol and paying for the listing and registration fees.

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Supplier removes carbon dioxide from the atmosphere	Supplier is issued unverified Carbon Removal Certificates
2.	Supplier gets carbon removal claim verified	Supplier's unverified CRCs become verified CRCs
3	Supplier lists CRCs for sale	CRC goes for sale
4	Buyer purchases CRCs	CRC changes ownership the Buyer. Supplier receives NORI tokens for CRCs. CRC is immediately retired in the Buyer's account.

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	Suppliers	Suppliers sell CRCs to Buyers in exchange for NORI tokens. It's a way to monetize activities they might already be doing that are continuing to draw incremental CO2 out of the atmosphere, and to inspire new entrepreneurs and businesses to invest in carbon removal. E.g. Farmers, manufacturing companies, mining companies, universities, biofuel producers, technology startups, forest managers, etc.

Participants and their roles		
Actor	**Type/Role**	**Description**
2	Buyers	Buyers use NORI tokens to purchase CRCs, and receive verified certificates that prove carbon dioxide has been removed and stored. They can use these certificates for meeting carbon reduction obligations and for corporate social responsibility reports. E.g. Food producer companies, socially-responsible corporations, events/conferences/festivals, power utilities, local/state governments, individuals, etc.
3	Verifiers	Verifiers of CRCs are independent third-parties in positions of fiduciary responsibility who vet carbon removal claims made by Suppliers, and in turn get new opportunities to expand their professional services businesses through the development of innovative and more accurate methods for verifying CO2 has been removed.
4	Baseline generators	The baseline generator takes in data about cropping and grazing practices. This includes information like what crop was grown, when it was planted, when it was harvested, how the land was tilled, how much fertilizer and lime was applied, and more. The baseline generator uses all this information plus other factors like traditional weather, temperature, and rainfall patterns, and national soil type maps, to model expected practice-driven changes in terrestrial organic and mineralized carbon stocks. Nori's first baseline generator is COMET-Farm, based in the NREL Laboratory at Colorado State University. Nori will add new baseline generators as they become known to us.
5	Peer reviewers	Similar to peer review committees for academic journals, peer reviewers are a collection of scientists, policy advisors, and industry experts who independently review, improve, and approve the Nori methodologies for measuring and verifying removed CO2.

Participants and their roles		
Actor	**Type/Role**	**Description**
6	Data platform providers	Providers of some form of software platform used to collect and store data that will make it easier for farmers to monitor soil health and participate in the Nori marketplace. Integration between these data platforms and Nori makes it easy for farmers to cost-effectively organize and transfer the data they need to supply to get paid for increasing carbon content in soils and drawing down atmospheric CO2.
7	Data managers	Entities that directly help growers manage and interpret their data, register projects in the Nori marketplace, and submit carbon removal claims. Data managers act like independent consultants to farmers. Most data managers operate data platforms, but not all data platform operators provide data management and interpretation services to their platform users.
8	CRC aggregators	Entities that have been assigned ownership of and the right to manage a portfolio of CRC-generating projects on behalf of farmers.

Data and information		
Data	**Type**	**Description**
1	Cropping practice data	Farmers provide cropping practice data to Nori that gets run through the COMET-Farm model. This data remains private and confidential to the farmer.
2	Carbon Removal Certificate	Each CRC will be a non-fungible token that includes such metadata as who removed the CO2, where it happened, how it was verified and by whom, etc.
3	Buyer dashboard	Each Buyer will have a public dashboard that displays information about the CRCs they've bought, where users can then trace back all the information about the CRC.

Data and information		
Data	**Type**	**Description**
4	CRC purchase data	Every CRC purchase will take place on-chain. Volume and price bid data from our forward contract auctions will be published publicly.

Security and privacy
It is important to farmers that their cropping practice data remain private, as that is effectively their trade secrets. Metadata about the CRC will all be public.

Main Success Scenario + expected time line
We project launching our market in late 2019 with 1–2 million CRCs available for sale. Success entails buyers purchasing CRCs at high enough price levels that more farmers are incentivized to continue registering their projects in the Nori marketplace. Long term, Nori's goal is for the NORI token to become a reference price for CO2 removal. We want to see the value of what buyers are willing to pay for carbon removal increase so that more and more entrepreneurs, farmers, businesses, and researchers invest time and money in increasing carbon removal capabilities, beyond soil sequestration which is Nori's starting point.

Conditions (pre- or post-)

Performance needs
On-chain transactions will occur infrequently. In a future state of many sensors reporting into the platform carbon removal activity, we will offload that onto a side chain application.

Legal considerations
For each issue, please describe the name of the legal act containing the identified barrier, what is the negative impact and a proposal to overcome this negative impact. 1. The US SEC has issued some dictum for how cryptocurrencies will be treated, but it is an ongoing process. We have made modifications to our token design to be more compliant with existing regulations. 2. The international community is currently debating new reporting standards and frameworks for international carbon trading. We are forming an exploratory group called Carbon Removal Action Group (CRAG) so that interested parties who wish to see carbon removal treated as distinctly different from carbon offsets have a more unified voice in international climate and policy discussions.

Risks
Legal risk: It is unclear if and how regulation surrounding digital assets will evolve, in their operational elements or financial categorization. Business risk: It is possible that a different platform supersedes us in some way. Or that national or international policy will recognize carbon removal and assets representing it in a way which disfavors or excludes Nori from participation. Technical risk: Beyond the risks basic to software companies, there is a dependency upon the Ethereum blockchain and its continued growth, robustness, and security.

Special Requirements

External References and Miscellaneous
Nori white paper: https://nori.com/white-paper Nori blog: https://nori.com/blog

Other Notes
Nori’s source of revenue is in a small transaction fee charged to the Buyer. We will not be charging listing or registration fees to the Suppliers.

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes

b. Government and non-profit transparency

c. Legislation, compliance & regulatory oversight

d. Voting

e. Taxation and customs

f. Intellectual property management

g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things
4. Data processing, storage and management
    a. Data Validation (includes provenance)

Pig farm monitoring & data traceability

Section 1 Summary

Use Case Summary			
Use Case ID:	IND-005	**Use Case Type:**	Vertical
Submission Date:	October 11, 2018	**Is Use Case supporting SDGs**	Yes
Use Case Title:	Pig farm monitoring & data traceability	**Domain:**	Agriculture
Status of Case	Pilot	**Sub-Domain**	Food traceability
Contact information of person submitting/ managing the use-case	Full Name: Hui Ding Job Title: Co-Founder, COO E-mail address: hui.ding@chaincomp.net Telephone number: 86-18311280681 Web site: www.chaincomp.net		
Proposing Organization	Chaincomp Technologies Co., Ltd., China Shenqiao Technologies Co., Ltd., Henan, China		
Short Description	Blockchain-based trusted data storage and dissemination among stakeholders in the meat industry, combined with IoT-based effective and complete pig farming monitoring and data collection enables efficient data sharing and promote food safety and quality.		
Long description	Currently, small to medium size pig farms (around 500 pigs per farm), which provide over 50% of total pigs (693.82 million in 2018) in China, cannot provide trusted data collection and traceability and gives chances to food safety hazards that happened in recent years. Our use case provides Blockchain-based IoT solution to pig farms and realizes: 1) IoT-based effective and complete pig farm monitoring and data collection; 2) Blockchain-based data storage and dissemination. The system can automatically record the environmental, physiological and feeding data and enables efficient and trusted data storage and sharing among stakeholders. After deployment of such system, a number of benefits can be achieved, such as 1) government inspector can access tamper-proof data to evaluate the farms and the quality of the meat; 2) consumers will be able to access the details of his/her purchase and be assured of food safety and quality; 3) furthermore, it enables lower cost of business operation: farms, feed/drug sellers, insurance providers can share information via DLT to perform transactions in lower cost.		
SDG in Focus (when applicable)	9 – Industry, Innovation and Infrastructure 9-1 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic		

	development and human well-being, with a focus on affordable and equitable access for all		
Value Transfer:	NA	**Number of Users:**	Thousands+
Types of Users:	farm owner, feed/veterinary drugs seller, insurance provider, logistics, government inspector, meat distributor, retailer, etc.		
Stakeholders	farm owner, feed/veterinary drugs seller, insurance provider, government inspector, meat distributor, meat retailer, consumer, etc.		
Data:	Massive amount of data is collected via sensors and devices every day from every animal in the farm, which makes it inefficient to store on DLT. In our system, such data are encrypted and stored in distributed file system, only the hash of a data unit is stored in DLT. The data unit is decided by data types and sampling frequency, e.g. the feeding data and environmental data in 24 hours.		
Identification:	Each pig, feeding device, sensor, farm site is uniquely identified and related data are collected and recorded. Anonymity is not required.		
Predicted Outcomes:	- Safe and high-quality meat production; - Efficient pig farming business by sharing animal data with feed/drug sellers, insurance providers, meat distributors and retailers.		

Overview of the Business Problem or Opportunity

Chinese people consume 55.9 million ton of pig meat in 2018, which constitutes nearly half of the pig meat consumption of the world [1]. However, current large-scale pig farming industry cannot provide trusted data collection and traceability in different stages of the process including farming, inspection, transportation, distribution to consumer. Hence, the safety and quality of pig meat is one of the most important unresolved food issues in China.

Business Problem:

- Safe and high-quality meat product is highly demanded;
- Efficient pig farming business by sharing pig data with feed/drug sellers, insurance providers.

Opportunities:

- IoT-based effective and complete pig farming monitoring and data collection can automatically record the environmental, physiological and feeding data;
- Blockchain-based trusted data storage and dissemination among stakeholders;
- Data close to pigs has great value in ensuring food safety and preventing fraud in logistics and sales process. Lack of such data will result in the lack of the most important source data for farm-oriented monitoring.

Why Distributed Ledger Technology?

- The distributed ledger technology will enable trusted data storage and dissemination among untrusted stakeholders and reduce the chance of data manipulation.

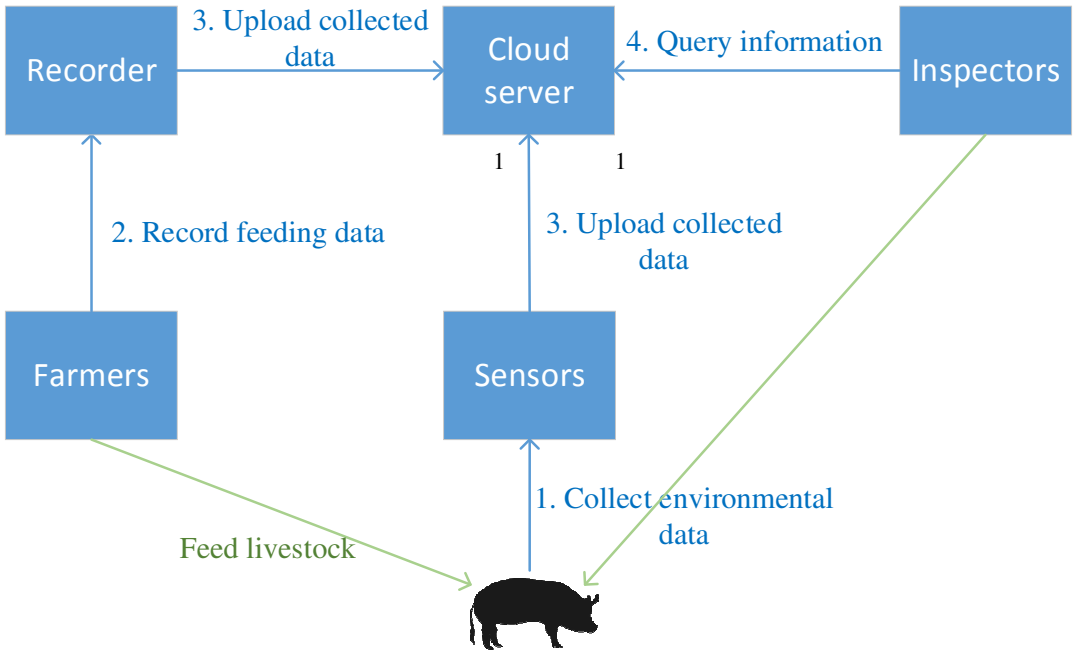
- Inspector can access tamper-proof data to evaluate the farm and the quality of the pig meat;
- Consumers will be able to access the details of his purchase be assured of food safety and quality.
- Lower cost meat feeding business operation: farms, feed/drug sellers, insurance providers can share information via DLT to perform transactions in lower cost.

