

Reverse Logistics Credits

Section 1: Summary

Use Case Summary					
Use Case ID:	IND-003	Use Case Type:	<i>Vertical</i>		
Submission Date:	January 4, 2019	Is Use Case supporting SDGs	<i>Yes</i>		
Use Case Title:	Reverse Logistics Credits	Domain:	<i>3</i>		
Status of Case	<i>Pilot</i>	Sub-Domain	<i>g</i>		
Contact information of person submitting/managing the use-case	<p><i>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/</i></p> <p><i>Web site: www.brpolen.com.br</i></p>				
Proposing Organization	<p><i>Legal Name: POLEN CONSULTORIA E INTERMEDIACAO DE NEGOCIOS EM SUSTENTABILIDADE LTDA - EPP</i></p> <p>Country: Brazil</p> <p>CNPJ: 28.038.406/0001-82</p>				
Short Description	<p><i>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.</i></p>				
Long description	<p>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:</p> <ul style="list-style-type: none"> - Waste Pickers collect, sort and sell post-consumption waste to recycling industry - Packaged goods manufacturers ‘buy’ the invoices from the 				

	<p>transactions described above from the association paying in the form of improvements in the association's infrastructure and machinery.</p> <ul style="list-style-type: none"> - Packaged goods manufacturers use these invoices to prove to authorities that they were financially responsible for the recycling of the post-consumption waste. <p>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.</p> <p>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.</p> <p>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.</p>	
SDG in Focus (when applicable)	<p>GOAL 8: DECENT WORK AND ECONOMIC GROWTH</p> <p>GOAL 9: INDUSTRY, INNOVATION AND INFRASTRUCTURE</p> <p>GOAL 12: RESPONSIBLE PRODUCTION AND CONSUMPTION</p> <p>GOAL 14: LIFE BELOW WATER</p>	
Value Transfer:	<i>Users transact tokens that represent the collection and recycling of 1 ton of post-consumption packaging waste</i>	Number of Users: TBA
Types of Users:	<i>Reverse Logistics Operator (company or association that is responsible for collecting and selling post-consumption packaging waste to the recycling</i>	

	<p><i>industry)</i></p> <p>Packaged Goods Manufacturers (<i>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</i>)</p> <p>Auditors (<i>Brazilian Government body that is responsible for overseeing the compliance of such legislation</i>)</p> <p>System Operator (<i>company that develops and maintain the online platform and infrastructure where tokens are issued, bought and sold</i>)</p>
Stakeholders	<p>General society: <i>is benefited by the increase in recycling rates and the environmental consequences that come from said increase.</i></p> <p>Waste Pickers Associations: <i>is benefited by the extra income earned due to the selling of the Reverse Logistics Credits.</i></p> <p>Packaged Goods Manufacturers: <i>are provided with a simple and secure mechanism to comply with legislation and offset environmental impact of their activities.</i></p> <p>Government bodies responsible for overseeing compliance of such legislations: <i>are provided with an easy and secure way to audit the compliance of such legislation</i></p>
Data:	<p>The DLT will store data about commercial transactions that complete the reverse logistics process (Reverse Logistics Operator selling post-consumption waste to Recycling Industry).</p> <p>Invoices of such transactions officially issued by the Brazilian fiscal authorities will be parsed and tokenized if adherent to the requisites above.</p> <p>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.</p>
Identification:	<i>Identity of participants will be available only for the marketplace provider and government authorities</i>
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.

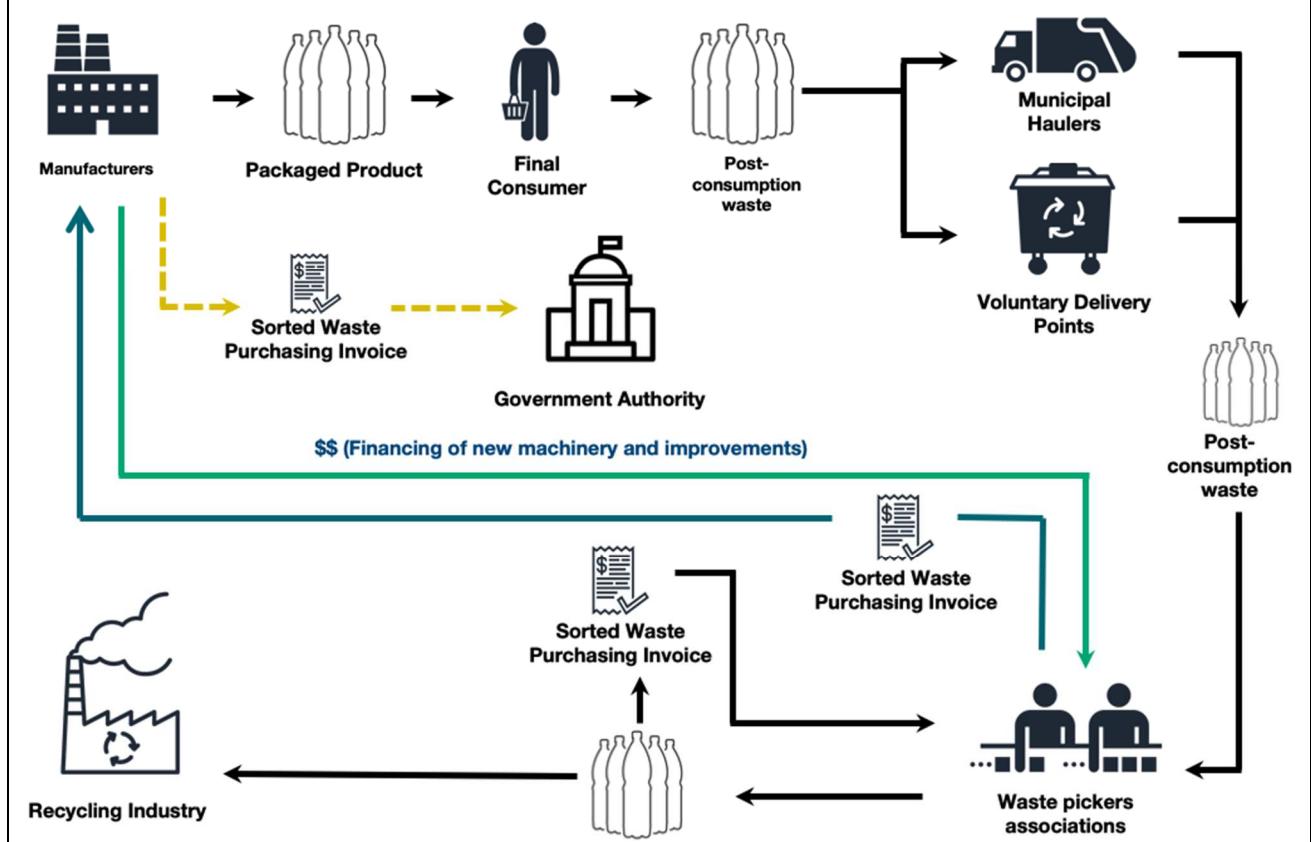
Section 2: Current process

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

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	<i>Invoices</i>	Invoices issued by the official Brazilian fiscal authority.

Participants and their roles (as-is)

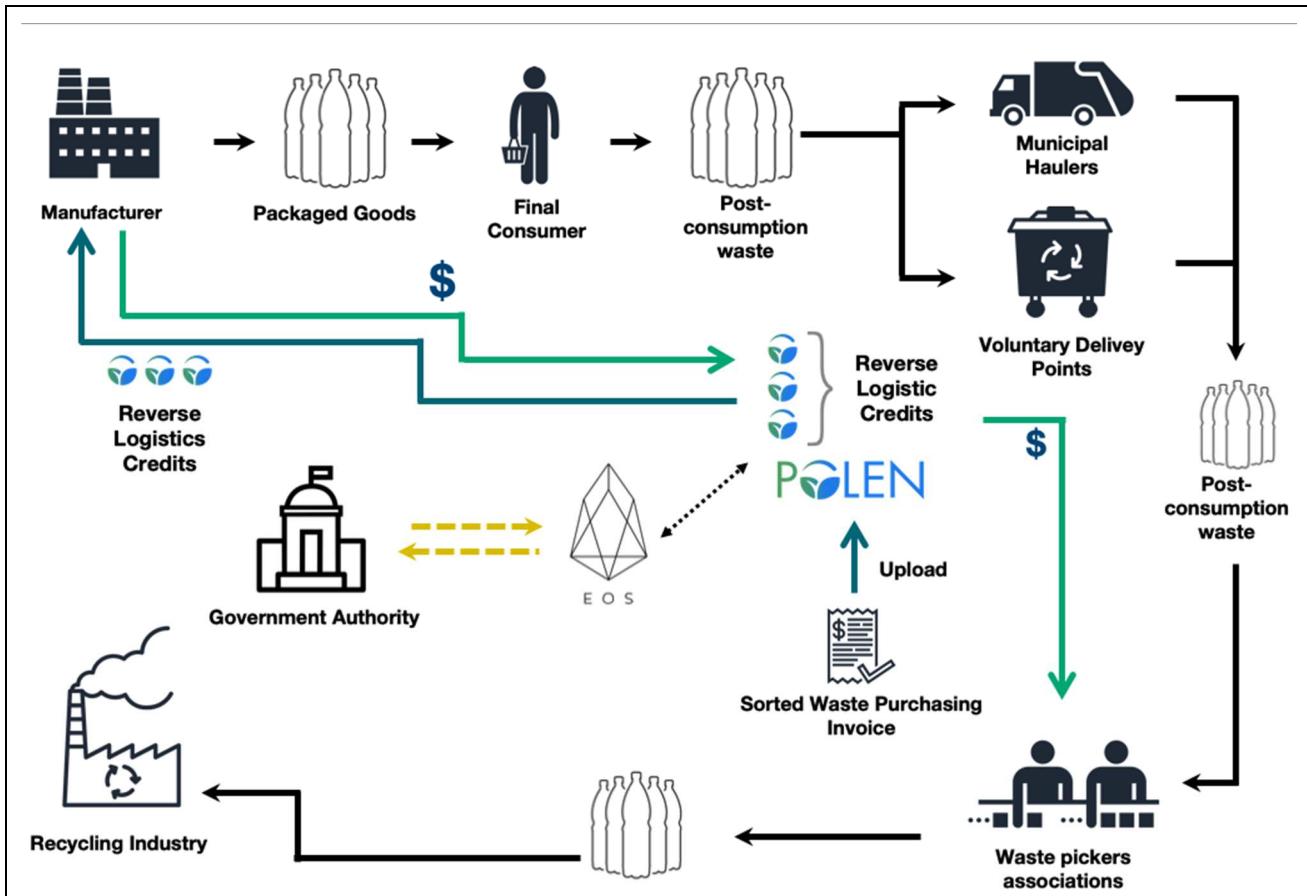
Actor	Type/Role	Description
1	<i>Packaged good manufacturers</i>	Buys invoices (representation of a commercial transaction) from waste pickers associations to provide evidence that they have funded the recycling of a certain amount of post-consumption packaging waste.
2	<i>Reverse Logistic Operators/Waste Pickers Association</i>	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	<i>Auditors</i>	Brazilian Government body that is responsible for overseeing the compliance of such legislation.

Other Notes
<i>Any assumptions, issues</i>

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 and assigns to user accounts.
3.	Reverse Logistic Operator uploads the electronic invoice to the platform	System parses 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 these 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 participant’s accounts and the provenance of these tokens.

Process scheme (to-be)



Participants and their roles

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

Data and information

Data	Type	Description
------	------	-------------

1	<i>Electronic Invoices</i>	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	<i>User Profile</i>	User profile on Polen's database for public-key and CNPJ syncing.
3	<i>Reverse Logistics Credits (cryptographic tokens)</i>	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	<i>'Burnt' tokens balance</i>	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
<i>The DApp functions are basically:</i>
<i>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.</i>
<i>Trade tokens - Polen tokens are free tradable.</i>
<i>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 forever frozen on behalf of a given CNPJ (brazilian company registry)</i>

Conditions (pre- or post-)
1.