Section 2 Current process

Current Solutions
Current system monitors the feeding, living environment of pigs. - Feeding system usually includes RFID ear tags for pigs and RFID reader on feeding devices. The reader identifies a pig by its tag and determines whether one pig has eaten to avoid excess feeding. - Temperature, humidity and light data in the breeding house are collected by sensors to monitor the living environment of the pigs so as to avoid diseases. However, current system doesn't obtain detailed information such as specific types of feed intake and physiological data of pigs. Furthermore, the authenticity of information is not trustworthy because sensing data is collected in the farm's own network and directly uploads to the its own private cloud. Data can be manipulated by certain party during the collection and storage process, making it difficult for government inspector and consumers to obtain the real information.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	Collect environmental data	Sensors collect environmental information of pig houses.
2.	Record feeding data	System checks RFID tags of pigs and prompt if they are fed repeatedly for the farmers. Record feeding information input by farmers, and store them in local storage temporarily.
3	Upload collected data	Sensors send collected environmental data and feeding data, and send stored records to private cloud servers respectively, and store them in the cloud.
4	Query information	System requests access permissions to the cloud, and then query for the required information when authorized.

Process scheme (as-is)



Data and information (as-is)		
Data	**Type**	**Description**
1	Identification	It includes the identity information of the pig, specifically, the RFID of the pig, is implemented on ear tags.
2	Environmental data	It includes the environmental status data of pig houses, such as temperature, humidity, and lighting.
3	Feeding data	It includes the pig feeding records, such as feeding amount, time, feeding frequencies and so on.

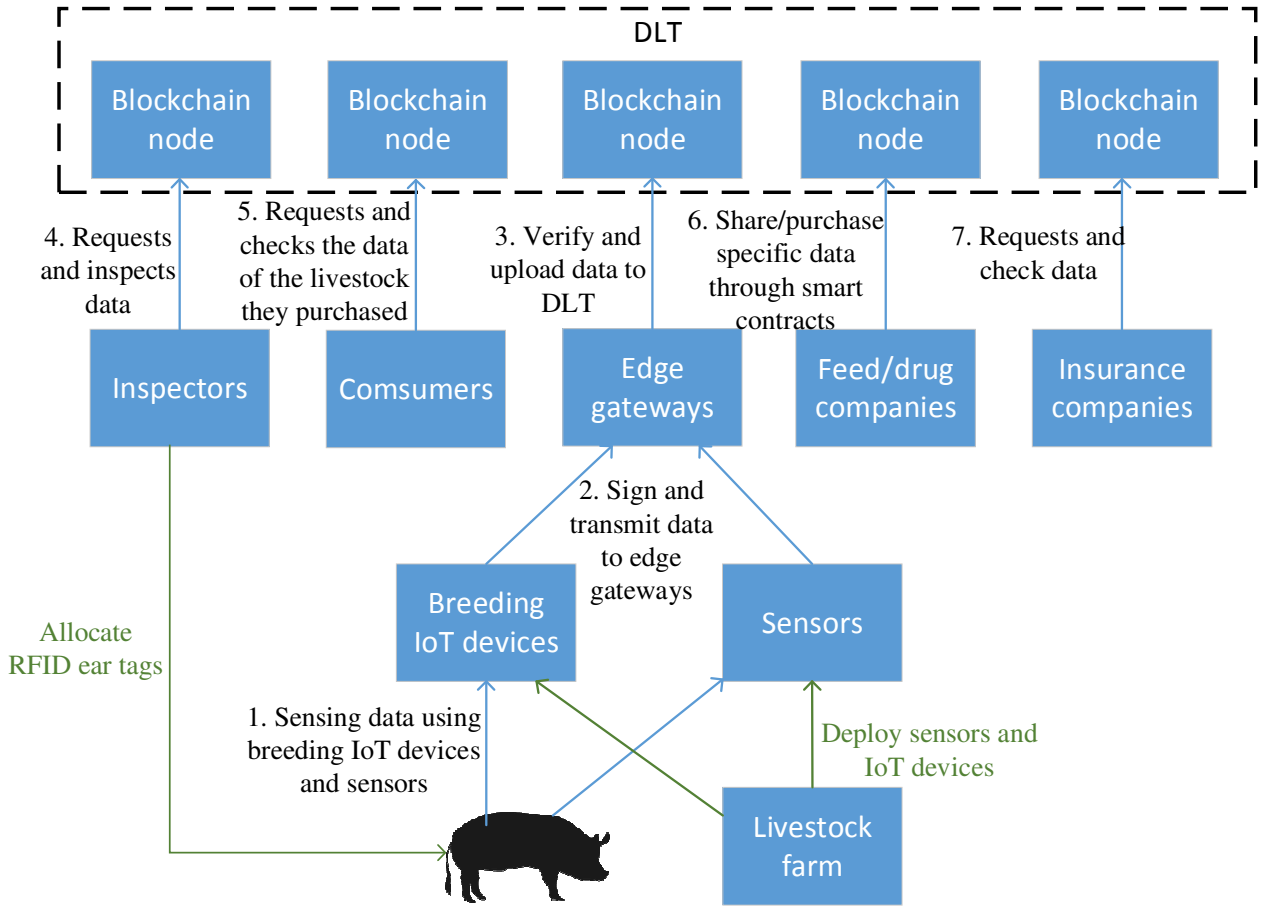
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	Pig farm manager	Deploy sensors in pig farm; tag pigs; construct data collecting systems; collect and manage data in private clouds; authorize access to the cloud; employ pig farmers.
2	Pig farmers	Feed pigs; record feeding information.
3	Inspectors	Allocate RFID ear tags, access and analyze feeding data as well as environmental data to inspect farming processes.

Other Notes

Section 3 Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Sensing data using breeding IoT devices and sensors	Collect environmental, feeding and pig's physiological information through sensors and RFID reader in the breeding house, including pig identity, temperature, humidity, ammonia gas, hydrogen sulphide gas, light, feeding status, body mass and etc.
2.	Sign and transmit data from IoT devices to edge gateway	Data collected by IoT devices are signed by the devices and then transmitted to edge gateway.
3	Edge gateway verifies and uploads the data to distributed ledger	Edge gateway verifies the authenticity of the data and encrypts data using its private key and then uploads the encrypted data to distributed ledger.
4	Inspector requests and inspects data	Government inspector may request and inspect certain data to check the safety and feeding conditions of all pigs in their jurisdiction. Inspector decrypts the data using public keys of the encryption gateway.
5	Consumer requests and checks the data of the pig they purchased	Consumers can request and check the data of the pig they purchased. These consumers include downstream slaughterhouses, food companies, restaurants and meat consumers.
6	Feed and drug companies share/purchases specific data through smart contracts	Feed and drug companies can share/purchase specific data through smart contracts.
7	The insurance company requests and checks the data	The insurance company can request and check the data of a pig farm to determine the insurance pricing.

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	Pig farm	Feed pigs; deploy environmental sensors, RFID readers, and breeding IoT devices; collect breeding data and then upload the collected data to distributed ledger; deploy edge gateways and data collecting systems; authorize data users to access the uploaded data.
2	Consumer	Include downstream slaughterhouses, food companies, restaurants and meat consumers. They purchase pig products or meat products. They can traceback the breeding data corresponding to the products they purchased.
3	Insurance company	Request and analyze the breeding data of a pig farm; determine the insurance price for that farm.
4	Feed/drug seller	Purchase specific breeding data from pig farms through smart contracts; adjust their production plans through analyzing the acquired data.
5	Inspector	Request and inspect breeding data of pig farms to regulate their breeding processes.

Data and information		
Data	**Type**	**Description**
1	Identification	It includes the identity information of pigs, specifically, the RFID of a pig, can be implemented on ear tags.
2	Environmental information	It includes the environmental status data of pig farms, such as temperature, humidity, ammonia gas, hydrogen sulphide gas, light and etc.
3	Feeding information	It includes the pig feeding records, such as feeding amount, feeding time, feeding frequencies and so on.
4	Pig's physiological information	It includes body mass of pigs, especially the weights varieties after each feeding.

Security and privacy

1. Sensors and feeding devices sign the data they generated using their private keys.
2. Original data are encrypted using owner's private keys. Corresponding public keys are provided by the farms to inspectors for data decryption.
3. Data are stored in a distributed file system.

Main Success Scenario

- Safe meat production: Record production-side data through the temper-proof nature of the distributed ledger, which covers the daily status of the pig and accurately reflects their health, thus making meat safety completely transparent to inspectors and downstream consumers.

- High quality meat production: Due to the temper-proof nature of distributed ledger, a farm can prove that it spends more time feeding a healthier pigs, which can give its products a high premium.

- Efficient pig farming and insurance by sharing pig data with feed, drug and insurance companies can be achieved by distributed ledger and smart contract.

Conditions (pre- or post-)

NA

Performance needs

1. Performance requirements for sensing data collection and uploading at edge gateway:

The edge gateway will obtain the sensing data from multiple subordinate IoT devices. In our system, each environmental sensor generates 20 bytes data per second, and one feeding device and physiologically sensing module produce approximately 30 bytes data per second. A medium-sized pig house requires approximately two environmental sensing devices and ten feeding devices, so that an edge gateway which covers only one pig house requires about 340 bytes per second.

2. Performance requirements for TPS of DLT system:

The demand for TPS is directly related to the amount of data. Regardless of storing data directly in the chain or in a distributed file system, some data need to be updated in the distributed ledger, so certain TPS is required for data submission and synchronization. A medium-sized pig farm in China usually holds 2000-5000 pigs. If one data unit is generated and stored for each pig, and the data is submitted every 24 hours, then a medium farm's demands is 0.02-0.06 TPS. When the data uploading frequency increases and the number of farms increases, such demands also increase. For example, 10000 pig farms require 200-600 TPS when they upload data daily.

3. Performance requirements for distributed data storing:

The edge gateway uploads data to a distributed ledger node for data packaging periodically. Data can be selected to store in a distributed file system, such as IPFS, rather than all data on ledge; so that the on-chain-data can only be the hash identifier to the data stored in IPFS. This reduces the space requirements for storage on the chain, but distributed storage needs to achieve a certain efficiency to meet the performance requirements of consumer when accessing.

Legal considerations

Risks

Special Requirements

External References and Miscellaneous

Other Notes

[1] https://gain.fas.usda.gov/Recent%20GAIN%20Publications/Livestock%20and%20Products%20Semi-annual_Beijing_China%20-%20Peoples%20Republic%20of_3-12-2019.pdf

Responsible Gold Ecosystem

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-006	**Use Case Type:**	***Vertical***
Submission Date:	May 28, 2019	**Is Use Case supporting SDGs**	***Yes***
Use Case Title:	Responsible Gold Ecosystem	**Domain:**	*www.responsiblegold.com*
Status of Case	***Implementation /*** *(Live in production)*	**Sub-Domain**	
Contact information of person submitting/ managing the use-case	Victor Vilmont VP Innovation and Product Management https://www.linkedin.com/in/victorvilmont/ Email: victor.vilmont@emergenttech.com Tel: +1 415 278 1100 Stephen Grinalds VP Engineering R&D https://www.linkedin.com/in/stephengrinalds/ Email: stephen.grinalds@emergenttech.com Tel : +1 408 669 2104 Kevin Cussen Senior Technical Product Manager - Responsible Gold Ecosystem https://www.linkedin.com/in/kevin-cussen-a4524917/ Email: kevin.cussen@emergenttech.com Tel: +1 206 604 4209 Web: www.emergenttechnology.com		
Proposing Organization	**Emergent Technology Holdings (EmTech)** EmTech is a global technology company that specializes in fintech and regtech innovation. EmTech's business units encompass payments, identity, and distributed ledger technology (DLT) solutions. The Company's DLT expertise allows for comprehensive identity and authentication management, regulatory compliance, supply chain provenance tracking, title transfer solutions, and efficient payments and remittance. Headquartered in Silicon Valley, EmTech operates in more than 70 high-growth markets across Asia-Pacific, Latin America, Africa, and the Middle East.		
Short Description	Gold due to its intrinsic nature is susceptible to money laundering, conflict sourcing, and financing of terrorist activities. There is increasing pressure on supply chain participants to demonstrate that their production practices do not contribute to conflict or any environmental, health and safety concerns.		

	EmTech's Responsible Gold Ecosystem ("Ecosystem") provides a much-needed solution to the increasing transparency and trust burden. The Ecosystem helps enhance integrity in the global gold supply chain by using DLT to irrefutably and immutably record ethical provenance and chain of custody from mine, to refinery, to vault or fabricator. It is underpinned by EmTech's Responsible Gold Standards, a set of critical environmental, social and governance (ESG) risks and controls for the precious metals industry. The Standards provide a framework by which participants can attest that their gold production practices adhere to the highest industry requirements, manage their impacts on workers, communities and the natural environment, and generate positive ESG impacts. EmTech is committed to sustainable development by: ● Supporting participants in embedding responsible business practices; ● Connecting responsible companies and people in one Ecosystem; and ● Trading Responsible Gold
Long description	Gold has long presented opportunities for bad actors to take advantage of its complex and lucrative supply chain. Examples of illicit activities presented below make news headlines regularly due to the absence of appropriate organizational controls: ● Classified as a "conflict mineral," proceeds from gold mining and trading perpetuate armed conflict, violence, and human rights abuse in politically unstable areas, and support corruption and money laundering. ● Producers in disadvantaged regions pour mercury into rivers to extract underlying gold inexpensively, creating irreparable environmental damage and introducing catastrophic health risks to workers and neighboring communities. ● Workers, including minors, work in confined spaces and unstable mineshafts, risking death from explosions, tunnel collapse, or exposure to toxic fumes. Despite regulations and international standards to manage these risks, illicit activities persist. EmTech developed the Responsible Gold Ecosystem to ensure that gold can be quickly and irrefutably proven to be responsibly sourced. The Responsible Gold Supply Chain Application (RG SCA) automates key parts of the responsible sourcing compliance process and helps Ecosystem participants obtain relevant and accurate transaction data for the transfer of gold across the supply chain, from the moment a bar of doré is packaged at a mine, all the way to bullion in a vault. The RG SCA is underpinned by EmTech's Responsible Gold Standards ("The Standards"), which are based on existing environmental, social and governance ("ESG") standards for the precious metals industry. The Standards set the conditions of participation in the Responsible Gold Ecosystem. They provide the framework by which a gold supply chain and its associated outputs are measured, and can be affirmatively declared "Responsible Gold." The Standards help ensure that gold in the Ecosystem:

	● Does not cause or contribute to infringements of internationally-recognized human rights; ● Is not susceptible to money laundering and financing of conflict and terrorist activities; ● Does not contribute to unacceptable health, safety and labor conditions for workers; and ● Minimizes the impact of gold mining and refinement on the natural environment and surrounding communities The Standards incorporate requirements not only for miners and refiners but also for logistics providers and vault operators to bolster the ESG profile of the entire gold supply chain. The Responsible Gold Ecosystem uses a combination of hardware and software to automatically: ● Record the provenance of independently certified, responsibly mined gold ● Track the custody of gold throughout the supply chain, from mine, to refinery, to vault ● Track the custody of gold grain beyond refineries and on to jewelers and manufacturers ● Present data for ongoing analysis and analytics by both human and AI auditors to identify red flags in real time. Responsible Gold, defined as gold that has traversed through our system, can now be traced back to its origin, giving regulators, investors, fabricators, and consumers confidence that it has been responsibly sourced. EmTech leverages a consortium DLT supported by a distributed set of independent node operators. DLT allows for these records to be immutable and irrefutable. It ensures the process is fully transparent and auditable, eliminating the possibility of bad actors altering records at any time.
SDG in Focus (when applicable)	EmTech is committed to helping enhance the integrity of the gold industry by using DLT to facilitate the creation of Responsible Gold, generate positive and sustainable impact, and contribute to the UN's "Transforming our World" 2030 agenda. The primary focus of our business is on the following SDGs: **12: Responsible consumption and production.** The Responsible Gold Standards were developed to document best practices in responsible sourcing and as a tool to support participants in enhancing their ESG practices. This mission contributes to target "12.6: Encourage companies, especially large and transnational companies, to adopt sustainable practice." **16. Peace, justice and strong institutions**. The Responsible Gold Ecosystem tracks provenance and the transfer of custody of responsibly sourced gold through the supply chain. This application contributes to target "**16.4:** By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime."

<table>
<tr><td></td><td colspan="3">Furthermore, the Responsible Gold Standards incorporate a number of the SDGs, as follows, assisting businesses participating in the Responsible Gold Ecosystem to make contributions to sustainable development:

#3. Good health and wellbeing
#5. Gender equality
#6. Clean water and sanitation
#7. Affordable and clean energy
#8. Decent work and growth
#10. Reduced inequalities
#12. Responsible consumption and production
#13. Climate action</td></tr>
<tr><td>Value Transfer:</td><td>Yes (also possible deployment without value transfer)</td><td>Number of Users:</td><td>Six different types of users</td></tr>
<tr><td>Types of Users:</td><td colspan="3">● Miners
● Refiners
● Logistics Operators
● Vaults
● Auditors
● Fabricators (e.g. jewelry, technology, manufacturing companies)</td></tr>
<tr><td>Stakeholders</td><td colspan="3">● The gold industry
● Industry associations (e.g. London Bullion Market, World Gold Council, Responsible Jewelry Council)
● Governments where these industry partners operate
● Government transparency groups
● Fabricators (e.g. jewelry, technology, manufacturing companies)
● Consumers</td></tr>
<tr><td>AntiData:</td><td colspan="3">Only hashes of transaction data are stored on the distributed ledger</td></tr>
<tr><td>Identification:</td><td colspan="3">To participate in the Responsible Gold Ecosystem, miners, refiners, logistic providers, vault operators as well as customers must meet robust KYC/AML standards. During onboarding, participants undergo counterparty identification procedures, verifying legal and operating structures and ultimate beneficial ownership. Partner records are updated annually. Risk assessments covering country of origin risks and suspicious activity monitoring are ongoing.
EmTech has also developed scanning technology to validate provenance and register gold bar identities on the distributed ledger. GoldID™ uses artificial intelligence to create secure identity keys from the surface analysis of each bar. These secure keys, combined with a serial number, make the authentication process foolproof. The keys are stored on the distributed ledger immediately following casting and imaging at the refinery. Users can verify the authenticity of Responsible Gold regardless of age and location.</td></tr>
<tr><td>Predicted Outcomes:</td><td colspan="3">Early identification of illicit activities and actors:
● Real-time detection of suspicious activities and red flags.
● Participants and regulators can respond faster to eliminate bad actors and illicit activities.</td></tr>
</table>

	Connecting responsible businesses in one Ecosystem: ● Immutable digital records of provenance and chain of custody boost transparency and trust. ● Adoption of the Responsible Gold Standards by supply chain participants enhances trust and Ecosystem integrity. ● Reduces audit burden and increases efficiencies by streamlining requirements and compliance data. ESG uplift for all Ecosystem participants: ● The Responsible Gold Standards are a consolidation of industry best practice controls. ● The Standards provide a practical guide to implement sustainability policies, procedures, and reporting. Continuous improvement in production practices: ● Driven by increased demand for Responsible Gold from: ○ Jewelers and other fabricators responding to customer need for gold with provenance ○ Ethical investors with ESG mandates ○ Islamic investors

Overview of the Business Problem or Opportunity

Gold plays an essential global role, from maintaining government reserves to its use in technology and healthcare. There is growing demand from end consumers for greater transparency into how the gold products they are buying come to market.

EmTech saw an opportunity to introduce DLT for gold supply chain participants to provide irrefutable assurance that gold has been mined and produced in adherence with the highest social, environment and safety standards.

All participants in the gold supply chain - from the miner to the end user - benefit from a simpler, less costly and more efficient way to ensure gold's provenance as Responsible Gold.

Why Distributed Ledger Technology?

The key advantages DLT offers over traditional systems include efficiency improvements, immutability, auditability, decentralization, and disintermediation as an internet native ledger.

- Efficiency Improvements: most business processes that are involved in global finance and trade can be scripted with computer code allowing results to be provable and permanent on the global ledger.

- Immutability and Auditability: distributed ledger utilizes peer-to-peer networking, asymmetric cryptography, and cryptographic hashing to secure the information and make it verifiable and trusted.

- Decentralization: decentralization of the distributed ledger reduces the potential for central points of failure.

- Internet Native Ledger: DLT is a distributed database leveraging native internet capabilities. Trade, financing, or industry processes can be digitally recorded and accessed anywhere by

any device that can access the internet. Although the term DLT or "blockchain" is widely used to cover a range of technologies, its core is comprised of three main components:

1. Cryptographic Hashing: a way to generate small and unique identifiers for any data, which allows for fast comparisons of large datasets and the ability to securely verify that data has not been altered. In modern DLT, various data structures are used to record the historical order of transactions, which are hashed into an identifier that functions as a method for comparison for servers on the network.

2. Peer-to-peer Networking: a set of computers that communicate among themselves without relying on a single central authority, and therefore do not have a single point of failure.

3. Asymmetric cryptography: a system that uses pairs of keys, including a public key that can be disseminated widely, and private keys that are managed securely. This cryptographic architecture allows computers to send messages to specific recipients, allowing anyone to verify the sender's authenticity, while only intended recipients can read the contents.

Section 2: Current process

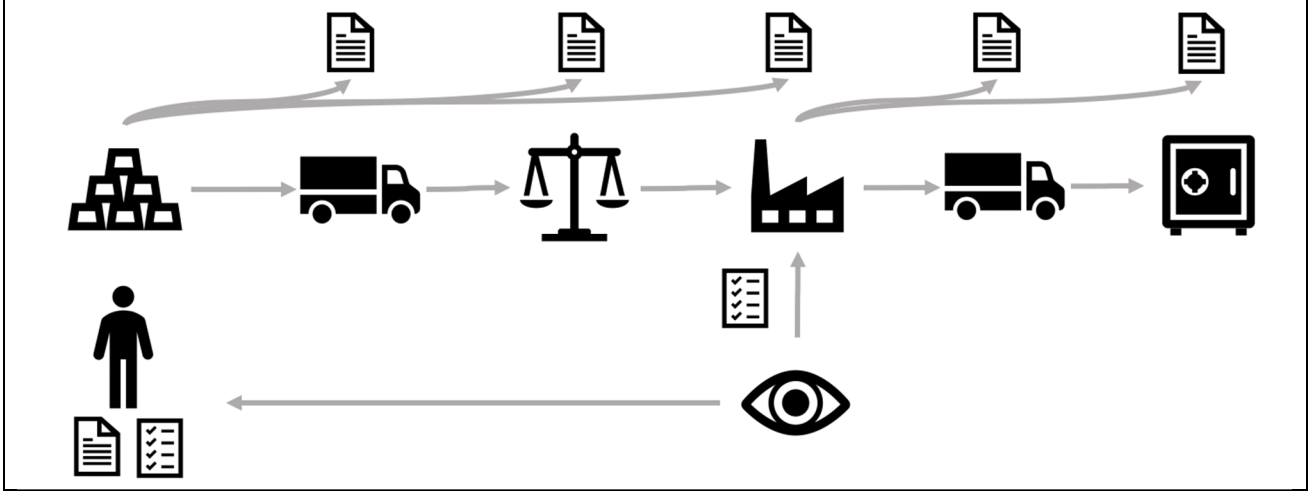
Current Solutions
Currently, there are no end-to-end systems that record the provenance of responsibly sourced gold from mine, to refiner, to vault. Current systems are siloed by organizations, largely paper-based, with ad-hoc communication taking place over phone and email. This fragmented landscape presents ample opportunities for error and manipulation.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	**Miner** pours molten ore into doré bars. Each bar is imprinted with a serial number. Its weight and assays are collected and documented. **Miner** readies the shipment for transport by packaging and sealing each bar. **Risks Identified:** ● **Miner** does not adhere to responsible mining practices resulting in negative impacts on the workforce, communities, and environment. ● Illicit metal is mixed in with legitimate gold during the pour.	**Miner** creates several hard copies of a document with information about produced bars, including serial number, weight, gold, and other element content. **Miner** shares this document with the **logistics operator**, **customs agent**, **refiner,** and **observer.** The **miner** keeps a copy of the documentation.
2.	**Logistics operator** arrives, accepts custody of the shipment and transports the shipment to **customs agents**.	**Logistics operator** confirms that physical goods for shipment are those described in the documentation.

3.	**Customs agents** inspect doré and paperwork, then take samples to levy excise tax. **Risks Identified:** ● Lack of transparency promotes corruption.	**Customs agents** document the weight of samples taken and share these with **miner** and **refiner**. Government assays are shared with **miner** to settle on payment of excise tax.
4.	**Logistics operator** delivers the shipment to the **refinery**.	
5.	**Refiner** receives the shipment and compares actual delivery against expected (via documentation from **miner** and **customs agents**). **Observer** watches unpacking, weighing, and sampling procedure on behalf of the **miner**. The **miner** is alerted of any discrepancies.	**Refiner** confirms that the physical goods in shipment are those described in the documentation from the **miner** and **customs agents**. **Observer** documents that receiving process complies with the contract between **miner** and **refiner** and attests that appropriate procedures were followed.
6.	**Refiner** settles payment with **miner**, then begins refining process. The final product (bullion) is sold to **end customers** (e.g. central banks, investors, retailers, manufacturers) who request delivery of their bullion. Often this destination is a **vault**. The **refiner** packages the bullion for delivery and contracts a **logistics operator** to carry out the delivery. **Risks Identified:** ● **Refiner** does not follow responsible production practices, resulting in harm to workers, communities, and the environment. ● Illicit gold is mixed in with legitimate gold during the refining process. ● Counterfeit bullion is introduced during storage.	**Refiner** documents refining and sales processes in different in-house systems. **Refiner** communicates shipment details to **logistics operator**.
7.	**Logistics operator** delivers the shipment to the **vault**. **Risks Identified:** ● Counterfeit bullion is introduced during transport.	**Logistics operator** confirms that physical goods for shipment are those described in the documentation.