Performance needs
<i>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 bandwidth). The irreversibility happens when 15/21 BPs build on top of a block, which happens in up to 90 seconds.</i>

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 CO ₂ , 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:	<p>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.</p> <p>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.</p>

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

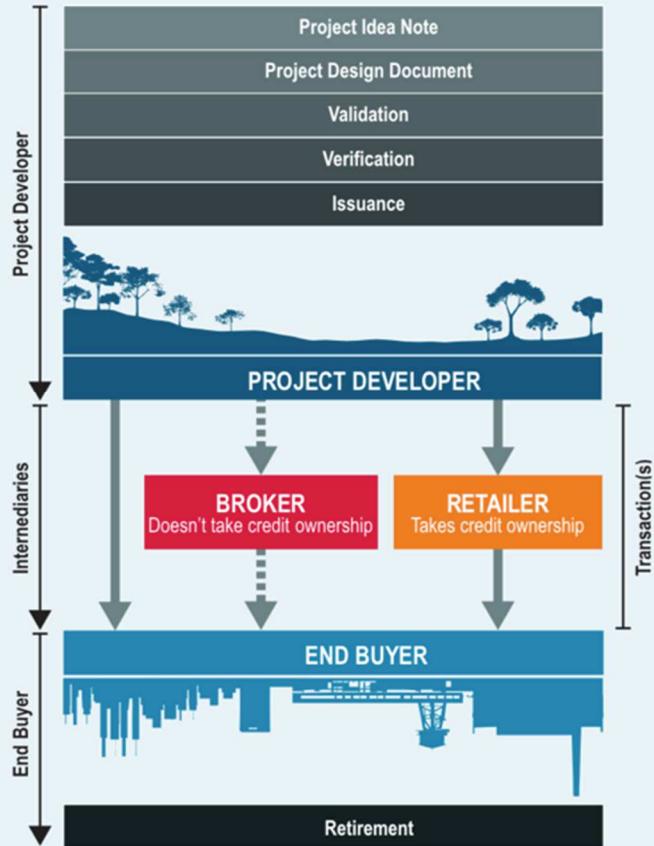
Current Solutions

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 Teraton 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)

Figure 1: The Offset Cycle, from Project Development to Retirement



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

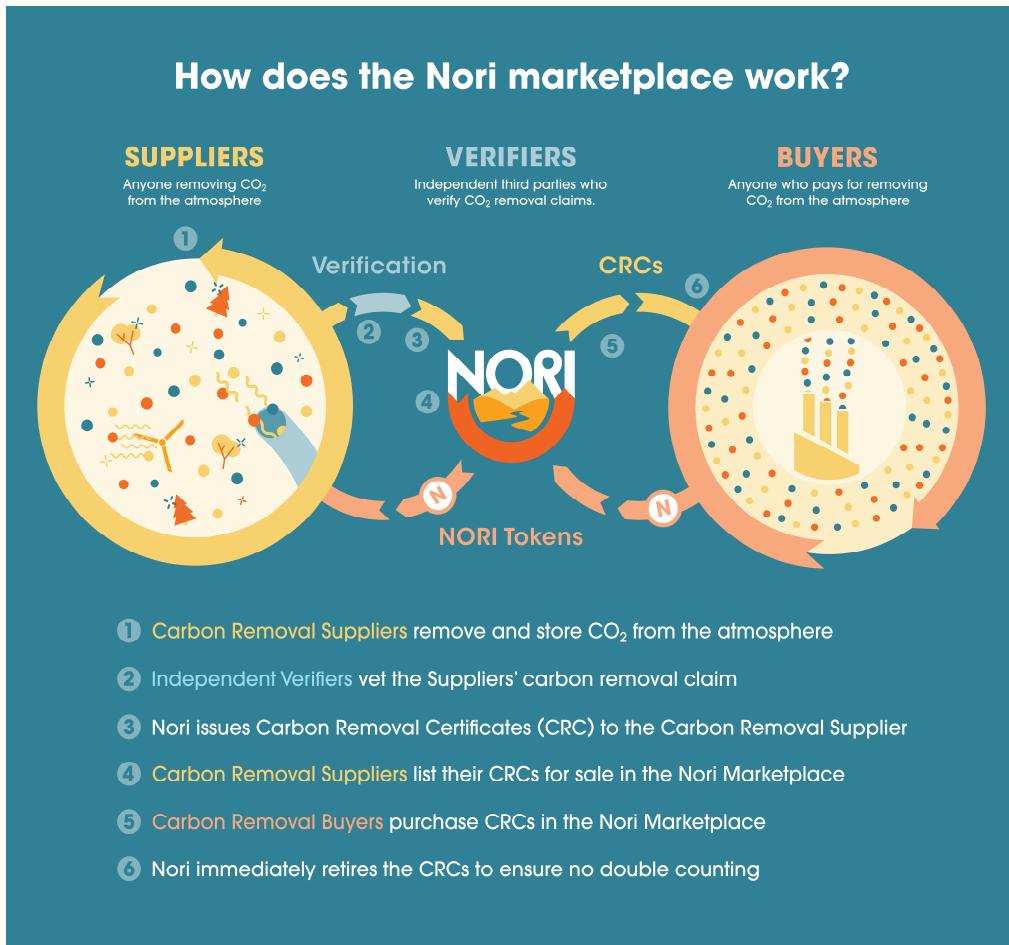
Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Corporate offset buyers	Typically sustainability officers at companies who purchase offset credits to meet voluntary or regulatory offsetting commitments.
2	Project developers	Developers of projects that avoid future GHG emissions.
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	<p>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.</p> <p>E.g. Farmers, manufacturing companies, mining companies, universities, biofuel producers, technology startups, forest managers, etc.</p>

Participants and their roles		
Actor	Type/Role	Description
2	Buyers	<p>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.</p> <p>E.g. Food producer companies, socially-responsible corporations, events/conferences/festivals, power utilities, local/state governments, individuals, etc.</p>
3	Verifiers	<p>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.</p>
4	Baseline generators	<p>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.</p> <p>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.</p>
5	Peer reviewers	<p>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.</p>

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 CO ₂ .
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 CO ₂ , 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:	<ul style="list-style-type: none">- 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

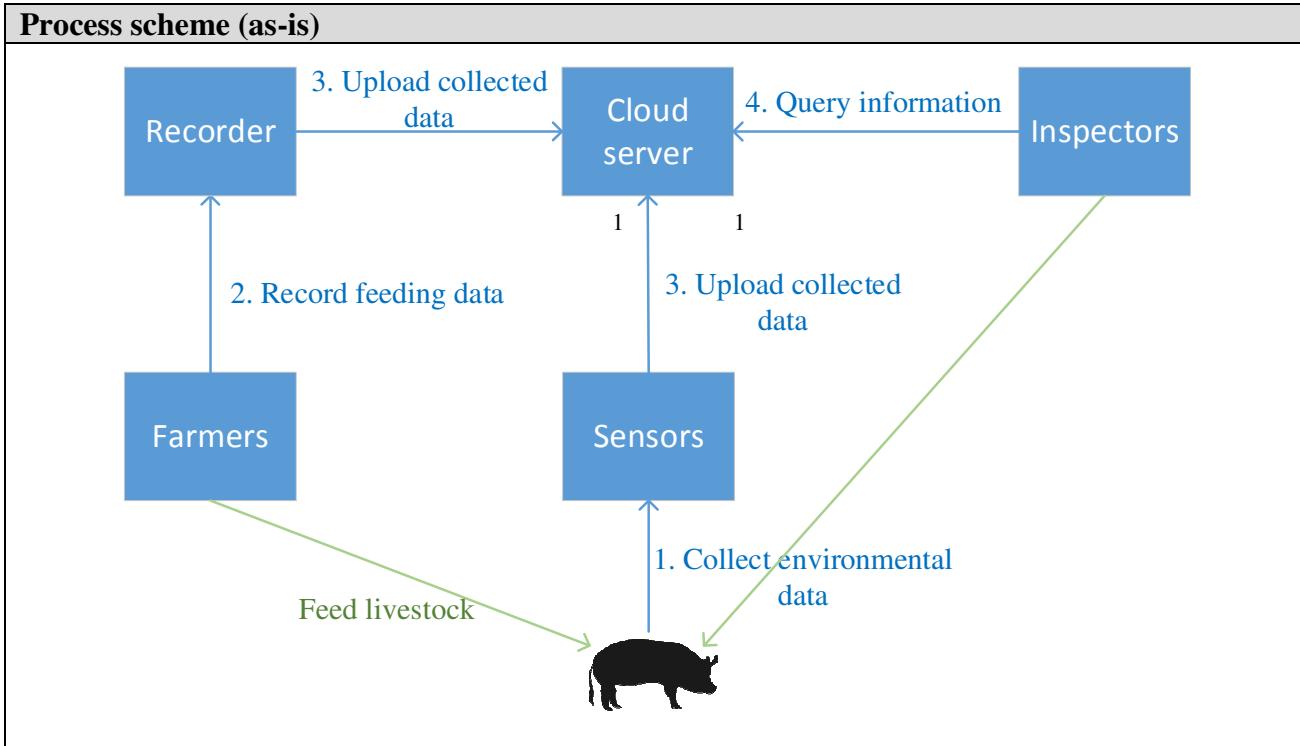
Current system monitors the feeding, living environment of pigs.

- 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 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.



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.

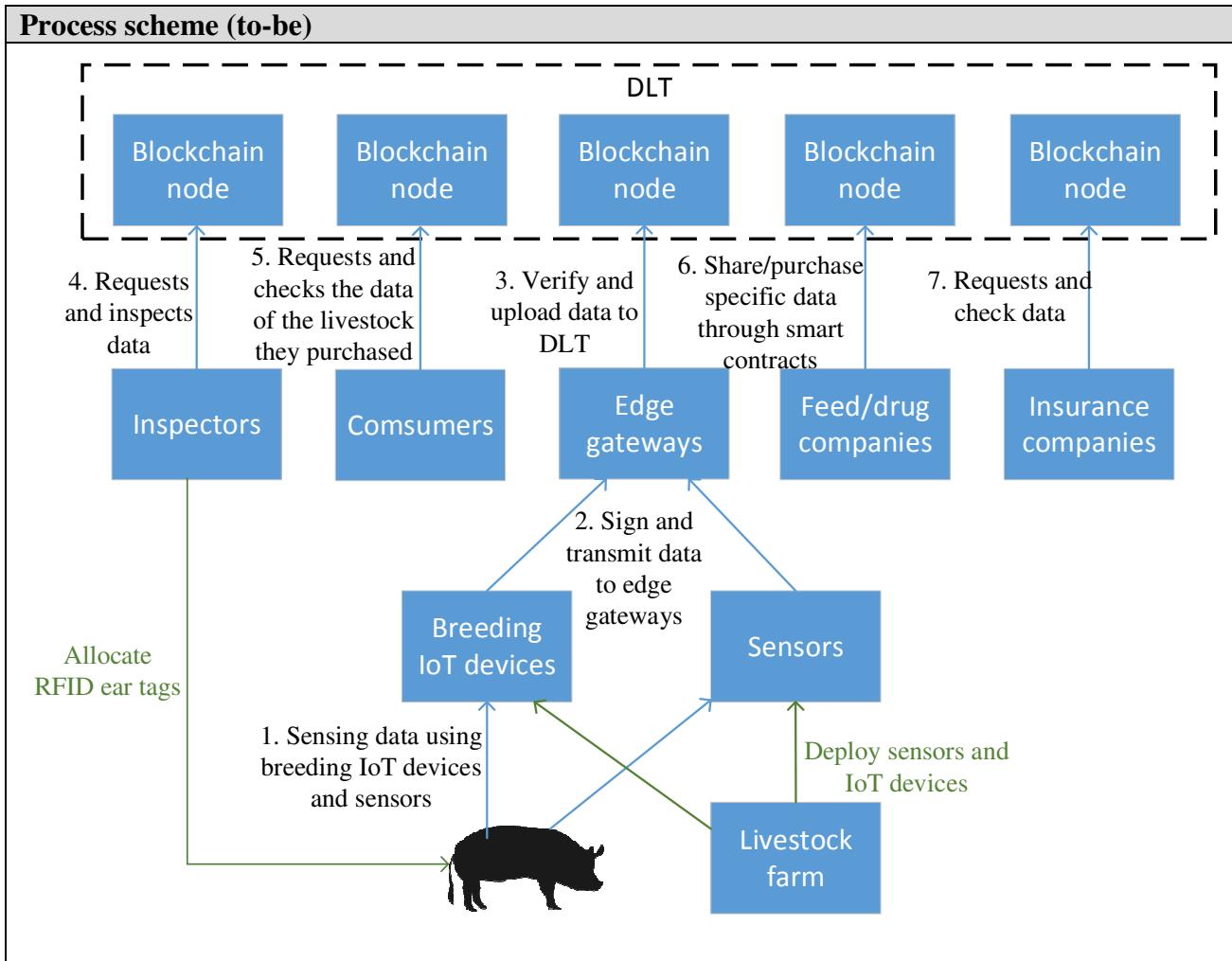
Participants and their roles (as-is)

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.



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%20Sem-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:	<i>Vertical</i>
Submission Date:	May 28, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Responsible Gold Ecosystem	Domain:	www.responsiblegold.com
Status of Case	<i>Implementation / (Live in production)</i>	Sub-Domain	
Contact information of person submitting/managing the use-case	<p>Victor Vilmont VP Innovation and Product Management https://www.linkedin.com/in/victorvilmont/ Email: victor.vilmont@emergenttech.com Tel: +1 415 278 1100</p> <p>Stephen Grinalds VP Engineering R&D https://www.linkedin.com/in/stephengrinalds/ Email: stephen.grinalds@emergenttech.com Tel : +1 408 669 2104</p> <p>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</p> <p>Web: www.emergenttechnology.com</p>		
Proposing Organization	<p>Emergent Technology Holdings (EmTech)</p> <p>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.</p>		
Short Description	<p>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.</p>		

	<p>EmTech's Responsible Gold Ecosystem ("Ecosystem") provides a much-needed solution to the increasing transparency and trust burden.</p> <p>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.</p> <p>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.</p> <p>EmTech is committed to sustainable development by:</p> <ul style="list-style-type: none">● Supporting participants in embedding responsible business practices;● Connecting responsible companies and people in one Ecosystem; and● Trading Responsible Gold
Long description	<p>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:</p> <ul style="list-style-type: none">● 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. <p>Despite regulations and international standards to manage these risks, illicit activities persist.</p> <p>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.</p> <p>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."</p> <p>The Standards help ensure that gold in the Ecosystem:</p>

	<ul style="list-style-type: none">● 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 <p>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.</p> <p>The Responsible Gold Ecosystem uses a combination of hardware and software to automatically:</p> <ul style="list-style-type: none">● 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. <p>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.</p> <p>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 auditible, eliminating the possibility of bad actors altering records at any time.</p>
SDG in Focus (when applicable)	<p>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.</p> <p>The primary focus of our business is on the following SDGs:</p> <p>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."</p> <p>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."</p>

	<p>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:</p> <p>#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</p>		
Value Transfer:	Yes (<i>also possible deployment without value transfer</i>)	Number of Users:	Six different types of users
Types of Users:	<ul style="list-style-type: none"> ● Miners ● Refiners ● Logistics Operators ● Vaults ● Auditors ● Fabricators (e.g. jewelry, technology, manufacturing companies) 		
Stakeholders	<ul style="list-style-type: none"> ● 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 		
AntiData:	Only hashes of transaction data are stored on the distributed ledger		
Identification:	<p>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.</p> <p>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.</p>		
Predicted Outcomes:	<p>Early identification of illicit activities and actors:</p> <ul style="list-style-type: none"> ● Real-time detection of suspicious activities and red flags. ● Participants and regulators can respond faster to eliminate bad actors and illicit activities. 		