8.	**Vault** takes custody of and vaults bullion. **Vault** confirms receipt with **end customer**. **Risks Identified:** ● Vault does not have appropriate security measures to protect gold resulting in potential theft, tampering, and risk to workers. ● Counterfeit bullion is introduced during storage.	**Vault** confirms that physical goods for shipment are those described in the documentation.

Process scheme (as-is)



Data and information (as-is)

Data	Type	Description
1	Documents	Examples include export documents, airway bills, assay reports, melt report, and sampling reports. These standardized documents convey relevant information to different participants in the supply chain.
2	Internal systems	Examples include ERP, CRM, invoicing, and quoting systems. No integrations between these systems across supply chain partners exist.
3	Contractual agreements	Documents describing expectations between two or more parties. For example, refiners require that doré have less than a certain threshold of different types of harmful elements (e.g. mercury, iron, arsenic, etc.) to complete the purchase.
4	Ad hoc phone calls and emails	When deviations from the "happy path" occur, settlement takes place via ad hoc telephone calls and emails.

Participants and their roles (as-is)

Actor	Type/Role	Description
1	Miner	Extracts precious metals from the ground.
2	Logistics Operator	Responsible for moving valuable goods from one location to another securely. Holds liability for any losses while in transit.
3	Customs agent	Accurately records precious metals as they leave the country to collect excise tax.
4	Refiner	Takes in ores, separates constituent compounds, and produces refined end products (bullion). Sells bullion to customers.
5	Vaulter	Responsible for housing valuable goods at a secure location. Holds liability for any losses while at rest.
6	Observer	Responsible for ensuring samples taken at the refinery are carried out correctly and in good faith. Represents the miner's interest in this situation.
7	End Customer	Central banks, investors, retailers, manufacturers, collectors, and other parties interested in purchasing refined gold.

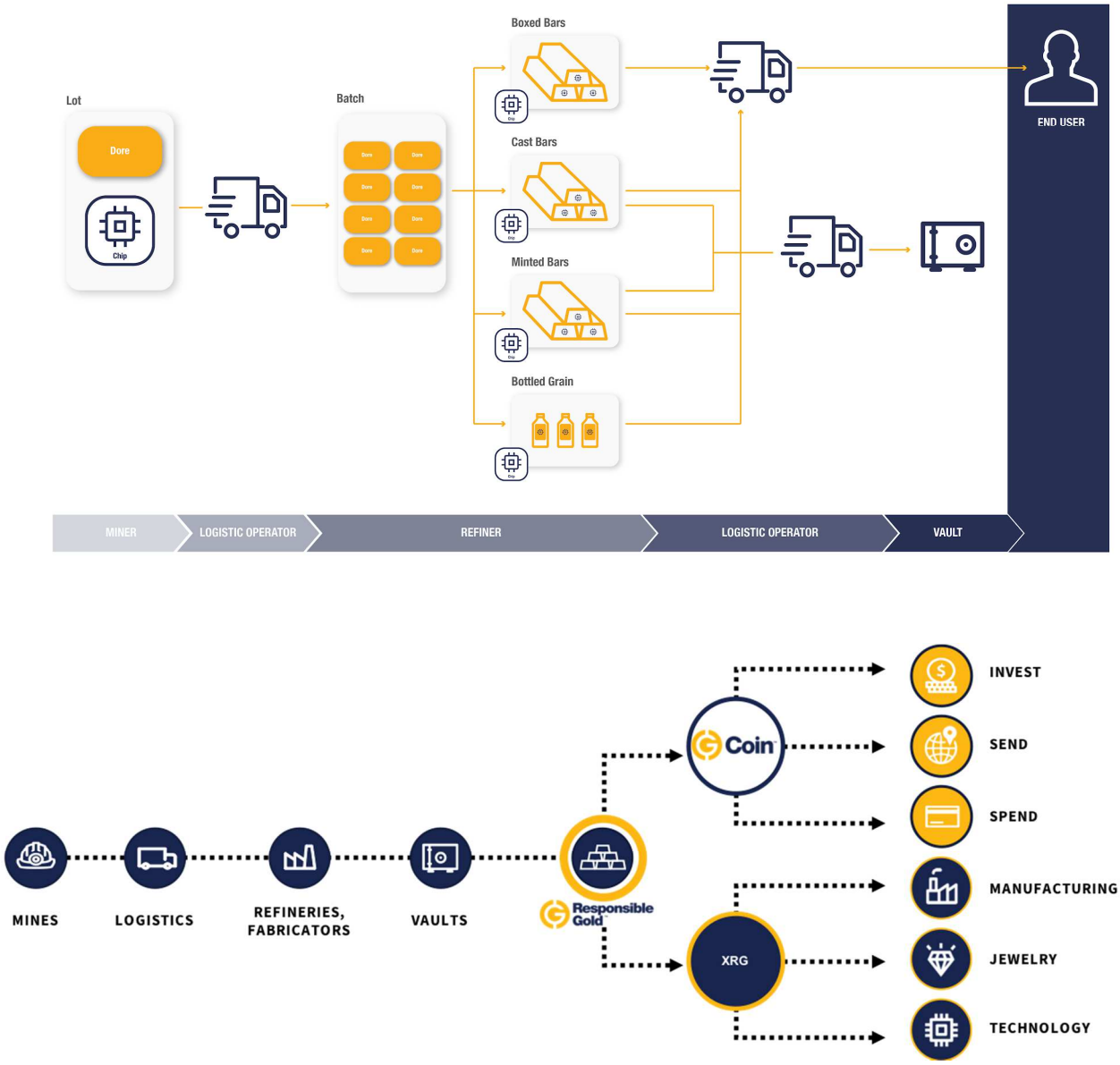
Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	**Miner** pours molten ore into doré bars. Each bar is imprinted with a serial number, and its weight and assays are collected and documented. **Miner** readies the shipment for transport by packaging and sealing each bar. **New Process:** ● **Miner** implements Responsible Gold Standards and is audited against compliance annually.	**Miner** uploads a spreadsheet containing all shipment information into the RG SCA, instantly generating assets in the system. Human and AI **auditors** compare each new shipment created by the **miner** against historical shipments from that site and flag any significant deviations for investigation. Using the RG SCA, the **miner** links each asset to a unique cryptobelt, recording all asset attributes. Upon initiating a transfer in the RG SCA, all relevant information is shared with the **logistics operator**.
2.	**Logistics operator** arrives, takes custody of the shipment and transports the shipment to the **customs agents**. **New Process:** ● **Logistics operator** implements Responsible Gold Standards and provides a self-	**Logistics operator** takes custody of each asset by using the RG SCA to scan each cryptobelt. **Logistics operator** confirms that physical goods for shipment are those described in the RG SCA and documented on the distributed ledger.

	certification of compliance annually. ● Human and AI **auditors** compare timestamps of custody transfers against expectations and flag any significant deviations for investigation.	
3.	**Customs agents** inspect doré and paperwork, then take samples to levy excise tax. **New Process:** ● Human and AI **auditors** compare sampling and assay statistics against expectation and flag any significant deviations for investigation. ● Updated values are instantaneously shared with permissioned supply chain participants.	**Logistics operator** uses the RG SCA to document the customs process on the distributed ledger, along with any supporting documents. Other participants in the supply chain corridor are notified and can view the details of the event. Upon initiating a transfer in the RG SCA, all relevant information is shared with the **refiner**.
4.	**Logistics operator** delivers the shipment to the refinery.	
5.	**Refiner** receives the shipment and confirms that physical goods they have received are those described in the RG SCA and documented on the distributed ledger.	**Refiner** takes custody of each asset by using the RG SCA to scan each cryptobelt. **Refiner** confirms that physical goods they have received are those described in the RG SCA and documented on the distributed ledger.
6.	**Refiner** settles payment with **miner**, then begins refining process. The finished product (bullion) is sold to **end customers** (e.g. central banks, investors, retailers, manufacturers) who request delivery of their bullion. Often this destination is a **vault**. The **refiner** packages the bullion for delivery and contracts a **logistics operator** to carry out the delivery. **New Process:** ● **Refiner** adopts the Responsible Gold Standards and is audited for compliance annually.	Through integrations between ERP systems and the Responsible Gold supply chain API, the **refiner** documents their refining process from doré to bullion on the distributed ledger. Human and AI **auditors** compare refining statistics against expectation and flag any significant deviations for investigation. **Refiner** uses GoldID to register an identity for each piece of bullion. Thousands of points on the surface of each bullion form a unique fingerprint, uniquely identifying that bullion and protecting it against counterfeiting. This unique identifier is hashed and stored on the distributed ledger. **Refiner** places GoldID-registered bullion into a shipping container. Using the RG SCA, the

	• Human and AI **auditors** compare refining statistics against expectation and flag any significant deviations for investigation. • Bullion is scanned using GoldID. The AI-powered technology registers a unique identity for each bullion to help future-proof against forgery.	**refiner** registers the shipping container with a new cryptobelt. This registers on the distributed ledger that the shipping container has been packed and sealed. The **refiner** initiates a transfer in the RG SCA to the **logistics operator**.
7.	**Logistics operator** delivers the shipment to the **vault**. **New Process:** • GoldID prevents substitution of counterfeit bars.	**Logistics operator** takes custody of each shipping container by using the RG SCA to scan each cryptobelt. **Logistics operator** confirms that physical goods for shipment are those described in the RG SCA and documented on the distributed ledger. Upon initiating a transfer in the RG SCA, all relevant information is shared with the **vault**.
8.	**Vault** takes custody of and vaults bullion. **Vault** confirms receipt with end customer. **New Process:** • **Vault** agrees to Responsible Gold Standards and provides a self-certification of compliance annually. • GoldID prevents receipt of counterfeit bars.	**Vault** takes custody of each shipping container by using the RG SCA to scan each cryptobelt. **Vault** confirms that physical goods for shipment are those described in the RG SCA by using GoldID.

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	Miner	Extracts precious metals from the ground.
2	Logistics Operator	Responsible for moving valuable goods from one location to another securely. Holds liability for any losses while in transport.
3	Customs agent	Accurately records precious metals as they leave the country to collect excise tax.
4	Refiner	Takes in ores, separates constituent compounds, and produces refined end products (bullion). Sells bullion to customers.

5	Vaulter	Responsible for housing valuable goods at a secure location. Holds liability for any losses while at rest.
6	Auditor	Human and AI auditors analyze data sets and flag any deviations from expected values for further investigation.
7	Customer	Central banks, investors, retailers, manufacturers, collectors, and other parties interested in purchasing refined gold.

Data and information		
Data	**Type**	**Description**
1	Responsible Gold Supply Chain Application (RG SCA)	Mobile application used by supply chain participants to track provenance and verify the integrity of gold from mine, to refinery, to vault. Documents key events on the distributed ledger.
2	Internal systems	Examples include ERP, CRM, invoicing, and quoting systems. These systems can be integrated into the RG SCA.
3	Contractual agreements	Documents describing expectations between two or more parties. For example, refiners require that doré bars have less than a certain threshold of different types of harmful elements (e.g. mercury, iron, arsenic, etc.) to complete the purchase.
4	Ad hoc phone calls and emails	When deviations from the "happy path" occur, settlement takes place via ad hoc telephone calls and emails.

Security and privacy

Semi-permissioned Blockchain

The Responsible Gold Ecosystem combines the best of both private and public blockchains. To ensure that the sensitive financial data is secure, the Responsible Gold Ecosystem has a private state. Simultaneously, the Ecosystem has a public state, which allows it to be transparent and verifiable. This hybrid configuration makes the distributed ledger highly interoperable with legacy systems and other blockchain platforms, as well as scalable with enterprise capable throughput.

Privacy

Endpoints are secured by required a web token to be supplied for any resource that is not publicly readable. The web token is issued by an authority who signs with the tenant private key. The server verifies the validity of the token using the public key from the same tenant. Inside the token is a property that identifies the specific user within the system. The system determines whether or not a user has access to the organization, which owns the resource in question. If they do, the system allows the request to be completed.