	<p>Connecting responsible businesses in one Ecosystem:</p> <ul style="list-style-type: none">• 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. <p>ESG uplift for all Ecosystem participants:</p> <ul style="list-style-type: none">• 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. <p>Continuous improvement in production practices:</p> <ul style="list-style-type: none">• Driven by increased demand for Responsible Gold from:<ul style="list-style-type: none">○ 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

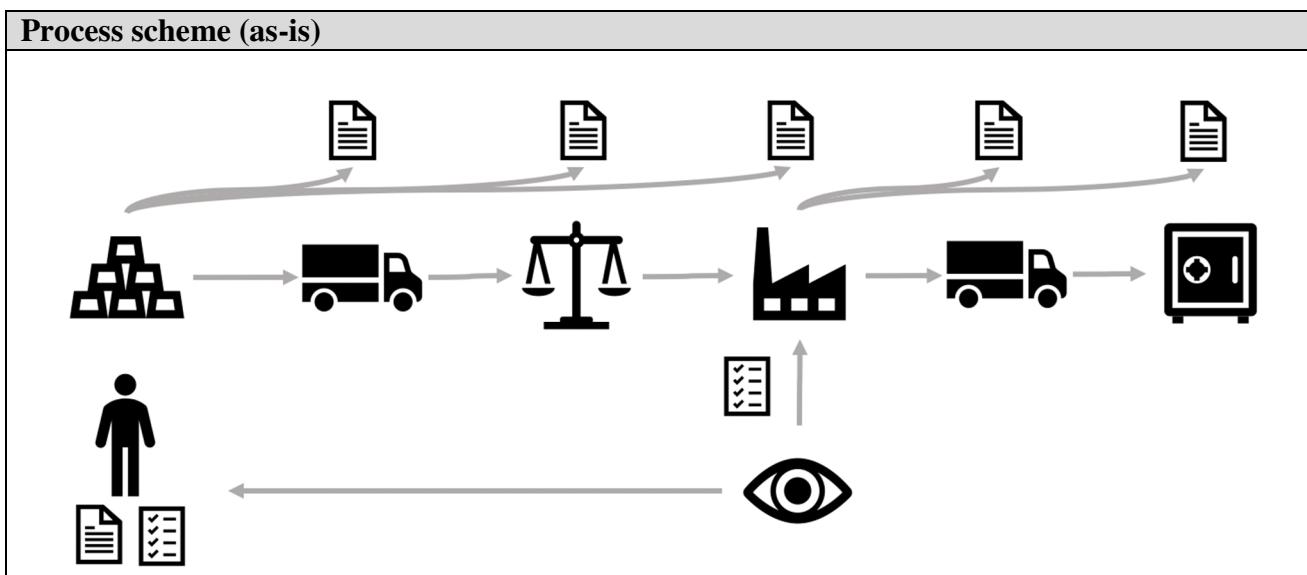
Currently, there are no end-to-end systems that record the provenance of responsibly sourced gold from mine, to refiner, to vault. Current systems are siloed by organizations, largely paper-based, with ad-hoc communication taking place over phone and email. This fragmented landscape presents ample opportunities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

Existing Flow (as-is)

Step	User Actions	System Actions
1.	<p>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.</p> <p>Risks Identified:</p> <ul style="list-style-type: none">• 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.	<p>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.</p>
2.	<p>Logistics operator arrives, accepts custody of the shipment and transports the shipment to customs agents.</p>	<p>Logistics operator confirms that physical goods for shipment are those described in the documentation.</p>

3.	<p>Customs agents inspect doré and paperwork, then take samples to levy excise tax.</p> <p>Risks Identified:</p> <ul style="list-style-type: none"> • Lack of transparency promotes corruption. 	<p>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.</p>
4.	<p>Logistics operator delivers the shipment to the refinery.</p>	
5.	<p>Refiner receives the shipment and compares actual delivery against expected (via documentation from miner and customs agents).</p> <p>Observer watches unpacking, weighing, and sampling procedure on behalf of the miner.</p> <p>The miner is alerted of any discrepancies.</p>	<p>Refiner confirms that the physical goods in shipment are those described in the documentation from the miner and customs agents.</p> <p>Observer documents that receiving process complies with the contract between miner and refiner and attests that appropriate procedures were followed.</p>
6.	<p>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.</p> <p>Risks Identified:</p> <ul style="list-style-type: none"> • 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. 	<p>Refiner documents refining and sales processes in different in-house systems.</p> <p>Refiner communicates shipment details to logistics operator.</p>
7.	<p>Logistics operator delivers the shipment to the vault.</p> <p>Risks Identified:</p> <ul style="list-style-type: none"> • Counterfeit bullion is introduced during transport. 	<p>Logistics operator confirms that physical goods for shipment are those described in the documentation.</p>

8.	<p>Vault takes custody of and vaults bullion. Vault confirms receipt with end customer.</p> <p>Risks Identified:</p> <ul style="list-style-type: none"> • 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. 	<p>Vault confirms that physical goods for shipment are those described in the documentation.</p>
----	---	---



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.

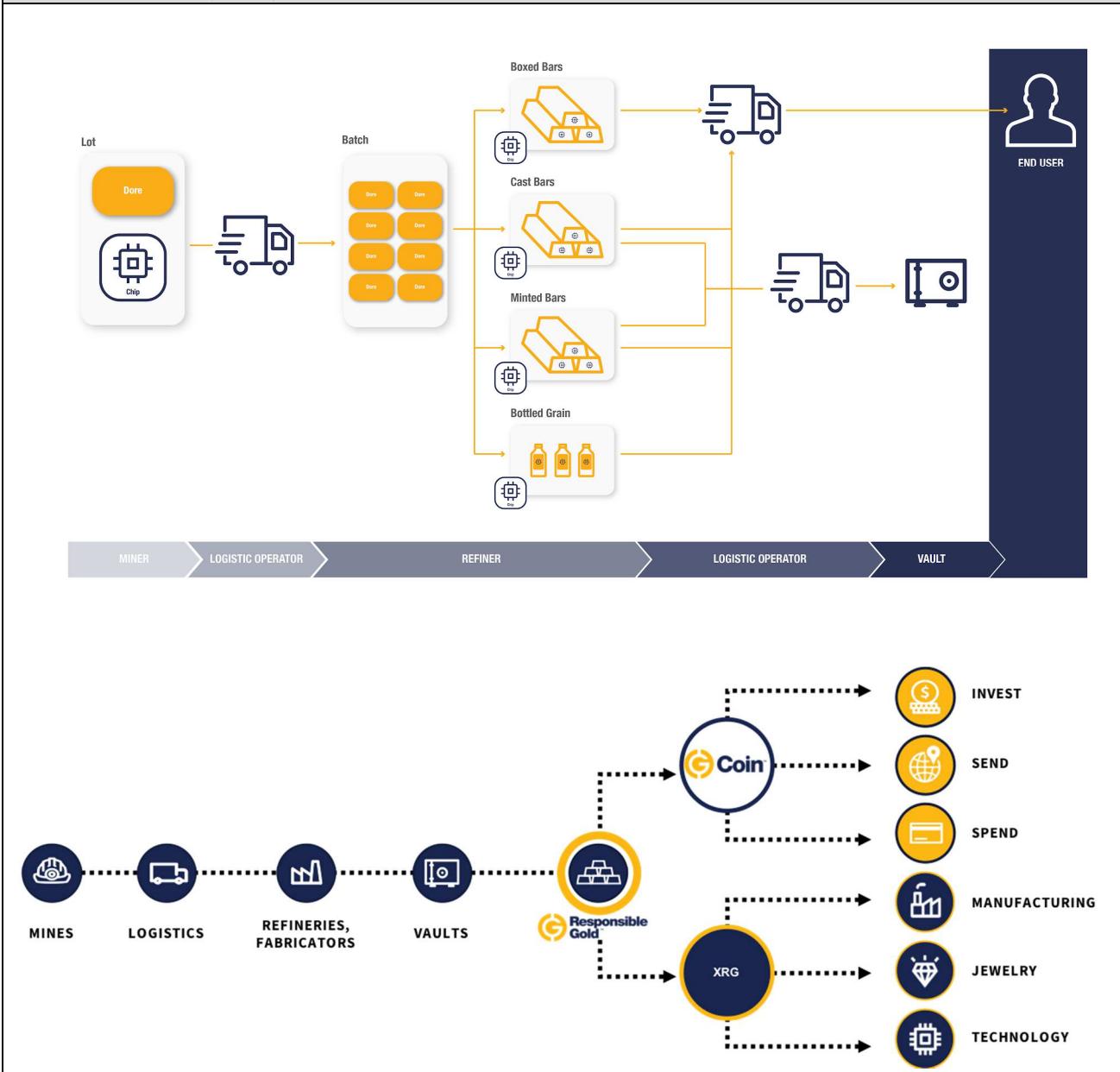
Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	<p>Miner pours molten ore into doré bars. Each bar is imprinted with a serial number, and its weight and assays are collected and documented.</p> <p>Miner readies the shipment for transport by packaging and sealing each bar.</p> <p>New Process:</p> <ul style="list-style-type: none"> • Miner implements Responsible Gold Standards and is audited against compliance annually. 	<p>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.</p> <p>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.</p>
2.	<p>Logistics operator arrives, takes custody of the shipment and transports the shipment to the customs agents.</p> <p>New Process:</p> <ul style="list-style-type: none"> • Logistics operator implements Responsible Gold Standards and provides a self- 	<p>Logistics operator takes custody of each asset by using the RG SCA to scan each cryptobelt.</p> <p>Logistics operator confirms that physical goods for shipment are those described in the RG SCA and documented on the distributed ledger.</p>

	<p>certification of compliance annually.</p> <ul style="list-style-type: none">• Human and AI auditors compare timestamps of custody transfers against expectations and flag any significant deviations for investigation.	
3.	<p>Customs agents inspect doré and paperwork, then take samples to levy excise tax.</p> <p>New Process:</p> <ul style="list-style-type: none">• 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.	<p>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.</p>
4.	<p>Logistics operator delivers the shipment to the refinery.</p>	
5.	<p>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.</p>	<p>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.</p>
6.	<p>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.</p> <p>New Process:</p> <ul style="list-style-type: none">• Refiner adopts the Responsible Gold Standards and is audited for compliance annually.	<p>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.</p> <p>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.</p> <p>Refiner places GoldID-registered bullion into a shipping container. Using the RG SCA, the</p>

	<ul style="list-style-type: none">• 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.	<p>refiner registers the shipping container with a new cryptobelt. This registers on the distributed ledger that the shipping container has been packed and sealed.</p> <p>The refiner initiates a transfer in the RG SCA to the logistics operator.</p>
7.	<p>Logistics operator delivers the shipment to the vault.</p> <p>New Process:</p> <ul style="list-style-type: none">• GoldID prevents substitution of counterfeit bars.	<p>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.</p>
8.	<p>Vault takes custody of and vaults bullion. Vault confirms receipt with end customer.</p> <p>New Process:</p> <ul style="list-style-type: none">• Vault agrees to Responsible Gold Standards and provides a self-certification of compliance annually.• GoldID prevents receipt of counterfeit bars.	<p>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.</p>

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:	<i>Vertical</i>
Submission Date:	March 29, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Traceability in the food supply chain in Brazil	Domain:	<i>Supply chain management</i>
Status of Case	<i>Pilot</i>	Sub-Domain	<i>Agriculture; Data processing, storage and management</i>
Contact information of person submitting/managing the use-case	<i>Rodrigo Lima Verde Leal rodleal@cpqd.com.br @cpqd https://www.linkedin.com/company/cpqd/</i>	<i>Innovation and Product Marketing +55 19 3705 5994 https://www.cpqd.com.br</i>	
Proposing Organization	<i>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</i>		
Short Description	<p>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.</p>		
Long description	<p>This Pilot is the first step for providing provenance and quality information to all relevant stakeholders in 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 bypassing all stakeholders in the supply chain, from producers to retailers, that is both safe and reliable.</p> <p>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.</p> <p>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.</p> <p>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.</p>		

	The development framework is Hyperledger Fabric, maintained by The Linux Foundation.		
SDG in Focus (when applicable)	<p><i>SDG 2: 2.4</i></p> <p><i>SDG 3: 3D</i></p> <p><i>SDG 8: 8.6 and 8.7</i></p> <p><i>SDG 12: 12.3, 12.6 and 12.A</i></p> <p><i>SDG 15: 15.1, 15.2, 15.5</i></p>		
Value Transfer:	Assets (<i>cattle</i>)	Number of Users:	<i>14 meatpackers and 1 retailer</i>
Types of Users:	<i>Farmer, Meatpacker, Retailer, Consumer, Traceability System Provider</i>		
Stakeholders	<i>NGO, Government</i>		
Data:	<p><i>Regarding what data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc:</i></p> <ul style="list-style-type: none"> ● <i>Identity of individual animals and animal batches.</i> ● <i>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).</i> ● <i>No data is stored in the DLT, only hashes, thus allowing for all participants to share registers on the ledger without exposing sensitive information.</i> <p><i>Regarding how the DLT solution would interact with external data and other systems:</i></p> <ul style="list-style-type: none"> ● <i>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.</i> 		
Identification:	<i>This Pilot does not work with pseudonyms. Full identification of relevant stakeholders participating in the network are required by the Traceability System Provider.</i>		
Predicted Outcomes:	<p>The predicted outcomes of adopting new processes based on this system are:</p> <ul style="list-style-type: none"> ● 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.

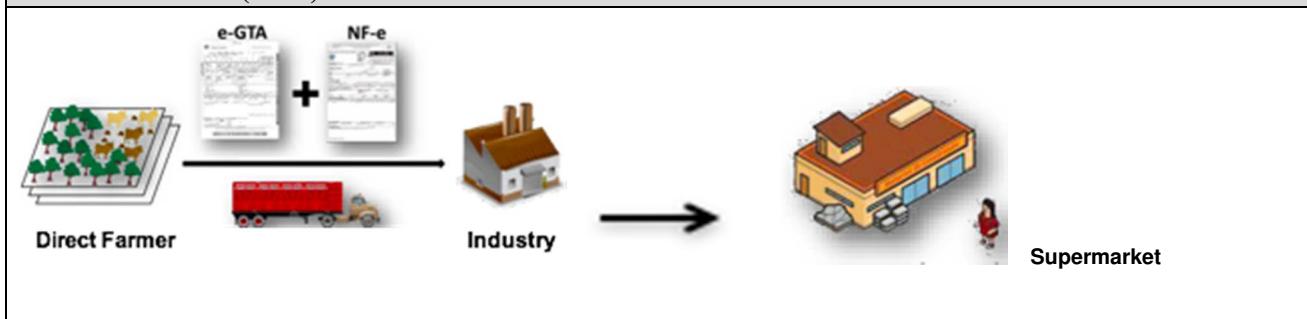
In such solutions, farmers and meatpackers are responsible for inserting their own information in the traceability system, bringing only partial information to the beef supply chain.