Logging and Monitoring

The applications within the Responsible Gold Ecosystem use a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. It provides applications with data and actionable insights to monitor their operation, understand and respond to

system-wide performance changes. It also collects monitoring and operational data in the form of logs, metrics, and events. This provides a unified view of resources, applications, and services that run on cloud services, and on-premises servers.

The applications also use a cloud log management and metrics monitoring solution. With the service, we monitor and troubleshoot our app in real-time to improve security and compliance. The applications also use sentry for error tracking to help monitor and fix crashes in real-time.

Data Protection

The applications within the Responsible Gold Ecosystem use Database-as-a-Service for data with inbuilt data protection features and tools. This increases the safety of accounts and data like:

- Database authentication
- Account-level security settings with two-factor authentication
- Secured communication (SSL connections)
- Custom firewalls with access only restricted from our environment using whitelisted IPs

Access Control List

Network accounts are implemented in a standard fashion and utilized consistently across the organization. Accounts are for individuals only. Account sharing and group accounts are not permitted. A specific example is database administrators who are not allowed to log in to databases as MySQL users and must use their own accounts. User accounts are not given administrator or 'root' access unless it is necessary to perform their job function. Individuals requiring access to confidential data have an individual and distinct account.

QA and development have no access to production systems. All production systems are accessed programmatically, via automated deployment scripts.

Intrusion Detection

A monitoring solution provides threat detection. The solution continuously monitors for malicious or unauthorized behavior to help protect cloud accounts and workloads. It monitors for activities, such as unusual API calls or potentially unauthorized deployments, that indicate a possible account compromise. It also detects potentially compromised instances or reconnaissance by attackers.

Main success scenario + expected timeline

The Responsible Gold Ecosystem is live in production and has been piloted with three different major gold mines. The technology is continuously being enhanced. There are significant ongoing efforts to promote it within the gold industry.

In the short term (1-3 years), similar ecosystems based on responsible standards can be created/replicated for other industries. Receiving acknowledgment and support from reputable industry bodies, such as ITU and UN, will help promote and educate prospective users on how DLT can enhance supply chain integrity.

Conditions (pre- or post-)

Pre-conditions:

1. Participants are required to sign legal agreements applicable to their part in the process.
2. Some fees may be payable, such as license and hardware costs.

Post-conditions:

1. Participants continue following the Responsible Gold Supply Chain process and adhere to the Standards that underpin the Ecosystem.
2. Participants must provide evidence when auditable DLT records are reviewed.

Performance needs

The production DLT utilized by Responsible Gold Ecosystem has been tuned and optimized for enterprise throughput demands. Currently, the production DLT has been tested exceeding 10,000 transactions per second. There are ongoing developments that will exceed this.

The DLT utilizes an iBFT consensus algorithm and generates a new block every second. The DLT provides the speed, security, and reliability required by almost all enterprise use cases and exceeds that of any existing supply chain provenance application.

The network leverages node-as-a-service operators who provide 99.99% uptime guarantees and cloud-based load balancing and failover protection.

Legal considerations

Distributed ledger technology and, by extension, the Responsible Gold Blockchain Network, may be subject to a variety of federal, state, and international laws and regulations, including those with respect to consumer privacy, data protection, consumer protection, content regulation, network neutrality, cybersecurity, intellectual property (including copyright, patent, trademark and trade secret laws), and others. These laws and regulations, and the interpretation or application of these laws and regulations, could change. In addition, new laws or regulations affecting the Responsible Gold Blockchain Network could be enacted.

Additionally, the users and developers of the Responsible Gold Blockchain Network may be subject to industry-specific laws and regulations or licensing requirements. If any of these parties fail to comply with any of these licensing requirements or other applicable laws or regulations, or if such laws and regulations or licensing requirements become more stringent or are otherwise expanded, it could adversely impact the Responsible Gold Blockchain Network.

Risks

To participate in the Responsible Gold Ecosystem, each party must commit to the Responsible Gold Standards. Each participant is directly responsible for attesting that all records they enter into the RG SCA are true and accurate. AI and human auditors review data entry against expectations (based on historical analysis) and flag potential mis-entry or fraudulent entries for review. Parties proven to have acted in bad faith could be exposed to legal action.

The primary technical risk to participants in the Responsible Gold Ecosystem is poor connectivity/slow internet. Inadequate connectivity may cause communication between a device and the distributed ledger to be delayed, or to fail. This would require a user to repeat the process once connectivity has been restored. This risk primarily exists only at the most remote mine sites.

Special Requirements

Prospective participants must be willing to implement the Responsible Gold Standards and follow specific steps in the supply chain workflow to record the provenance of Responsible Gold.

Implementation of the solution also requires participants to install the RG SCA on a registered mobile device and provide an infrastructure with an internet connection.

External References and Miscellaneous

THE RESPONSIBLE GOLD STANDARDS

The Responsible Gold Standards draw on existing ESG standards and industry guidance. Examples include:

- World Gold Council Conflict Free Standard
- LBMA Responsible Gold Guidance
- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas
- UN Global Compact
- UN Principles of Responsible Investment

- Fork of blockchain
- Quorum blockchain consensus algorithms
- Cryptobelts use asymmetric encryption to remain unique
- GoldID uses artificial intelligence and hashes

RECENT NEWS COVERAGE OF EMTECH AND RESPONSIBLE GOLD

- Discussing Responsibly Sourced Gold Business - CNBC
- Blockchain Comes to the Gold Market - SBMA
- Blood Gold Drives an Industry Mine to Market Transparency Push - Bloomberg
- EmTech Brings Gold on the Blockchain - Ethereum World News

Other Notes

Implementation of Responsible Gold Ecosystem may involve some license fees and hardware cost charged to the participants.

Traceability in the Food Supply Chain in Brazil

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-007	**Use Case Type:**	*Vertical*
Submission Date:	**March 29, 2019**	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Traceability in the food supply chain in Brazil	**Domain:**	*Supply chain management*
Status of Case	*Pilot*	**Sub-Domain**	*Agriculture; Data processing, storage and management*
Contact information of person submitting/ managing the use-case	*Rodrigo Lima Verde Leal* *Innovation and Product Marketing* *rodleal@cpqd.com.br* *+55 19 3705 5994* *@cpqd* *https://www.cpqd.com.br* *https://www.linkedin.com/company/cpqd/*		
Proposing Organization	*Fundação CPqD - Centro de Pesquisa e Desenvolvimento em Telecomunicações, simply called CPqD Foundation.* *Brazil.* *National registration number, C.N.P.J. in Brazil: 02.641.663/0001-10*		
Short Description	Pilot for beef traceability solution comprised of the integration of Safe Trace's food supply chain traceability system to a DLT in order to provide transparent, immutable and verifiable data to relevant stakeholders.		
Long description	This Pilot is the first step for providing provenance and quality information to all relevant stakeholders in the the food supply chain. The DLT-based system creates a digital identity for each asset being traced, which contains information that is needed for an end-to-end audit trail perpassing all stakeholders in the supply chain, from producers to retailers, that is both safe and reliable. For instance, if a disease in a given farm or region is detected, all by-products from those animals that may be contaminated can be traced back more efficiently and with lower costs due to recalls. The integration of DLT to Safe Trace's system provides transparency, reliability and immutability of data to all relevant stakeholder in the beef supply chain. Other characteristics that are also important to consumers, such as social and environmental compliance of farms, animal wellbeing and quality assessments throughout the supply chain, can also be part of the solution. In this Pilot, CPqD created the DLT-based network and smart contracts (aka chaincodes), as well as the services layer, which includes the integration APIs for legacy systems, which are also part of the network.		

	The development framework is Hyperledger Fabric, maintained by The Linux Foundation.		
SDG in Focus (when applicable)	*SDG 2: 2.4* *SDG 3: 3D* *SDG 8: 8.6 and 8.7* *SDG 12: 12.3, 12.6 and 12.A* *SDG 15: 15.1, 15.2, 15.5*		
Value Transfer:	*Assets (cattle)*	**Number of Users:**	*14 meatpackers and 1 retailer*
Types of Users:	*Farmer, Meatpacker, Retailer, Consumer, Traceability System Provider*		
Stakeholders	*NGO, Government*		
Data:	***Regarding what data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc:*** ● ***Identity*** *of individual animals and animal batches.* ● ***Hashes*** *of transactions data (e.g. vaccines, weight measurements, sensor data etc), operations between participants (ownership transfers) and transformations of raw materials (e.g. cuts, wrapping pieces).* ● ***No data is stored in the DLT****, only hashes, thus allowing for all participants to share registers on the ledger without exposing sensitive information.* ***Regarding how the DLT solution would interact with external data and other systems:*** ● *Daaps are integrated to a DLT solution developed on Hyperledger Fabric and integration APIs are used by legacy systems, such as the one provided by the Traceability System Provider.*		
Identification:	*This Pilot does not work with pseudonyms. Full identification of relevant stakeholders participating in the network are required by the Traceability System Provider.*		
Predicted Outcomes:	The predicted outcomes of adopting new processes based on this system are: ● increased trust in a trustless supply chain that has players with conflicting interests. ● increased transparency of relevant food quality information; ● increased transparency of social compliance information (i.e. slavery conditions); ● increased transparency of environmental compliance information (i.e. deforestation and forest burning); ● reduce audit and compliance costs; ● decrease food recall direct and indirect costs; ● better risk management; ● produce data that may be relevant for aggregate analysis of the supply chain condition.		

Overview of the Business Problem or Opportunity

Since 2009, the Brazilian Federal Public Ministry has imposed a conduct adjustment term (TAC) to the meatpackers, where they commit to only buy cattle from farmers that are not related to illegal deforestation, by checking their suppliers with geomonitoring tools and crossing that information with the product invoice information and the animal transport authorization (GTA).

Despite Brazil having plenty of monitoring tools to avoid socio-environmental and sanitary risks, and the commitment of Amazon biome industries and national retailers to buy only deforestation free beef, Brazil fails to obtain greater value added to bovine meat by ineffectiveness of public policies to guarantee the sanitary and socio-environmental control of the production chain, resulting in production still largely associated with deforestation.

The business problem is to keep traceability records for beef supply chain, from the birth farms to the consumer, relating to this sanitary events, quality informations, and socio-environmental analysis related to illegal deforestation and forced labor.

Those informations are collected from multiple databases from public and private sector, validated and converted in KPIs and scorecards provided to the demand side, bringing enhanced risk analysis and transparency.

Why Distributed Ledger Technology?

DTL improves current solutions by assuring provenance and quality information in a transparent way to all relevant stakeholders of the food supply chain, and in this Pilot the focus is cattle. The DLT solution created a digital ID for each asset that will be traced. It is with this ID that information regarding the animal, as well as production lots formations, movements, sanitary data, quality and transformations, are exchanged between different actors in the food chain - from production phase in farms and processing industry, to meat available to retailers, This creates an audit trail, safe and secure, of animal provenance.

*The main DLT features required for this solution are **transparency** and **immutability** of data, which, along with, **verifiability**, allow for all players to develop a safer food supply chain.*

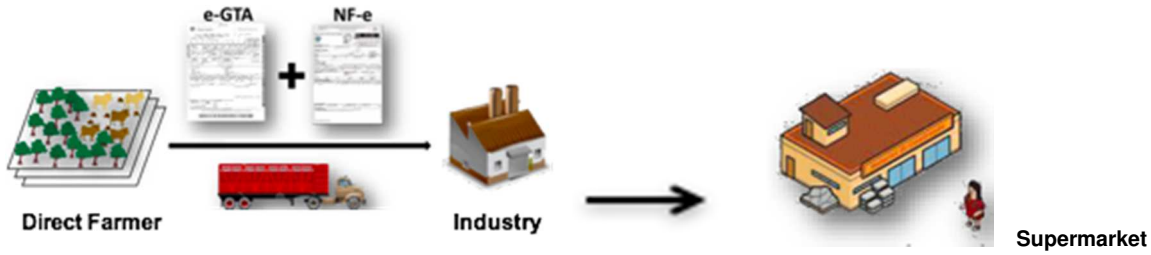
Section 2: Current process

Current Solutions
Current solutions are dependent on siloed information from farmers, industries and retailers, having limitations to crosscheck information without an audit process. *In such solutions, farmers and meatpackers are responsible for inserting their own information in the traceability system, bringing only partial information to the beef supply chain.* *Based on the information entered, the traceability system asks suppliers of geomonitoring solutions for evidence that the properties indicated by the meatpacker do not have reports of slave labor or illegal deforestation and then records this result, used in the performance indicators used by retailers.*

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Farmer	In general does not inform any data. Only registers an Invoice (Nota Fiscal) and a GTA into the government database. In specific market chain programmes, may input specific sales information into the system, such as lot number or animal ID.
2.	Meatpacker	Register animal acquisition, socio-environmental checks and sales to retailers.
3.	Retailer	Verifies that data input was made by the meatpacker.
4.	Consumer	For specific meat lines that represent less than 1% of the market (e.g. premium cuts), may have access to the list for provenance farms that supplied the meatpacker in a given production date. In other cases, consumer have no access to information.
5.	Traceability System Provider	Gather information on animals acquired by meatpacker, socio-environmental checkings, production lots and its sales to retailers.

Process scheme (as-is)



Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents and supply chain data*	GTA, Invoices (buyer, seller), geomonitoring data, logistics data (boxes and pallets identifiers etc).

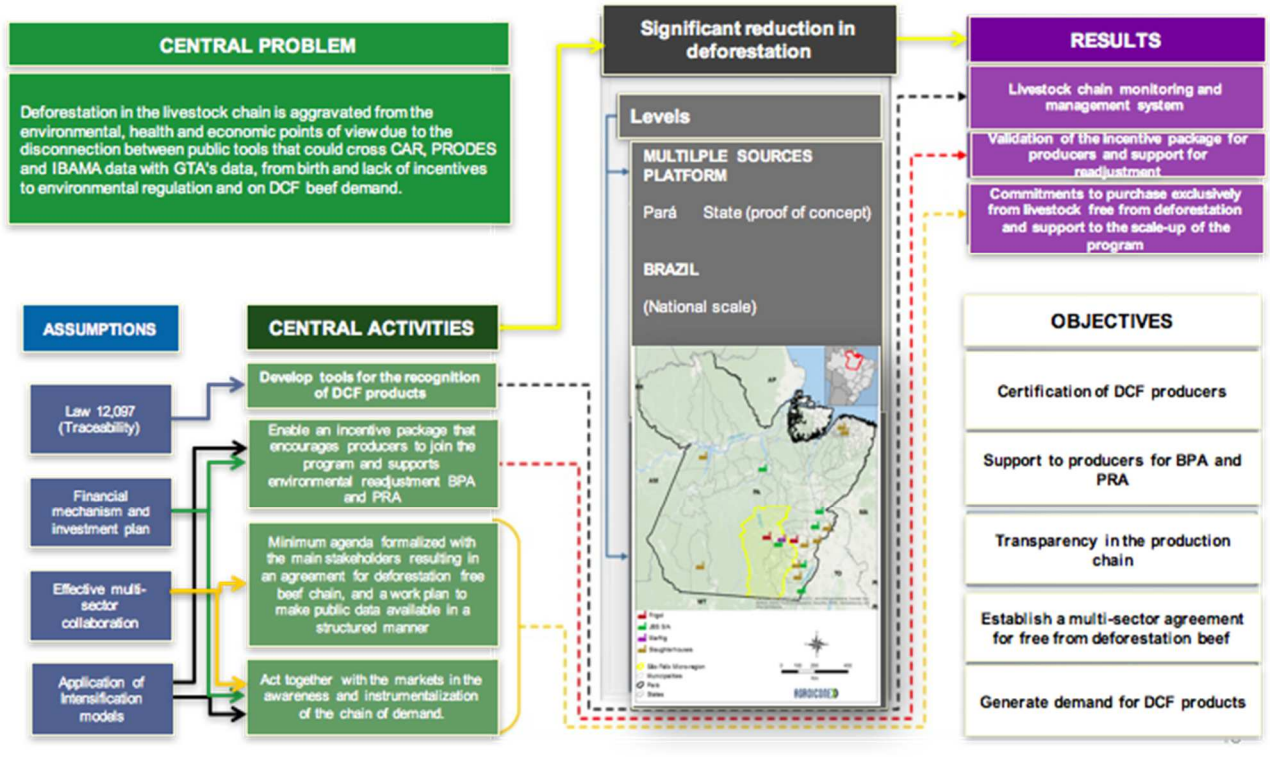
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Farmer*	Generates invoices (Nota Fiscal) and GTA when a sale is made to the metapacker.
2	*Meatpacker*	Buys animals, verifies socio-environmental info, provides production traceability data.
3	*Retailer*	Put pressure on meatpackers to make them compliant to legislation and agreements with the Public Ministry.
4	*Consumer*	Transparency.
5	*Traceability System Provider*	Gathers information and generates evidences for auditing.
6	*NGO*	Supervises and demand transparency.
7	*Government*	Controls the generation of GTA and invoices (Notas Fiscais).

Other Notes
N/A

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Farmer	Manages its ID, inputs information on good production practices and monitors data on its risk level, calculated from sanitary and social-environmental information. Applicable to all production chain (farmer that sells animals to another farmer) and not only the farm that sells directly to the meatpacker.
2.	Meatpacker	Inserts the data of the purchase and the social-environmental analysis of the farm, which are validated in the blockchain in order to protect the identity of the producer.
3.	Retailer	Tracks KPIs about the level of risk in its supply chain and works to minimize these risks.
4.	Consumer	Access key data on traceability via QRcode.
5.	Traceability System Provider	Acts on the interfaces with users and systems, standardizing the data so that they are registered in the ledger.

Process scheme (to-be)



Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Farmer*	Will provide more information and engage other producers that are not part of the sustainable food chain.
2	*Meatpacker*	Will provide more information and engage other meatpackers that are not part of the sustainable food chain.
3	*Retailer*	Will provide access to suppliers from other food chains.
4	*Consumer*	Will have access to transparent traceability from deforestation free suppliers.
5	*Traceability System Provider*	Will expand its clients number and ticket.
6	*NGO*	May become observer nodes.
7	*Government*	Government bodies may mandate stakeholder in the food chain to become part of this network. Government bodies may also participate in the network by providing information to all stakeholders, such as black list of slavery conditions, IBAMA, PRODES and CAR.

Data and information		
Data	**Type**	**Description**
1	*Documents and supply chain data*	GTA, Invoices (buyer, seller), geomonitoring data, logistics data (boxes and pallets identifiers etc).
2	*Government databases*	Relevant information from various government databases related to social-environmental aspects.

Security and privacy
1. Information is available only to participants in a given business transaction in the supply chain. i.e. other players that are not part of such transaction have no access. Only hashes of the data are in the ledger, allowing for any player that have access to that data may verify its authenticity. *2. TLS, secure storage of PKI, OAuth2.* *3. The Traceability System Provider should provide mechanisms for data integrity control and access control.*

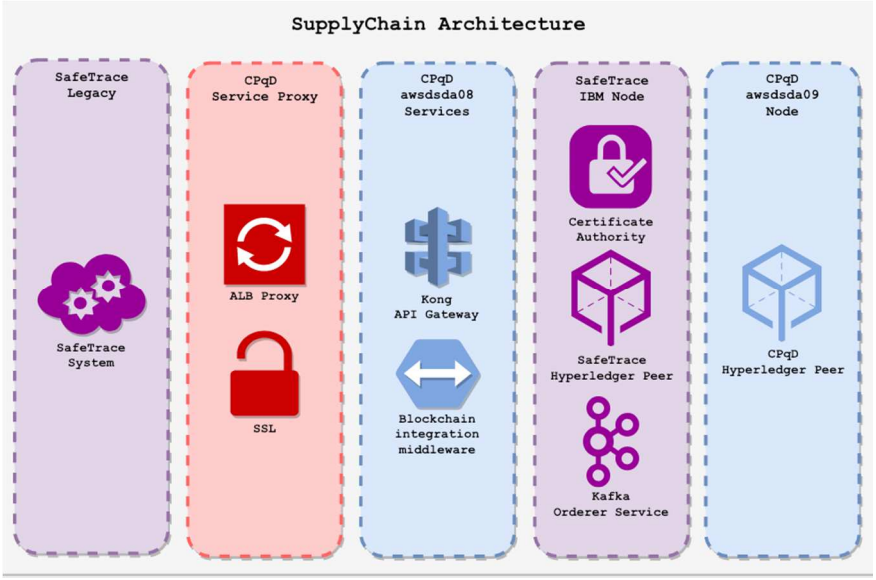
4. DLT should be available 24/7/365.

Main Success Scenario + expected time line

DLT-based solution that registers events that occured in any given time, throughout each step of a food supply chain, in a reliable way.

Main success scenario comprises the ability of any participant organization to register signature data of an asset (i.e. the identifier of a cattle or a batch), in order to allow for traceability of information throughout the network, such as, but not limited to, transactions data (e.g. vaccines, weight measurements, sensor data etc), operations between participants (ownership transfers) and transformations of raw materials (e.g. cuts, wrapping pieces), and also the verification of the authenticity of registered data.

The architecture below is already implemented and running in a Pilot.



Current work is focused on performance, scalability and resilience with real data until May/2019.

Based on results, future work will be focused on further requirements brought by relevant stakeholders, specially retailers, in order to create a second version of the solution.

Conditions (pre- or post-)

1. The Traceability System Provider must have established a financial contract with relevant stakeholders.

2. Relevant stakeholders must be registered in the identity solution and enabled to read/write hashes of transactions data (e.g. vaccines, weight measurements, sensor data etc), operations between participants (ownership transfers) and transformations of raw materials (e.g. cuts, wrapping pieces).

3. No data is stored in the DLT, only hashes.

4. Other products in the food supply chain should be easily included in the solution, such as coffee, fish etc.

5. Chaincodes and integration APIs must be deployed.

6. All relevant parties are connected to DLT-network and be compliant with a governance framework.

Performance needs

Due to the high volume of data registered by the users, the solution may have to comply with 800 TPS or more.

Interoperability needs are related to native multi-cloud support, in order to allow for the infrastructure diversity used by organizations, such as on premises data-center or clouds services.

Reliability and availability should be met using a fault tolerant microservices architecture, such as downtime in any organization that are not part of a given transaction being processed.

Legal considerations

1. The legal basis for using the DLT-based solution as an official version of facts in case of a legal dispute.

Risks

1. Legal risks, including regulation of legal basis of data validated in a DLT-based solution;

2. Security risks;

3. Relevant stakeholder do not accept to be part of the network;

4. Difficulty in having stakeholder develop and comply with governance framework;

5. Immaturity of DLT.

Special Requirements

N/A

External References and Miscellaneous

Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.

Rules for the protection of personal data inside and outside the EU.

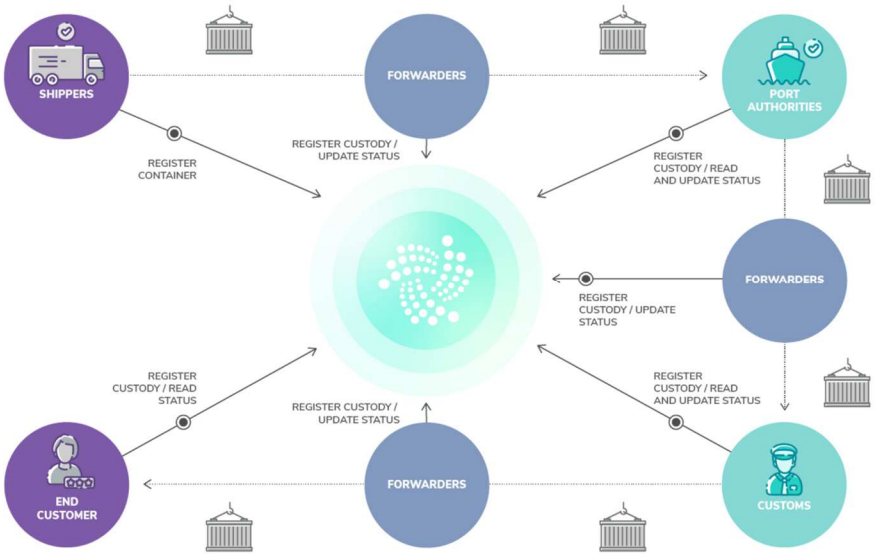
Other Notes

N/A

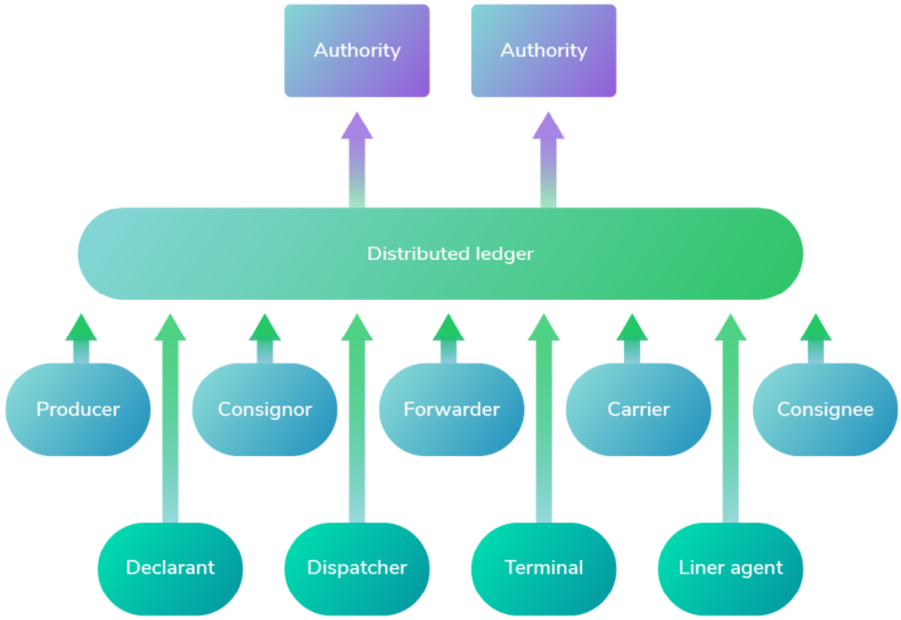
Trade Facilitation and Customs Management