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)



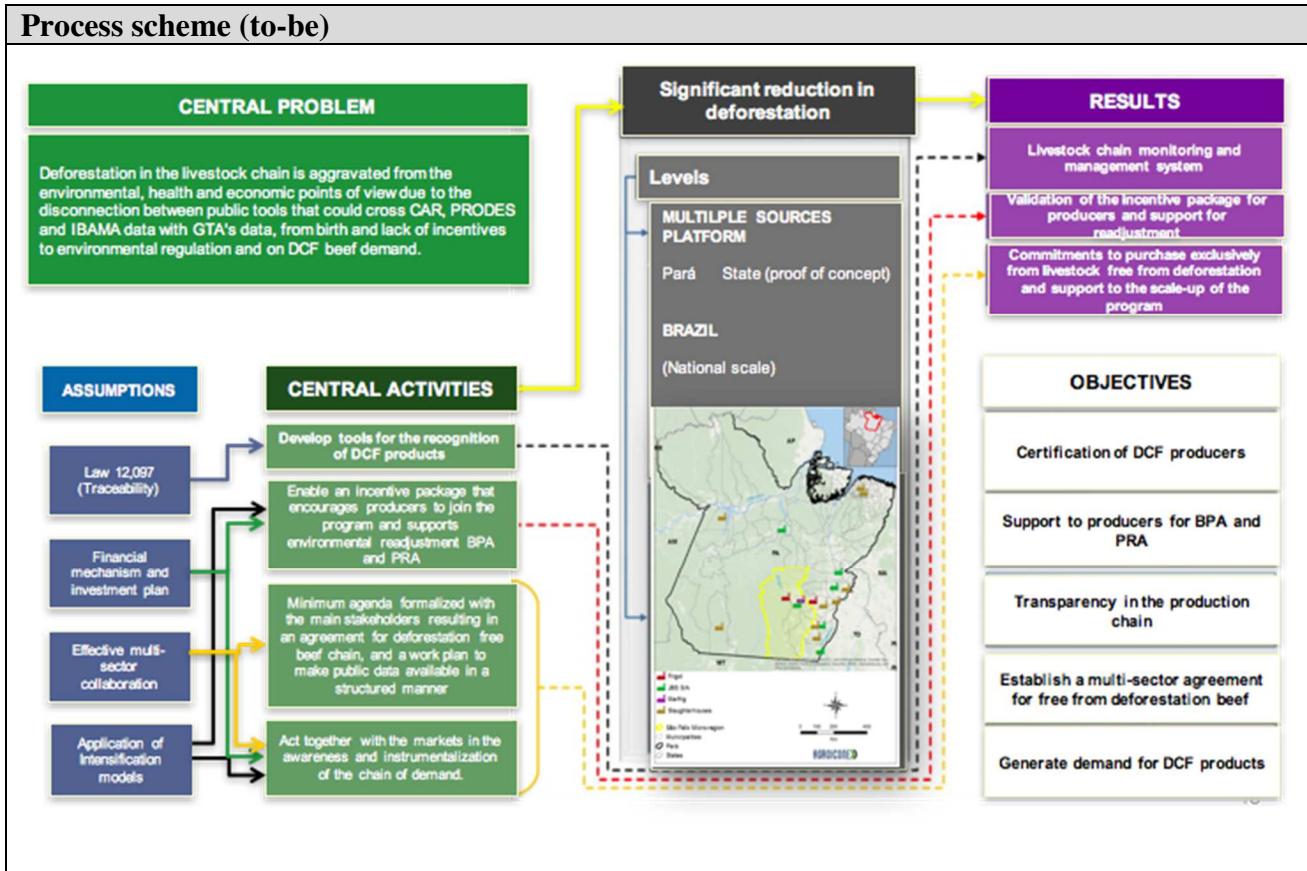
Data and information (as-is)		
Data	Type	Description
1	<i>Documents and supply chain data</i>	GTA, Invoices (buyer, seller), geomonitoring data, logistics data (boxes and pallets identifiers etc).

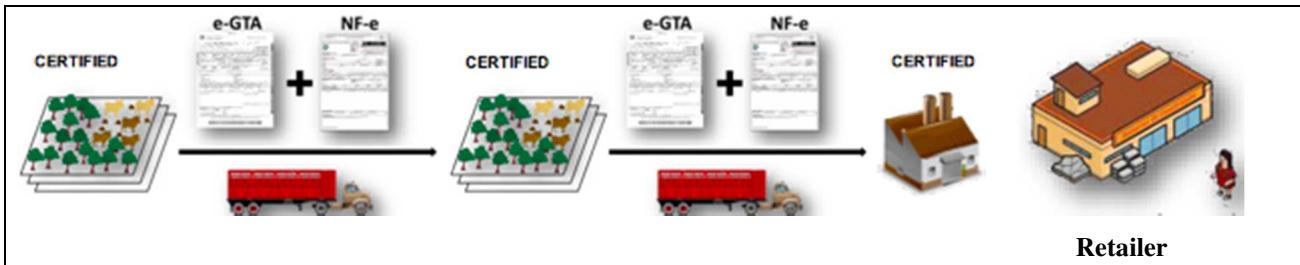
Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Farmer</i>	Generates invoices (Nota Fiscal) and GTA when a sale is made to the metapacker.
2	<i>Meatpacker</i>	Buys animals, verifies socio-environmental info, provides production traceability data.
3	<i>Retailer</i>	Put pressure on meatpackers to make them compliant to legislation and agreements with the Public Ministry.
4	<i>Consumer</i>	Transparency.
5	<i>Traceability System Provider</i>	Gathers information and generates evidences for auditing.
6	<i>NGO</i>	Supervises and demand transparency.
7	<i>Government</i>	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	<p>Manages its ID, inputs information on good production practices and monitors data on its risk level, calculated from sanitary and social-environmental information.</p> <p>Applicable to all production chain (farmer that sells animals to another farmer) and not only the farm that sells directly to the meatpacker.</p>
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.





Participants and their roles		
Actor	Type/Role	Description
1	<i>Farmer</i>	Will provide more information and engage other producers that are not part of the sustainable food chain.
2	<i>Meatpacker</i>	Will provide more information and engage other meatpackers that are not part of the sustainable food chain.
3	<i>Retailer</i>	Will provide access to suppliers from other food chains.
4	<i>Consumer</i>	Will have access to transparent traceability from deforestation free suppliers.
5	<i>Traceability System Provider</i>	Will expand its clients number and ticket.
6	<i>NGO</i>	May become observer nodes.
7	<i>Government</i>	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	<i>Documents and supply chain data</i>	GTA, Invoices (buyer, seller), geomonitoring data, logistics data (boxes and pallets identifiers etc).
2	<i>Government databases</i>	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.		

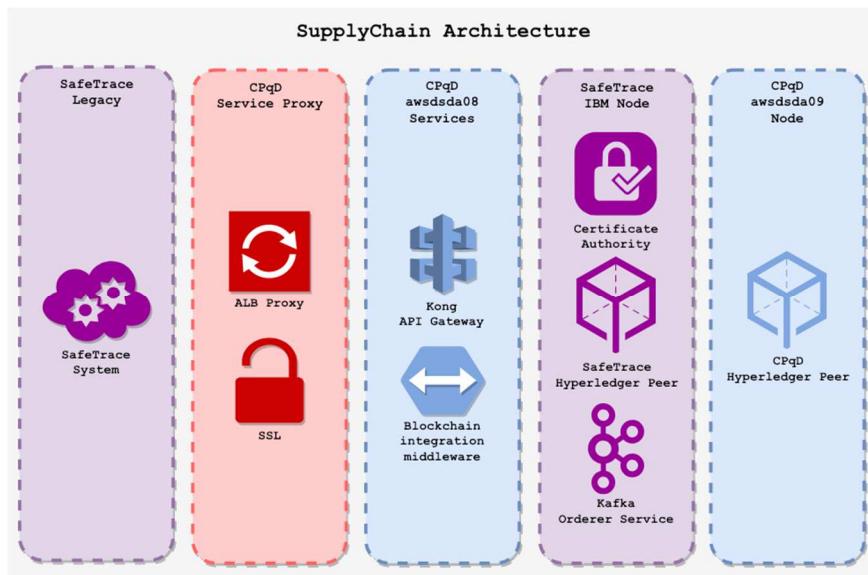
4. DLT should be available 24/7/365.

Main Success Scenario + expected time line

DLT-based solution that registers events that occurred 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

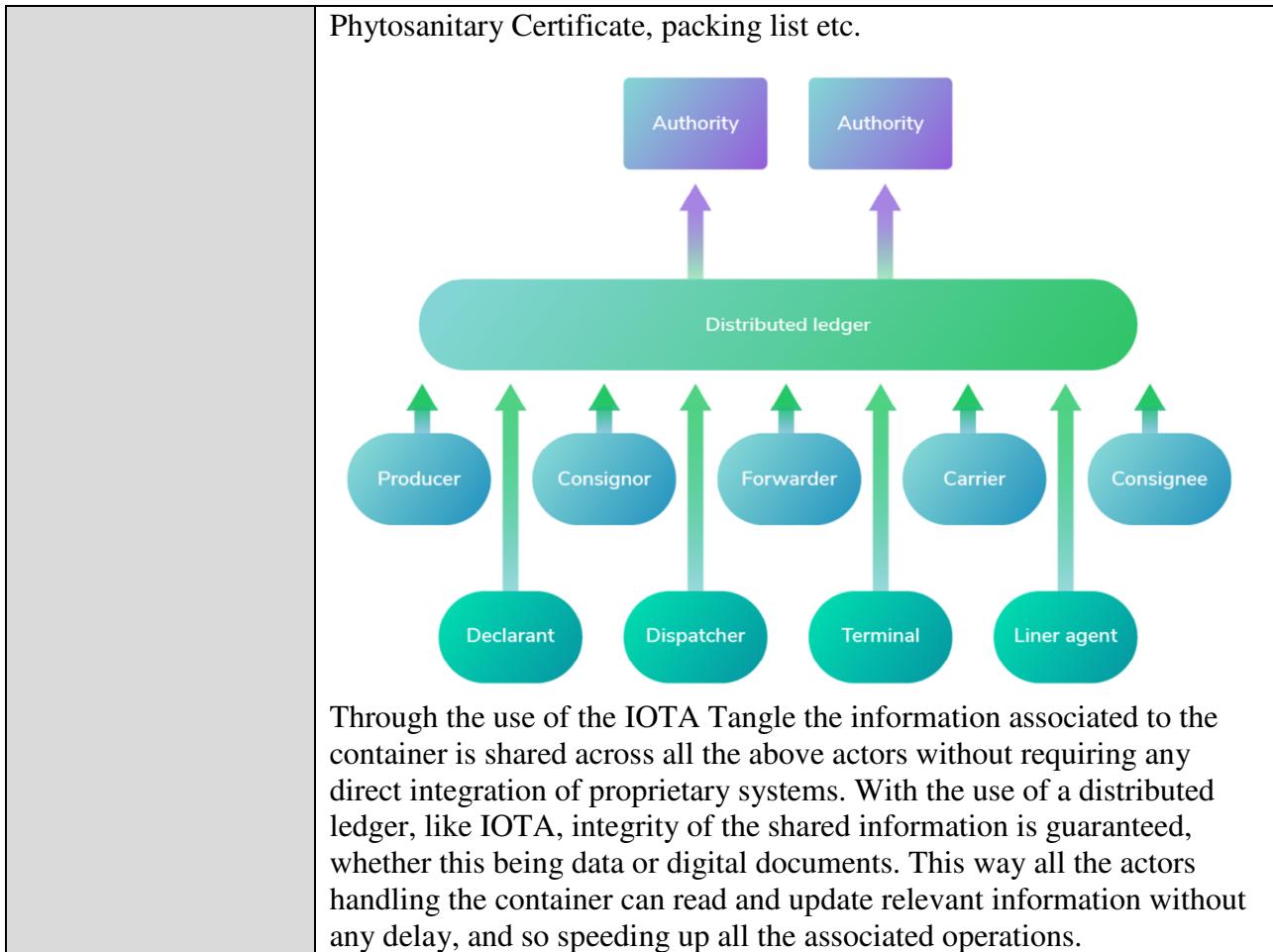
Trade Facilitation and Customs Management

Section 1: Summary

Use Case Summary			
Use Case ID:	IND-008	Use Case Type:	<i>Vertical</i>
Use Case Title:	Trade facilitation and customs management	Is Use Case supporting SDGs	<i>No</i>
		Domain:	Industry/Supply Chain
Status of Case	<i>Proof of Concept</i>	Sub-Domain	
Contact information of person submitting	Full Name: <i>Lewis Freiberg</i> Job Title: <i>Director of Ecosystem</i> E-mail address: lewis@iota.org Telephone number: <i>+1 443 693 7730</i> Social media: Web site: https://iota.org		
Proposing Organization	IOTA Foundation, Germany Organisation ID: 3416/1234/2		
Short Description	<p>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.</p>		
Long description	<p>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:</p> <ul style="list-style-type: none"> ● 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). <p>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.</p>		
SDG in Focus (when applicable)	<i>None as of yet</i>		
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		