Section 1: Summary

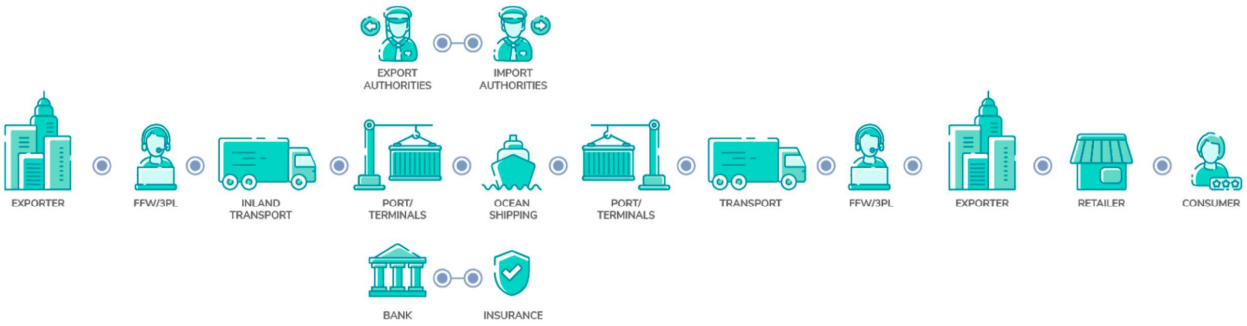
Use Case Summary			
Use Case ID:	IND-008	**Use Case Type:**	*Vertical*
Use Case Title:	Trade facilitation and customs management	**Is Use Case supporting SDGs**	*No*
		Domain:	Industry/Supply Chain
Status of Case	*Proof of Concept*	**Sub-Domain**	
Contact information of person submitting	*Full Name:* ***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.

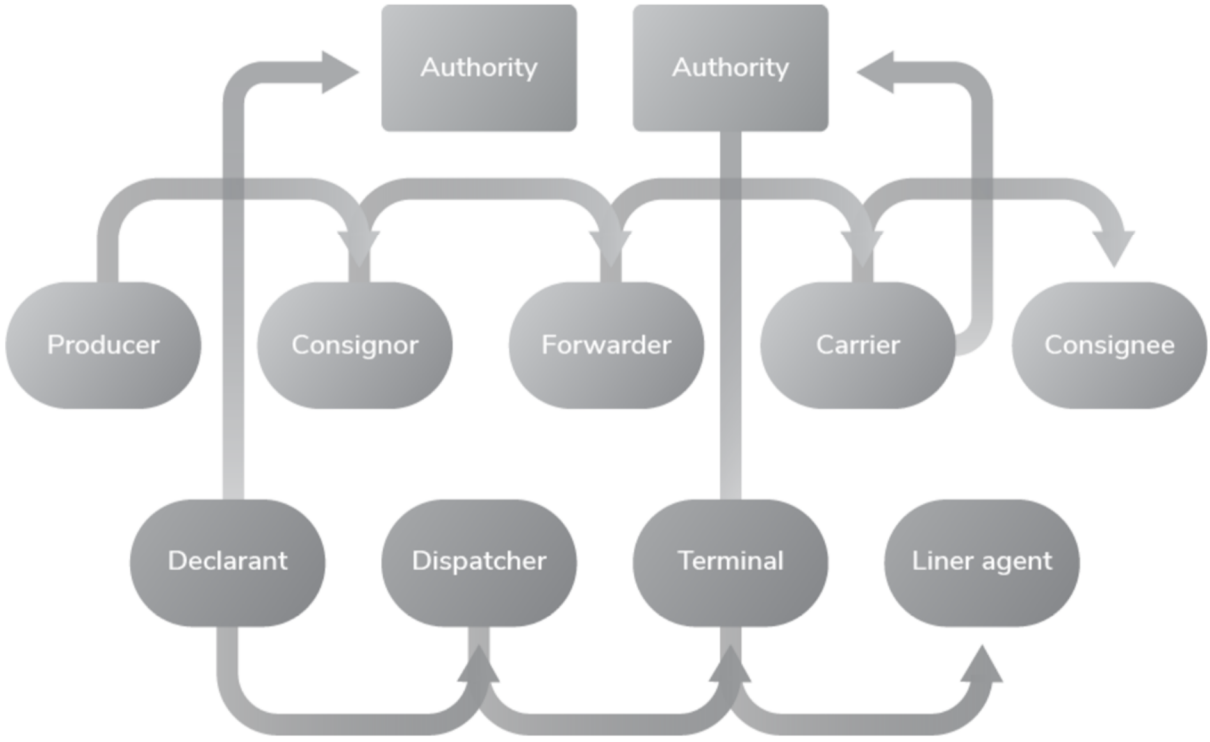
Overview of the Business Problem or Opportunity
International trade is a complex system facing a number of inefficiencies. Figure 4 below shows how international containers shipment of goods is mainly composed of many actors and three flows: ● the physical movement of containers; ● the exchange of data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

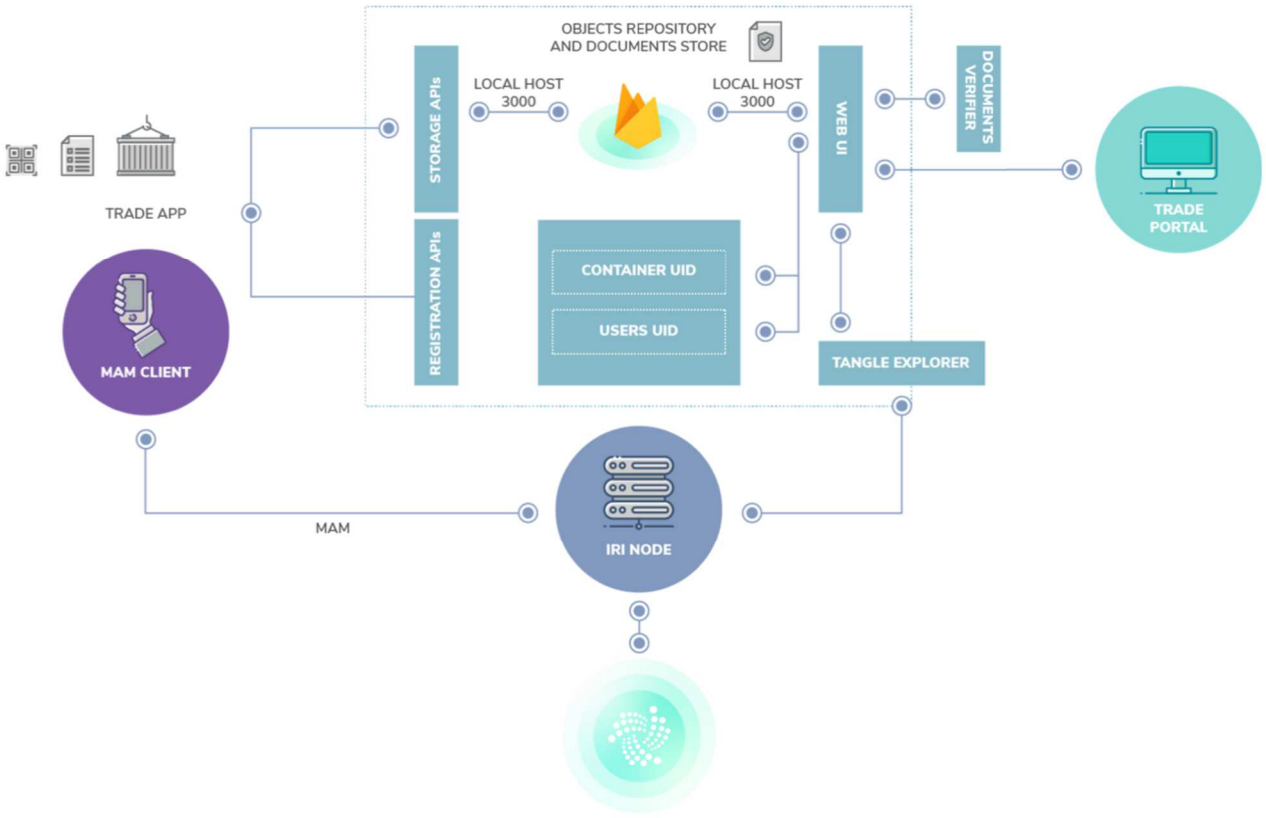
Section 3: Expected process

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);

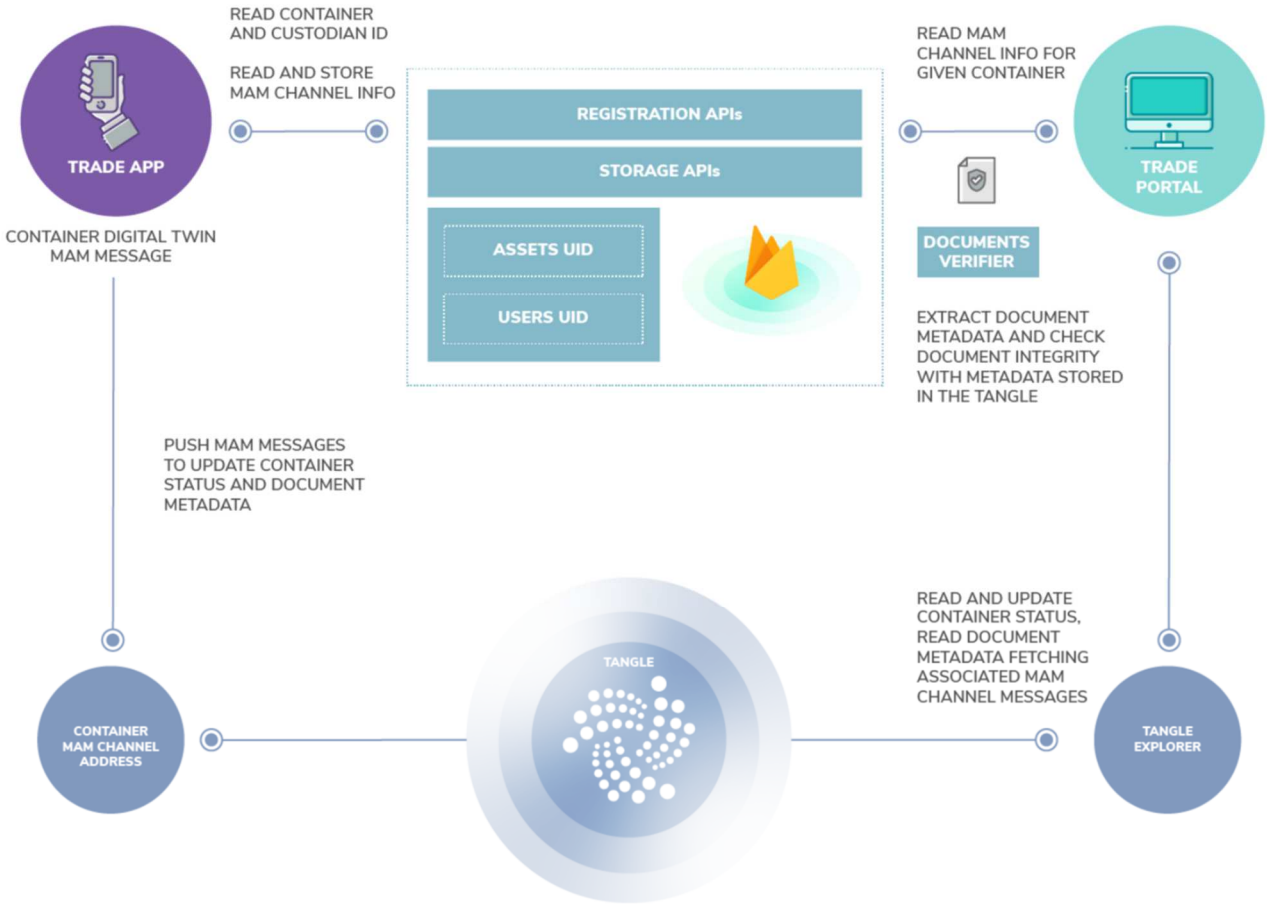
have been implemented in order to respectively access and update existing MAM channel information (e.g. adding new messages to update the stored digital twin). Information is then attached to the correct MAM channel and stored immutably onto the IOTA Tangle.