	<p>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.</p> <pre> graph TD Shipper((SHIPPER)) -- "REGISTER CONTAINER" --> Forwarders1((FORWARDERS)) Forwarders1 -- "REGISTER CUSTODY / UPDATE STATUS" --> Ledger((IOTA LEDGER)) Forwarders1 -- "REGISTER CUSTODY / UPDATE STATUS" --> PortAuth((PORT AUTHORITIES)) PortAuth -- "REGISTER CUSTODY / READ AND UPDATE STATUS" --> Ledger PortAuth -- "REGISTER CUSTODY / READ AND UPDATE STATUS" --> Customs((CUSTOMS)) Customs -- "REGISTER CUSTODY / UPDATE STATUS" --> Ledger Customs -- "REGISTER CUSTODY / UPDATE STATUS" --> EndCustomer((END CUSTOMER)) EndCustomer -- "REGISTER CUSTODY / READ STATUS" --> Forwarders2((FORWARDERS)) Forwarders2 -- "REGISTER CUSTODY / UPDATE STATUS" --> Ledger </pre>
Data:	<p>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.</p> <p>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.</p> <p>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.</p>
Identification:	<p>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 correctly 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.</p>

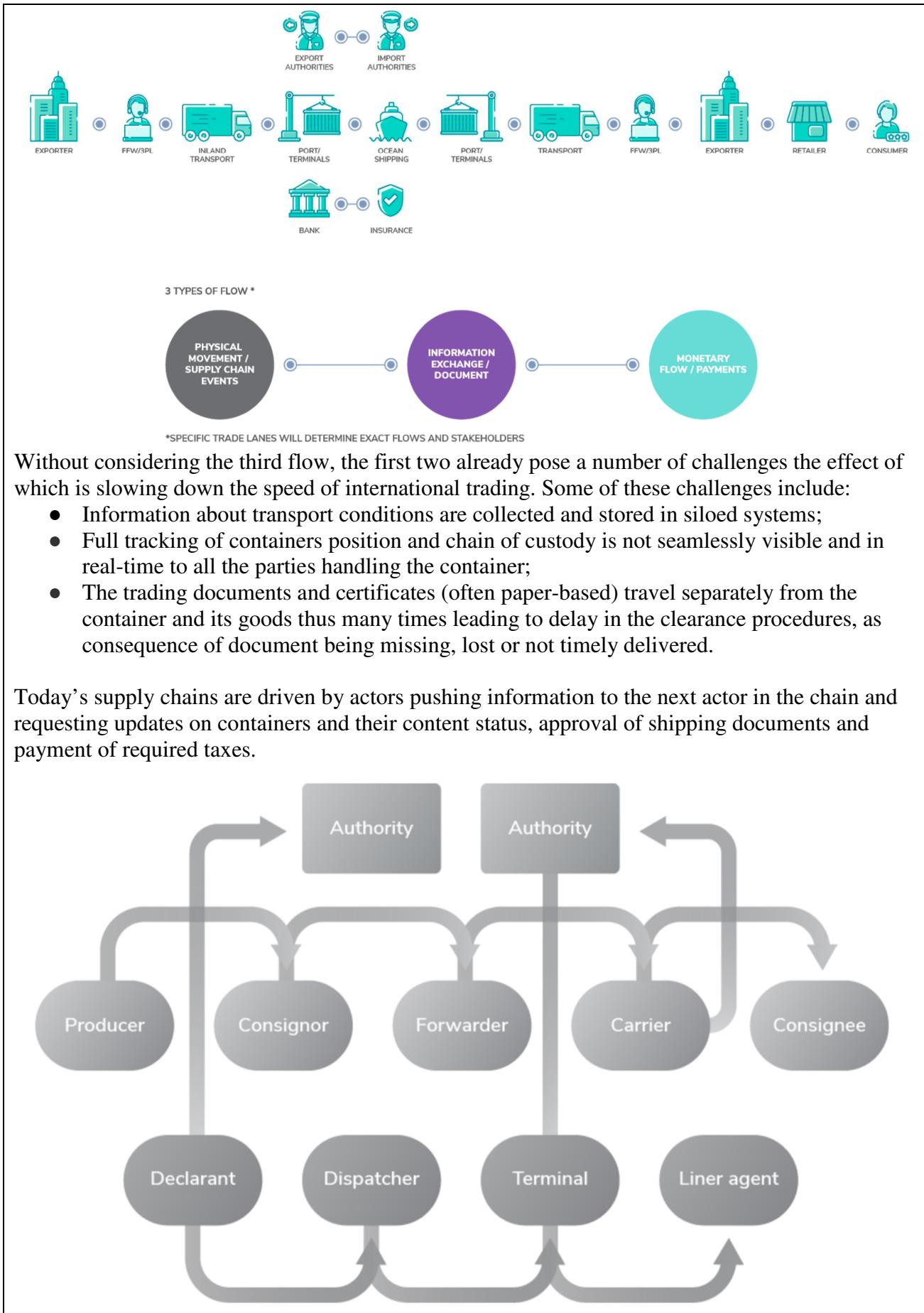
	<p>Given the large complexity of this, identity verification is out of scope for the proof of concept at this point. What the PoC does do is ensure once an actor engages with the shipment, all subsequent transactions that are related can be verified as coming from the same entity. However at the moment 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.</p>
Predicted Outcomes:	<p>An IOTA powered data exchange layer for trade can deliver the following benefits for each stakeholder category.</p> <p>For shippers:</p> <ul style="list-style-type: none">● 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. <p>For customs clearance :</p> <ul style="list-style-type: none">● 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. <p>For port authorities and freight forwarders:</p> <ul style="list-style-type: none">● 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. <p>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.</p> <p>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,</p>



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.



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	<i>Documents</i>	

2	<i>Payment transactions</i>	
---	-----------------------------	--

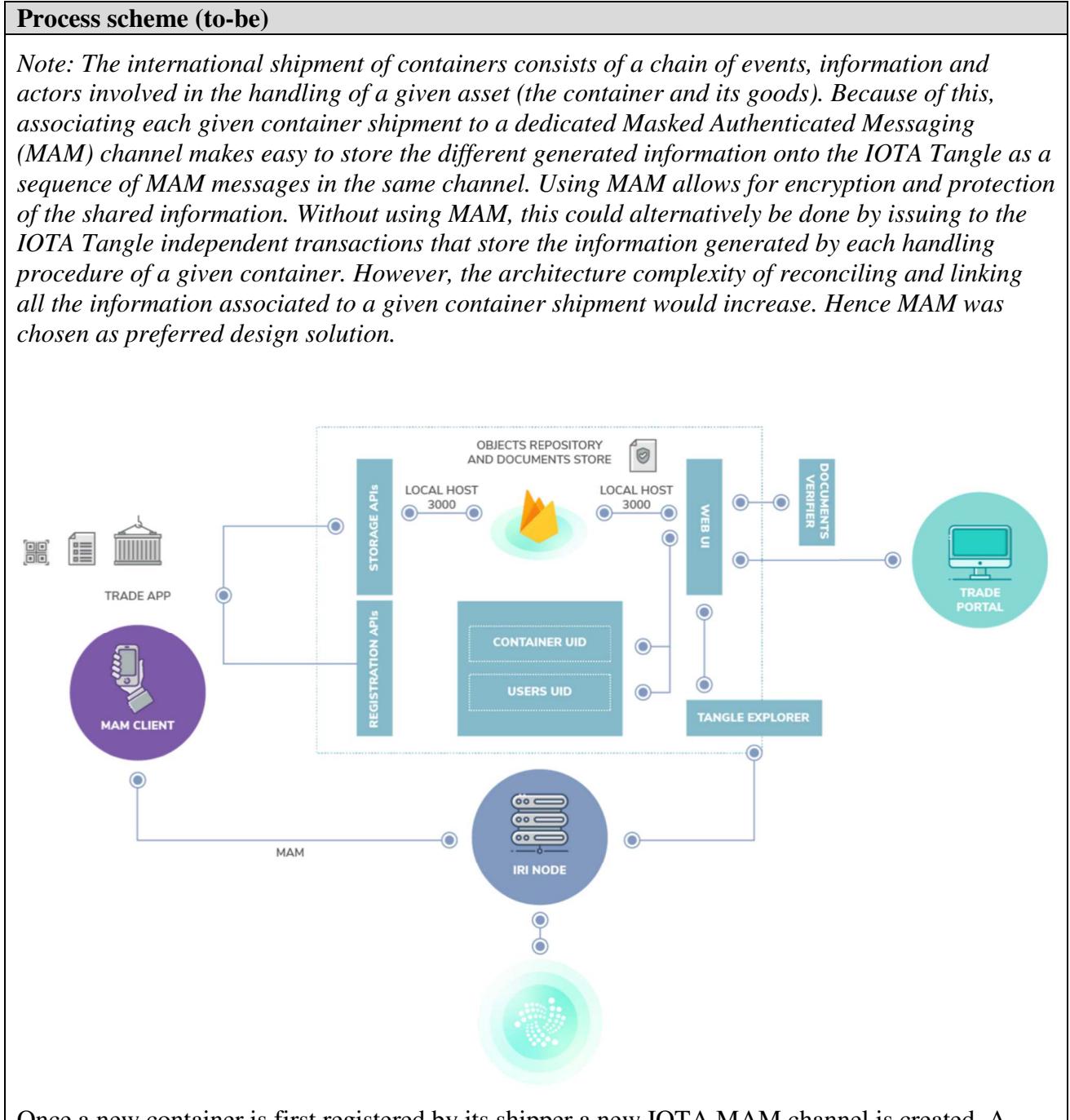
Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Lawyers</i>	
2	<i>Bank</i>	

Other Notes
<i>Any assumptions, issues</i>

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,	<p>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).</p> <p>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;</p>
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 clearance 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).



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 is 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);

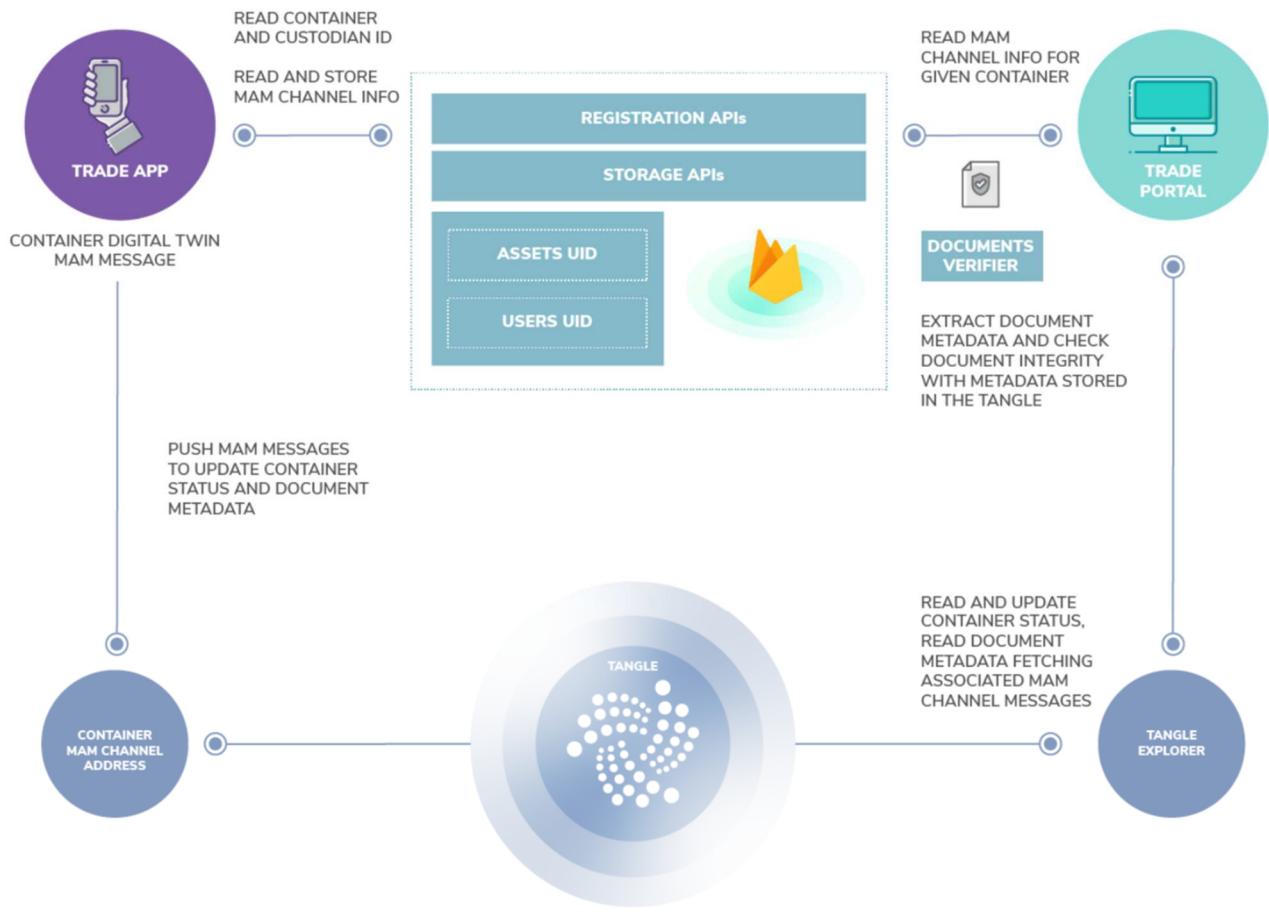
have been implemented in order to respectively access and update existing MAM channel information (e.g. adding new messages to update the stored digital twin). Information is then attached to the correct MAM channel and stored immutably onto the IOTA Tangle.