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

Polo Multimodal PECEM

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-009	**Use Case Type:**	*Industry/3 and 4*
Submission Date:	January 4, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Polo Multimodal Pecem	**Domain:**	*List 1 Appendix 1*
Status of Case	*Proof of Concept (POC)*	**Sub-Domain**	*Supply chain management*
Contact information of person submitting/ managing the use-case	*Ingrid Barth* *Chief Blockchain Officer* *E-mail address: ingrid@cosmosblockchain.co* *Telephone number: 11 983615309* *Social media:https://www.linkedin.com/in/ingrid-barth-48a17b19/* *Web site:* ***http://www.polomultimodal.com/***		
Proposing Organization	*Polo Multimodal Pecem* Fotaleza (Ceará) - Brazil		
Short Description	Polo Multimodal Pecem is a project with over 20 million square meters located in the logistic corridor of Port of Pecém, in the municipality of São Gonçalo do Amarante, State of Ceará, that will create a Blockchain Lab with the intention to create Blockchain and DLT solutions to help industries inside the Polo to solve problems. The first solution will be use blockchain time stamp and immutability to track goods into the Porto do Pecem.		
Long description	Polo Multimodal Pecem is a project with over 20 million square meters located in the logistic corridor of Port of Pecém, in the municipality of São Gonçalo do Amarante, State of Ceará. Conceived to house both national and international companies from different sectors, the POLO MULTIMODAL PECEM was designed within the most modern and rigorous criteria of infrastructure, technology and sustainability; promoting innovation to contribute to the progress of a new industrial age. The idea is also having a Blockchain Lab inside de Polo, with the intention to create blockchain and DLT solutions for all opportunities there. The first idea, based on problems that companies are having in all Ports around the world, is create a solution in a public Blockchain to help companies register in blockchain, in a permanent way and using the time stamp, all tracking about goods, process, containers, flows, in order to bring more security, avoid losses and create new solutions for the flow. Also, other benefits as hold all data and use it for further works – provide data for insurance companies to have a best score and price.		
SDG in Focus (when applicable)	*8 – Decent Work and Economic Growth* *8.3 Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation,*		

	and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services		
Value Transfer:	*Security in shipping and transportation processes, possibility to reduce costs and security for the goods.*	**Number of Users:**	*All companies and people involved. The Pecem Port is growing about 34% year.*
Types of Users:	*Companies, society, employees, Pecem port*		
Stakeholders	*Companies, society, employees, Pecem port*		
Data:	*Data will be basically all data involved in shipping processes: Company name, shipping documents, type of goods, date, locations, destination, serial numbers, container number, seals, employees that input data, receivers.*		
Identification:	*Full identification of all participants, like company, employees, location, destination, goods to be transported.*		
Predicted Outcomes:	*The predicted outcomes of the adopting the new process are to:* *- increase transparency in all supply chain scheme* *- Avoid losses and frauds during the shipping and transportation* *- More control about shipping process* *- More security in shipping process* *- Higher efficiency and consequently better companie's reputation* *- Less bureaucracy once they can certify the veracity in all infos*		

Overview of the Business Problem or Opportunity

After the Panama Canal expansion, the port of Pecém began to gain a growing importance in the international logistics scenario.

With its 18 metres natural depth, it is on the list of the main ports in the world capable to dock large containers ships (post-panamax) and it has been attracting relevant overseas investments to the region in the last few years. Pecem port is growing about 34% per year, and the region is lacking in resources.

Because of that, is important to consider solutions that use 4.0 technologies, as DLT/ Blockchain, that can improve process and transform the port and the region in a model abroad, showing concerns with security, losses with frauds, efficiency in shipping process, that cause millions dollar in losses.

Supply chain is today the most important and efficiently uses cases in DLT/ Blockchain because the possibility of traceability and immutability, creating a huge transformation in supply chain process.

Why Distributed Ledger Technology?

DLT/ Blockchain is today one of the most exponent and sophisticated technological constructions. This is because in addition to being a decentralized and distributed database, the information once inserted and validated is immutable and with the time stamp, which creates a chain of trust in the processes where Blockchain is inserted and avoid problems with frauds and security of data.

Another important point is that it allows the level of governance to be high since each new information registered will be validated and will only continue if most of the participants in that chain validate it.

Section 2: Current process

Current Solutions

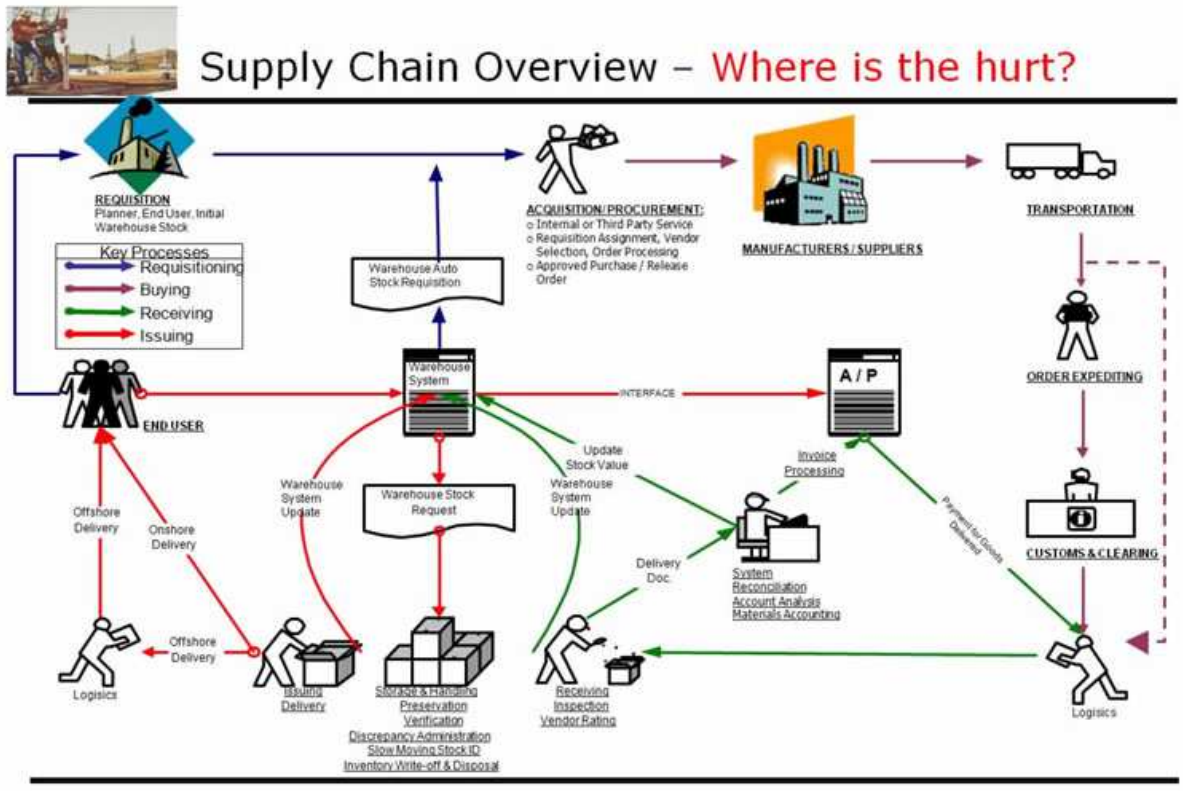
Today in supply chain a huge part of processes is manual, and companies sometimes can use their own systems to store data and other information.

There is no problem to store data inside the company, but there are a lot of fraud cases in this manual process. Also, is very difficult identify the phase that a problem happened, the number of steps is huge, so if you can register phases in an immutable DLT, for sure they can find and fix problems more quickly.

Important to mention that in all port supply chain scheme companies can have problems already described.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Requisitioning	Create a requisition into the specific system and generate agreements that will be used in the shipping process
2.	Buying	Payments will be done by the buyer and compensated by the seller. This process also will generate documentation that will be used in the shipping process.
3.	Receiving	Receiving goods and prepare all docs and licenses to start the delivery.
4.	Issuing	Aggregate information about transactions joined with entities additional information. Company will also hire shipping enterprises that will delivery goods in the placed or country agreed. All information, documentation and licenses here should be right, or the shipping will be cancelled.

Process scheme (as-is)


Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	Common export/ import docs: Commercial invoices Export/ Import packing list Pro form invoice Bill of landing Export licenses Generic certificate of Origin Insurance certificate Shipper's letter if instruction
2	*Payment transactions*	Payments should be done in a several ways: through bank loans, money transfer, prorated. In this case the most important is receive the ok from the seller and the buyer, or in same cases from the bank involved.

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Buyer*	People or company that want to buy the goods. Can be inside the country, in other city, or other country.
2	*Seller*	Entity who sells a product or service to the buyer
3	*Bank*	Financial institution to provide transfer/payment between parts
4	*Shipping companies*	Companies that provide shipping services
5	*Insurance companies*	Companies that provide insurance for goods to be transported.

Other Notes
Important the remind that process described above is the very basic one. Depending on the goods, countries involved, companies and banks, will be necessary to increase docs and processes.

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Requisitioning	Create a requisition into the specific system and generate agreements that will be used in the shipping process
2.	Buying	Payments will be done by the buyer and compensated by the seller. This process also will generate documentation that will be used in the shipping process.
3.	Receiving	Receiving goods and prepare all docs and licenses to start the delivery.
4.	Issuing	Aggregate information about transactions joined with entities additional information. Company will also hire shipping enterprises that will deliver goods in the placed or country agreed. All information, documentation and licenses here should be right, or the shipping will be cancelled.

Process scheme (to-be)
The main shipping process will basically be the same, the difference here will be that all docs and related information will be registered in DLT/ Blockchain technology for all participants envolved, and the time stamp (via hash) will be generated, to create the security that info was not changed. This hash should be included in docs.

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Buyer*	People or company that want to buy the goods. Can be inside the country, in other city, or other country.
2	*Seller*	Entity who sells a product or service to the buyer
3	*Bank*	Financial institution to provide transfer/payment between parts
4	*Shipping companies*	Companies that provide shipping services
5	*Insurance companies*	Companies that provide insurance for goods to be transported.

Data and information		
Data	**Type**	**Description**
1	*Documents*	Common export/ import docs: Commercial invoices - hash Export/ Import packing list – hash Pro form invoice - hash Bill of landing - hash Export licenses - hash Generic certificate of Origin -hash Insurance certificate - hash Shipper's letter if instruction - hash
2	*Payment transactions*	Payments should be done in a several ways: through bank loans, money transfer, prorated. In this case the most important is receive the ok from the seller and the buyer, or in some cases from the bank involved.

Security and privacy

1. *Information will be encrypted, DLT/ Blockchain system will not keeping any type of docs, the only think that the DLT/ Blockchain will do is provide a existence prove and time stamp that will certify the veracity of information.*
2. *Since transparency is the main requirement, the ideal information visibility is public;*
3. *If business privacy prevent public visibility, this critical subset of data can be encrypted or protected;*
4. *DLT system should be able to provide mechanisms of DLT data integrity control;*
5. *DLT data and related services (System Actions) should be available in 24/7/365 mode;*
6. *The entity identity solution should prevent identity fraud.*
7. *The products and services type identification solution should prevent fraud. (Future Vision only)*

Main Success Scenario + expected time line

Registration process to avoid frauds or improve logistics problems.

benefits data published without human intervention.

Expected time line – End of 2019

Conditions (pre- or post-)

1. *Process should be accepted for all participants involved.*
2. *All parties are connected to DLT Network*

Performance needs

1. Transactions processing near real time;

2. 24/7/365 availability;

3. API integration to the DLT Network

Legal considerations

Changes in the original process should be consider in a legal perspective

Risks

1. Legal risks, including regulation of DLT uses and taxation;

2. Security risks;

3. Sellers do not accept new process;

4. Buyers do not want new process;

5. Risks related to DLT immaturity.

6. Data security

Special Requirements

N/A

External References and Miscellaneous

http://www.polomultimodal.com/blockchain-lab-en

https://build.export.gov/main/logistics/eg_main_018121

https://www.ibm.com/blockchain/industries/supply-chain

https://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain

Other Notes

N/A