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	<i>Digital Twin</i>	<p>This is the data representation of the Digital Twin used in the trade facilitation PoC:</p> <pre> "data": [{ "containerUniqueID": "number", "containerOwnerID": "string", "containerUserID": "number", "location": "string", "temperature": "number", "time": "date", "documents": [{ "link": "string", "hash": "string" }], "status": "string" }] </pre>

Security and privacy
<p>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.</p> <p>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</p>

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:	<i>Industry/3 and 4</i>
Submission Date:	January 4, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Polo Multimodal Pecem	Domain:	<i>List 1 Appendix 1</i>
Status of Case	<i>Proof of Concept (POC)</i>	Sub-Domain	<i>Supply chain management</i>
Contact information of person submitting/managing the use-case	<p><i>Ingrid Barth Chief Blockchain Officer</i> <i>E-mail address: ingrid@cosmosblockchain.co</i> <i>Telephone number: 11 983615309</i> <i>Social media: https://www.linkedin.com/in/ingrid-barth-48a17b19/</i> <i>Web site: http://www.polomultimodal.com/</i></p>		
Proposing Organization	<p><i>Polo Multimodal Pecem</i> Fotaleza (Ceará) - Brazil</p>		
Short Description	<p>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.</p>		
Long description	<p>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.</p>		
SDG in Focus (when applicable)	<p><i>8 – Decent Work and Economic Growth</i> <i>8.3 Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation,</i></p>		

	<i>and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services</i>		
Value Transfer:	<i>Security in shipping and transportation processes, possibility to reduce costs and security for the goods.</i>	Number of Users:	<i>All companies and people involved. The Pecem Port is growing about 34% year.</i>
Types of Users:	<i>Companies, society, employees, Pecem port</i>		
Stakeholders	<i>Companies, society, employees, Pecem port</i>		
Data:	<i>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.</i>		
Identification:	<i>Full identification of all participants, like company, employees, location, destination, goods to be transported.</i>		
Predicted Outcomes:	<p><i>The predicted outcomes of the adopting the new process are to:</i></p> <ul style="list-style-type: none"> - 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 company'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.

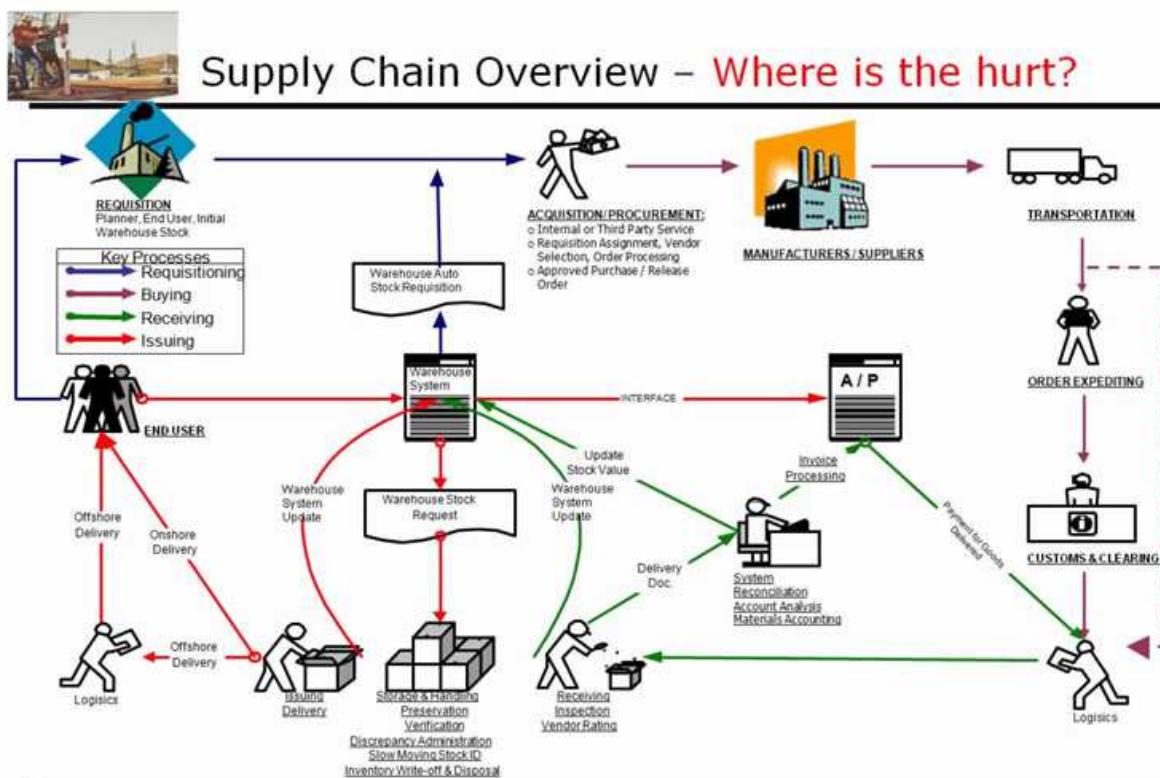
There is no problem to store data inside the company, but there are a lot of fraud cases in this manual process. Also, is very difficult identify the phase that a problem happened, the number of steps is huge, so if you can register phases in an immutable DLT, for sure they can find and fix problems 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	<i>Documents</i>	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	<i>Payment transactions</i>	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	<i>Buyer</i>	People or company that want to buy the goods. Can be inside the country, in other city, or other country.
2	<i>Seller</i>	Entity who sells a product or service to the buyer
3	<i>Bank</i>	Financial institution to provide transfer/payment between parts
4	<i>Shipping companies</i>	Companies that provide shipping services
5	<i>Insurance companies</i>	Companies that provide insurance for goods to be transported.

Other Notes
<p><i>Important to 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.</i></p>

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	<i>Buyer</i>	People or company that want to buy the goods. Can be inside the country, in other city, or other country.
2	<i>Seller</i>	Entity who sells a product or service to the buyer
3	<i>Bank</i>	Financial institution to provide transfer/payment between parts
4	<i>Shipping companies</i>	Companies that provide shipping services
5	<i>Insurance companies</i>	Companies that provide insurance for goods to be transported.

Data and information		
Data	Type	Description
1	<i>Documents</i>	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	<i>Payment transactions</i>	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
<ol style="list-style-type: none">1. Information will be encrypted, DLT/ Blockchain system will not keep 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
<p>Registration process to avoid frauds or improve logistics problems. benefits data published without human intervention.</p> <p>Expected time line – End of 2019</p>

Conditions (pre- or post-)
<ol style="list-style-type: none">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](https://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain)

Other Notes

N/A

Public Key Infrastructure: DLT based Decentralized Public Key Infrastructure System

Section 1 Summary

Use Case Summary			
Use Case ID:	SEM-002	Use Case Type:	Horizontal
Use Case Title:	DLT based Decentralized Public Key Infrastructure System	Is Use Case supporting SDGs	<i>Yes</i>
Status of Case	Proof of Concept	Domain:	Security Management
Contact information of person submitting/managing the use-case	<i>Xinpeng Wei</i> <i>Bingyang Liu</i>	wexinpeng@huawei.com liubingyang@huawei.com	
Proposing Organization	<i>Huawei</i>		
Short Description	PKI, Public Key Infrastructure, acts as the trust foundation in many scenarios, but the current hierarchical PKI system faces the problem of single point of failure. This document describes how to build a decentralized PKI system.		
Long description	<p>A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.</p> <p>Currently the PKI system is built in a hierarchical mode, one root CA exist at the top of the system and several intermediate CAs at lower level. The security of the whole system based on the security of root CA, if root CA is corrupted or misbehavior then the whole system fails.</p> <p>By using DLT, a decentralized PKI system can be built without highly centralized root CA, and avoid the single point of failure problem.</p>		
SDG in Focus (when applicable)	<p>Goal 9: Industry, Innovation and Infrastructure</p> <p>9.3 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.</p>		
Value Transfer:	token	Number of Users:	Tens of thousands
Types of Users:	ISP, OTT, web user, enterprise, bank, government...		
Stakeholders	certificate authority, anyone needs a certificate		

Data:	1. Token account 2. Digital certificate related information (e.g. Identity, application specific information, cryptographic-related information etc.) 3. Smart contract, including running code for PKI-related operations
Identification:	Both anonymous Identification and identifiable identification should be supported.
Predicted Outcomes:	A decentralized PKI system based on DLT.

Overview of the Business Problem or Opportunity

Currently the PKI system is built in a hierarchical mode, one root CA exist at the top of the system and several intermediate CAs at lower level. The security of the whole system based on the security of root CA, if root CA is corrupted or misbehavior then the whole system fails.

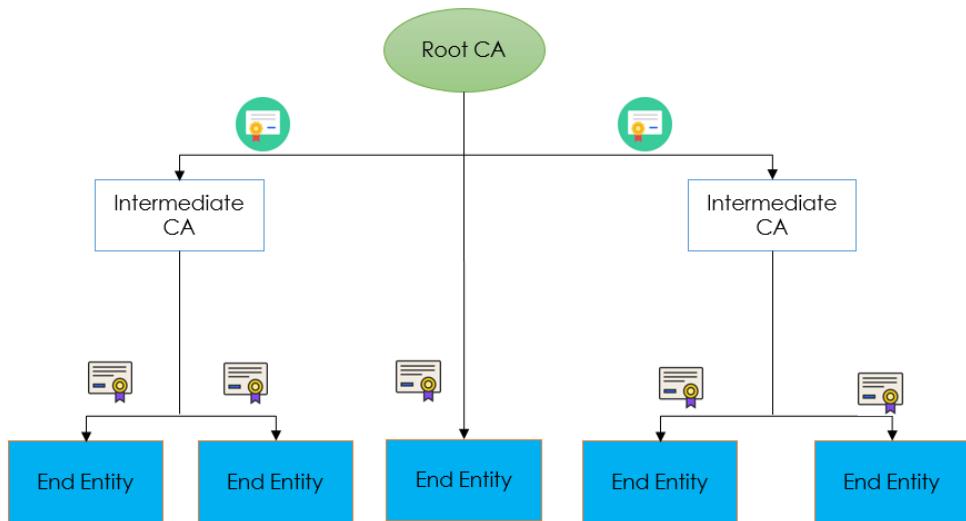


Figure 1: Centralized and Hierarchical Public Key Infrastructure

Why Distributed Ledger Technology?

The distributed and unaltered features of DLT make it easy to build a decentralized system on it, and especially its support of smart contract makes it possible to issue the digital certificate fully automated.

Section 2 Current process

Current Solutions

Certificate Transparency is a solution that can, to a certain extent, mitigate risk caused by mistakenly issued certificates or certificates that have been issued by a certificate authority (CA) that's been compromised or gone rogue.

Certificate Transparency aims to remedy these certificate-based threats by making the issuance and existence of SSL certificates open to scrutiny by domain owners, CAs, and domain users. Specifically, Certificate Transparency has three main goals^[1]:

- Make it impossible (or at least very difficult) for a CA to issue a SSL certificate for a domain without the certificate being visible to the owner of that domain.
- Provide an open auditing and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly or maliciously issued.
- Protect users (as much as possible) from being duped by certificates that were mistakenly or maliciously issued.

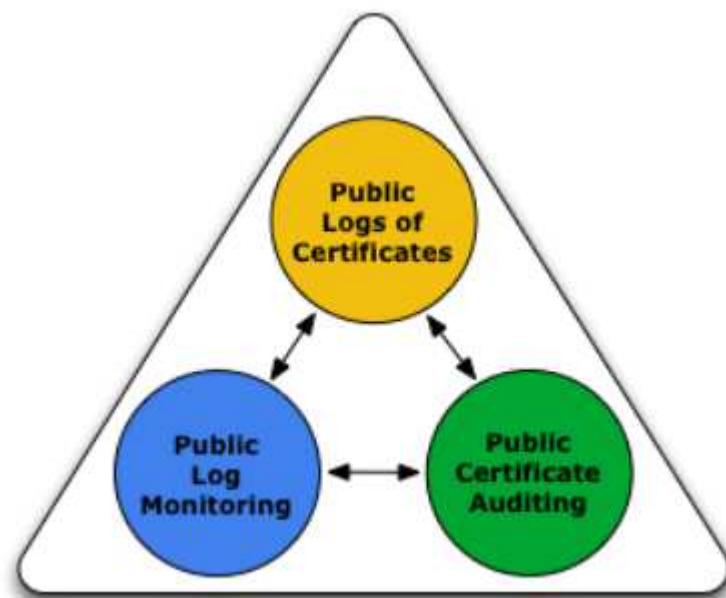


Figure 2: Basic Components of Certificate Transparency^[1]

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Certificate authority submit certificate to Log Server.	N/A
2.	Log Server provides a response to certificate authority to acknowledge the submission.	N/A
3.	Monitors watch logs for suspicious certificates and verify that all logged certificates are visible.	N/A
4.	Certificate owners query Monitors to verify that nobody has logged illegitimate certificate for their domain.	N/A

Existing Flow (as-is)		
Step	User Actions	System Actions
5.	Auditors verify that logs are behaving properly; they can also verify that a particular certificate has been logged.	N/A
6.	Monitors and Auditors exchange information about logs to help detect forked or branched logs.	N/A

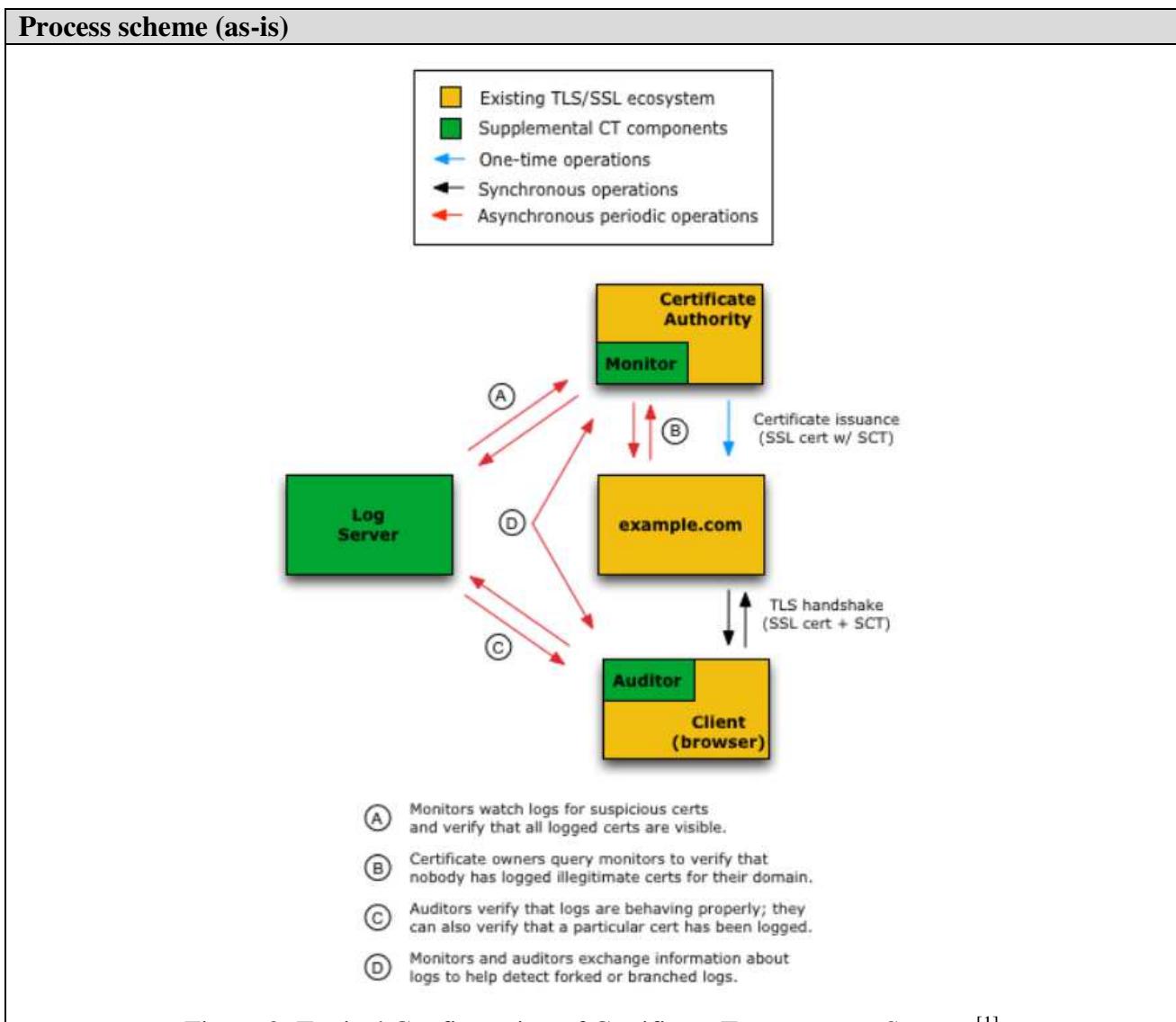


Figure 3: Typical Configuration of Certificate Transparency System ^[1]

Data and information (as-is)		
Data	Type	Description
1	Certificate	Certificates are stored in certificate Log Server.

Data and information (as-is)		
Data	Type	Description

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Log Server	Log Server is simple network services that maintain cryptographically assured, publicly auditable, append-only records of certificates
2	Monitors	Monitors are publicly run servers that periodically contact all of the log servers and watch for suspicious certificates.
3	Auditors	Auditors are lightweight software components that typically perform two functions.

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	End Entity apply for certificate from distributed ledger by sending transactions to specific smart contract.	The distributed ledger checks if the application from End Entity is acceptable, if true records the application request.
2.	Client verifies certificate base on the ledger.	The distribute ledger provides certificate-related information to the Client.

Process scheme (to-be)

There are three kinds of certificate:

DV certificate: Domain validated, the most common type of SSL certificate. They are verified using only the domain name.

OV Certificate: Organization validated, requiring more validation than DV certificates, but provide more trust. The organization's name is also listed in the certificate, giving added trust that both the website and the company are reputable. OVs are usually used by corporations, governments and other entities that want to provide an extra layer of confidence to their visitors.

EV Certificate: Extended validation, providing the maximum amount of trust to visitors, and also require the most effort by the CA to validate. As in the OV, the EV lists the company name in the certificate itself. However, a fully validated EV certificate will also show the name of the company or organization in the address bar itself, and the address bar is displayed in green.

The application of OV Certificate and EV Certificate needs endorsement from specific Endorser, but the application of DV certificate doesn't need endorsement. In order to cope with single point of failure problem for Endorser, the endorse procedure could be required endorsement from multiple Endorsers. The EV Certificate could always be used for domain validation purpose even in case the endorsement is corrupted.

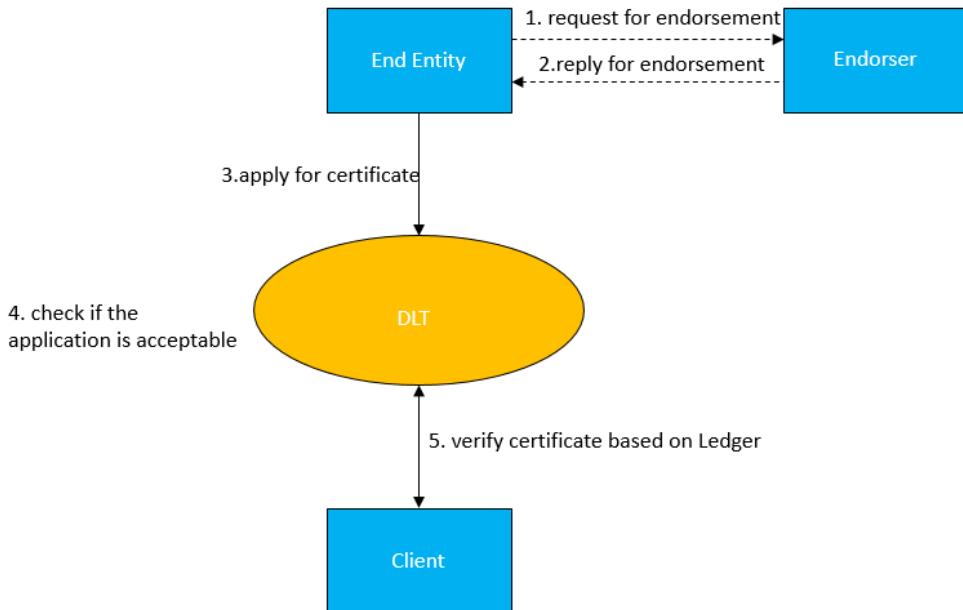


Figure 4: Procedure of DLT-based Public Key Infrastructure

Participants and their roles		
Actor	Type/Role	Description
1	End Entity	The entity that apply certificate from decentralized public key infrastructure.
2	Endorser	Providing endorsement for End Entity. The Endorser could be implemented as a smart contract in the ledger.

Participants and their roles		
Actor	Type/Role	Description
3	Client	The entity that verifies certificate in specific application scenario, e.g. web browser.

Data and information		
Data	Type	Description
1	Certificate-related information	Digital certificate related information (e.g. Identity, application specific information, cryptographic-related information etc.)
2	Certificate application transaction	End Entities use transactions to interact with the ledger.
3	Smart contract	Including running code for PKI-related operations.
4	Token account	Each End Entity has a token account in the ledger.

Security and privacy
1. The security of distributed ledger itself is very critical.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode.
2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way.
2. All parties are connected to DLT system.

Performance needs
1. Transactions processing near real time;
2. 24/7/365 availability;
3. Volume of transactions > 1000 TPS.

Legal considerations
N/A

Risks
1. DLT-related security risk.

Special Requirements

N/A

External References and Miscellaneous

[1] <http://www.certificate-transparency.org/what-is-ct>

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)

Smart Contracts for Data Accountability and Provenance Tracking

Section 1 Summary

Use Case Summary			
Use Case ID:	DTM-001	Use Case Type:	<i>Horizontal</i>
Submission Date:	December 14, 2018	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Smart contracts for data accountability and provenance tracking	Domain:	<i>Data processing, storage and management</i>
Status of Case	<i>Proof-of-concept</i>	Sub-Domain	
Contact information of person submitting/managing the use-case	<p><i>Full Name:</i> Ricardo Neisse</p> <p><i>Job Title:</i> Scientific Project Officer</p> <p><i>E-mail address:</i> ricardo.neisse@ec.europa.eu</p> <p><i>Telephone number:</i> +39 0332 78 9592</p> <p><i>Social media:</i> https://twitter.com/EU_ScienceHub</p> <p><i>Web site:</i> https://ec.europa.eu/jrc/en</p>		
Proposing Organization	<i>European Commission Joint Research Center, Ispra, Italy</i>		
Short Description	<i>Smart contracts can be used to track data provenance and encode usage control policies regulating the access and usage (e.g., redistribution) of subject's data by controller and processors.</i>		
Long description	<p><i>The recent approval of the General Data Protection Regulation (GDPR) imposes new data protection requirements on data controllers and processors with respect to the processing of European Union (EU) residents' data. These requirements consist of a single set of rules that have binding legal status and should be enforced in all EU member states. In light of these requirements, this use case propose the use of a blockchain-based approach to support data accountability and provenance tracking. This approach relies on the use of publicly auditable smart contracts deployed in a blockchain that increase the transparency with respect to the access and usage of data. Smart contracts can be used to encode data usage policies and provenance tracking information in a privacy-friendly way.</i></p>		
SDG in Focus (when applicable)	<i>Goal 16: Promote just, peaceful and inclusive societies</i>		
Value Transfer:	<i>Fingerprints of digital identity and personal data items</i>	Number of Users:	<i>Large scale including citizens of many EU countries</i>
Types of Users:	<i>Data Subjects, Data Controllers, and Data Processors</i>		
Stakeholders	<i>Citizens, enterprises handling digital identity and personal data items, government institutions auditing privacy practices of enterprises.</i>		

Data:	<i>Fingerprints of pairs of data type and values exchanged between a data subject and data controller, including an obfuscated usage control policy regulating how the data should be used by the controller/processor.</i>
Identification:	<i>The use case proposes a privacy-friendly way of encoding identities, data and policies in a way that is still meaningful for auditability purposes. The only thing that can be learned is the structure of the policy specified by data subjects and no details about the data or restricted activities that can be performed by data processors and controllers.</i>
Predicted Outcomes:	

Overview of the Business Problem or Opportunity	
<i>Subjects provide data to controllers and processors and have no auditable way of verifying how their data is being processed, stored, and redistributed. In case of privacy violations reported by subjects controllers and processors should be able to prove the data is stored and processed according to the subjects' privacy requirements.</i>	
<i>Smart contracts can be used as an auditable way of encoding data provenance information and privacy requirements to enable subjects to evaluate who has accessed their data and the conditions for storage, processing, and redistribution of the data. In case subjects believe their privacy requirements are not being fulfilled they can revoke data access and usage rights using the blockchain. This provides a mechanism for legal compliance in the face of the new EU General Data Protection Regulation (GDPR). Since in public blockchains the smart contracts are readable by anyone the data provenance and accountability information should be encoded in a privacy friendly way.</i>	
Why Distributed Ledger Technology?	
<i>In traditional centralized ledgers data subjects have no way of auditing and verifying (1) the set of data accessed by data controllers and processors and (2) how the provided data is being used. The use case relies on the immutability, verifiability, and transparency of DLT.</i>	

Section 2 Current process

Current Solutions	
<i>Not available.</i>	

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

Process scheme (as-is)

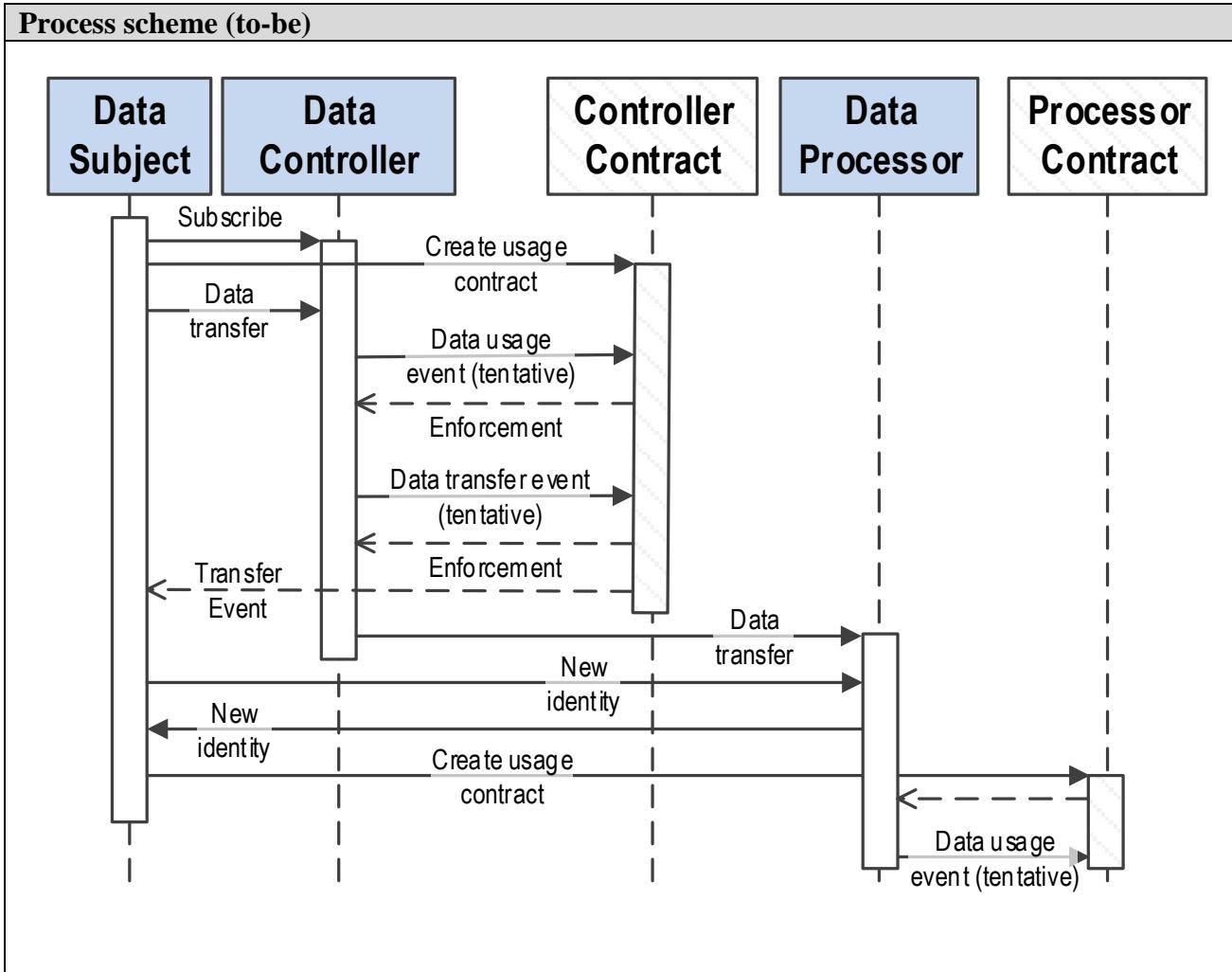
Data and information (as-is)		
Data	Type	Description

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

Other Notes

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	The data subject subscribes with the data controller and provides the list of data types/values that are exchanged together with an usage control policy.	A data usage contract is created in the blockchain using a random nonce and fingerprints for the identities, data items (types/values) and usage control policies associated to the data items.
2.	The data subject transfer data to the data controller.	The data controller stores the data and a reference to the smart contract.
3.	The data controller is about to use the data for any internal activity.	The data usage contract is consulted to verify if the activity is allowed to be performed with the data item and an answer is returned (allow/deny/modify/delay data usage).
4.	The data is about to be transferred to a data processor.	The data usage contract is verified and if the transfer is allowed a new contract is created for the specific data processor. The cycle repeats the same for each data processor starting with step 1.



Participants and their roles		
Actor	Type/Role	Description
1.	<i>Data subject</i>	Any person providing data to a data controller/processor.
2.	<i>Data controller</i>	Any organization receiving data from a data subject.
3.	<i>Data processor</i>	Any organization receiving data from a controller to perform specific data processing activities.

Data and information		
Data	Type	Description
1.	<i>Subject, controller, and processor identities</i>	Unique identities for subjects, controller, and processor that are not re-used for other contracts in order to avoid linkability.
2.	<i>Data type and value fingerprints</i>	Fingerprints of data types and values using a one-way hash function in combination with a random nonce to prevent dictionary attacks.

Data and information		
Data	Type	Description
3.	<i>Usage control policy</i>	An Event-Condition-Action policy specifying the data usage event, the condition, and the respective action (allow, deny, modify, delay, or execute).

Security and privacy
<p><i>The data items and identities stored in the blockchain are obfuscated to allow a privacy-by-design approach for the use case.</i></p>

Main Success Scenario + expected time line
<p><i>The main success scenario is a public blockchain where all data subjects are able to record and audit the data exchanged with data controllers and processors including their usage control policies in a privacy friendly way.</i></p> <p><i>There is currently no expected time line since this is a research prototype.</i></p>

Conditions (pre- or post-)
<p><i>Subjects provide data to controllers and processors and have no auditable way of verifying how their data is being processed, stored, and redistributed. In case of privacy violations reported by subjects controllers and processors should be able to prove the data is stored and processed according to the subjects' privacy requirements.</i></p> <p><i>Smart contracts can be used as an auditable way of encoding data provenance information and privacy requirements to enable subjects to evaluate who has accessed their data and the conditions for storage, processing, and redistribution of the data. In case subjects believe their privacy requirements are not being fulfilled they can revoke data access and usage rights using the blockchain. This provides a mechanism for legal compliance in the face of the new EU General Data Protection Regulation (GDPR). Since in public blockchains the smart contracts are readable by anyone the data provenance and accountability information should be encoded in a privacy friendly way.</i></p>

Performance needs
<p>In public blockchains, scalability is an issue considering the amount of data accessed, stored, and processed by many data controllers and processors. Maybe this approach is more viable for very sensitive data, for example, medical records.</p>

Legal considerations
<p><i>1. The goal of the use case is to support the implementation of the General Data Protection Regulation (GDPR)</i></p>

Risks
<p><i>No legal, business and technical risks related to use case were identified.</i></p>

Special Requirements

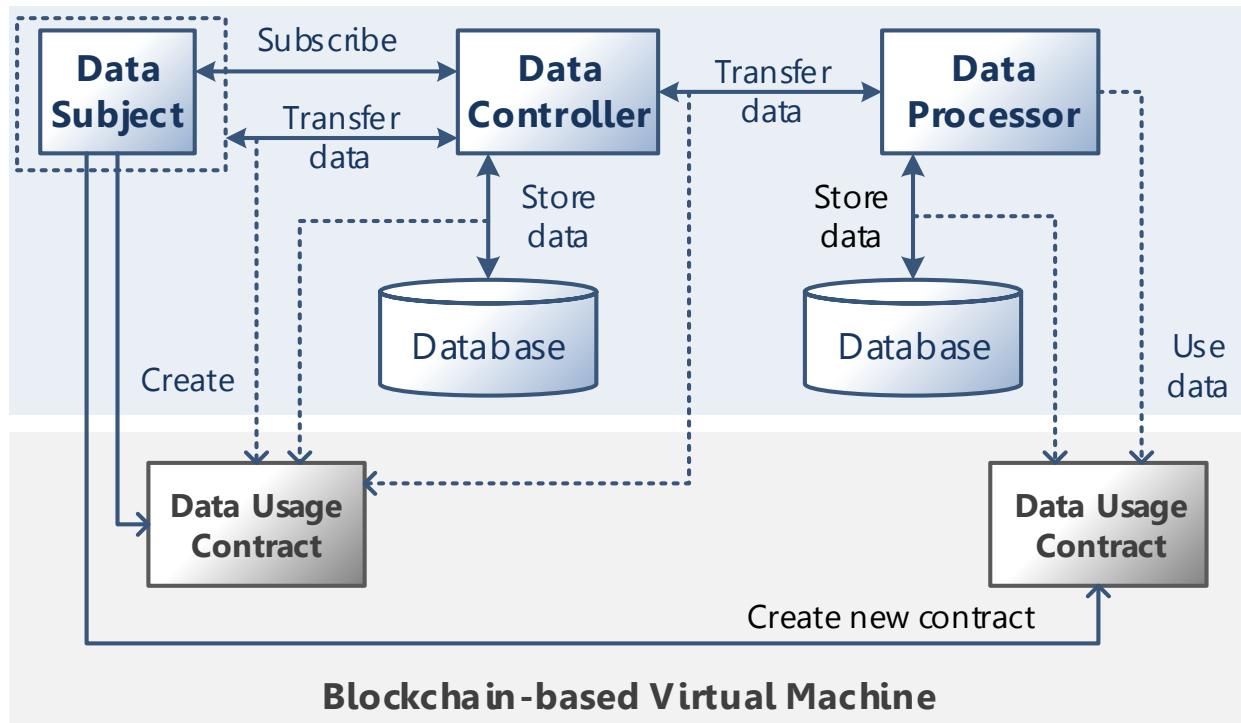
No special business and technical requirements of use case were identified.

External References and Miscellaneous

Ricardo Neisse, Gary Steri, and Igor Nai-Fovino. 2017. A Blockchain-based Approach for Data Accountability and Provenance Tracking. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). ACM, New York, NY, USA, Article 14, 10 pages. DOI: <https://doi.org/10.1145/3098954.3098958>

Other Notes

The following figure presents the high-level architecture of the data accountability and provenance tracking model proposed in this use case. In this architecture, three main entities are depicted following the GDPR terminology: the Data Subject, the Data Controller, and the Data Processor. When the subject subscribes with a controller, which is typically the role of a service provider, it creates a policybased Data Usage Contract specifying constraints on the usage and redistribution of any data obtained explicitly or implicitly by the controller. Explicit data is any data provided directly through interactions with the subject such as the e-mail addresses or birth date. Implicit data is any data acquired automatically, for example, sensor data from IoT devices in the environment surrounding the subject, data acquired by apps installed in mobile devices, or even server log files registering details of the network interactions between subject and controller services (e.g., IP addresses). The contract in this model acts as a data provenance tracker, policy evaluation entity, and event logger that allow the subject to easily check all data transfers and usage transactions providing assurance that only transactions conforming to the contract policies are authorized and registered in the blockchain.



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)

Lithopia: Engaging Stakeholders in Blockchain and Satellite Futures

Section 1: Summary

Use Case Summary					
Use Case ID:	ENT-001	Use Case Type:	Horizontal		
Submission Date:	March 14, 2019	Is Use Case supporting SDGs	Yes		
Use Case Title:	Lithopia: engaging stakeholders in blockchain and satellite futures	Domain:	Internet of Things		
Status of Case	PoC	Sub-Domain	Land Registries		
The contact information of the person submitting/managing the use-case	Full Name Denisa Reshef Kera Job Title Marie Curie Fellow E-mail address: denisa.kera@usal.es Telephone number: +34622631271 Social media: https://linkedin.com/in/denisakera/ https://usal.academia.edu/DenisaKera Web site: http://anonetted.net				
Proposing Organization	BISITE, University of Salamanca, Spain				
Short Description	Template of Hyperledger Fabric based service (chaincode) that uses satellite data as a trigger and explores stakeholder engagements in blockchain futures. The contract is featured in a design fiction parody of a “smart village,” but it can be utilized by activists reclaiming symbolic ownership of various resources on an NGOs operated ledger for mobilization through land-art performances.				
Long description	Lithopia https://github.com/anonetted/lithopia is a parody of a “smart” blockchain-managed village that uses open satellite data to trigger smart contracts on the Hyperledger Composer/Fabric. It reflects the current search for national cryptocurrencies and speculative investments in mining, such as ICOs or Lithium reserves in the Czech Republic. It is a functional prototype of a Node-RED interface/dashboard connected to the blockchain smart contracts on Hyperldger over a REST API service. It uses open data from Sentinel 2A Copernicus to change ownership of a location or a resource when covered by 10 x 10 m textile creating a pixel of data for the satellite. The project supports inclusive and democratic “future-making” (anticipatory governance) against the current misuses of emerging technologies in the so-called predictive, anticipatory and frictionless design. The villagers in Lithopia govern their affairs in an extremely transparent, but also aesthetic manner. Special long gestures and large LiCoins, but also acts of covering spaces in a land-art, Christo manner trigger the transactions. Lithopian DLT is inspired by Micronesian island of Yap that uses large stone coins to preserve their oral memory of ownership, marriages, and important events. Lithopians deploy smart contracts as a form of oral culture timestamping emphasizing genealogy over exchange and stewardship over ownership. The project is currently installed at the Milan design Triennial until September 2019.				

SDG in Focus (when applicable)	<p>Goal 1: end of poverty (1.4 supports ownership and control over land and other forms of property, inheritance, natural resources, appropriate new technology and financial services)</p> <p>Goal 9: resilient infrastructure (9.1, 9.3, 9a -c)</p> <p>Goal 11: inclusive and safe settlements and safeguarding of cultural and natural heritage (11.1, 11.3, 11.4, 11a)</p> <p>Goal 13: combat climate change (13.b)</p> <p>Goal 15: sustainable use of terrestrial ecosystems(15.6, 15.9)</p> <p>Goal 16: effective, accountable institutions (16.6, 16.7)</p>		
Value Transfer:	Assets changing ownership	Number of Users:	Users registered on the permissioned Hyperledger Fabric blockchain network (unknown limitations)
Types of Users:	Citizens, artists, activists		
Stakeholders	Investors, owners of a property, tenants, property management teams, public administration workers, indigenous groups		
Data:	<p>The contract includes human actors and external data from Sentinel 2A satellites and online services (Twitter, Weather, Cryptocurrency exchanges).</p> <ol style="list-style-type: none"> 1. Sentinel 2A data shared over an API service developed for the project (http://anonetted.net:8000/summary/). It updates on when is the satellite available in a given GPS location. It includes custom made visual recognition/tracking system searching for 1 pixel (10 x 10m) of red color data in a given location. 2. Human actor's data include identification data of participants in the blockchain network and assets. The Hyperledger Composer BNA (business network archive) includes cto file defining the users (participants), assets and the transactions (adding data from satellites and changing the ownership of an asset) in the JS script file. The ACL file them defines access control rules. The BNA data are available through a REST API (http://anonetted.net:3000/explorer/ - only authorized users). <p>Privacy is ensured by the Hyperledger Fabric blockchain structure of creation of different channels, where one needs the authorization to access any specific channel in the blockchain network achieved through the Certification Authority(CA) of the blockchain architecture.</p> <p>The interface to interact with the blockchain is Node-RED dashboard. Currently, you can add and see participants, properties and also types of partnerships. The DLT solution interacts with Twitter and external data over the dashboard (following weather data over open API and cryptocurrency exchanges influencing the decision to trigger the contracts).</p> <p>This PoC connecting satellite API with Hyperledger Composer REST API and Node-RED interface is currently stored only on one server with limited privacy and access for the developers and workshop participants.</p>		
	<p>The PoC is used in a design fiction project with fake participants and assets for testing purposes and as a tool to engage stakeholders in workshops. We plan to use identification mechanism offered by Hyperledger Composer Certification Authority and their channel tool. The participants are not anonymous.</p>		

Predicted Outcomes:	<ol style="list-style-type: none">1. Properties registered on the ledger symbolically change ownership through land-art mobilization and performance by individuals or group of citizens in front of the satellites at a given time.2. The dashboard informs the participants about the right time and weather condition to cover a given area and trigger the transaction. It also keeps a record of participants interested in a specific cause and the type of properties they try to own symbolically. It gives them tools (sentiment analysis of Twitter feeds and cryptocurrency exchange) to make the decisions.

Overview of the Business Problem or Opportunity
The tool is an opportunity for various stakeholders to understand and test the possibilities of Hyperledger based blockchain systems through a real near future scenario. It can also be used by NGOs and indigenous groups to reclaim symbolic ownership of natural resources or property by supporting an alternative ledger and a type of a ritual in front of the satellites. It is a tool to mobilize citizens to manage various resources which need stewardship by the commons or that have cultural and other value for a given group.
Why Distributed Ledger Technology?
Anticipatory governance of emerging DLT infrastructure is possible only if we involve a diversity of stakeholders to be part of the early development of a given technology. DLT, in this case, is a tool for stakeholder engagement over design fiction scenario with real prototypes. It has a potential to be used as a tool for public participation in the management of natural and other resources on a ledger operated by NGOs and various organizations interested in such land uses or to support the plea of indigenous population for symbolic ownership of their ancestral land etc. The solution offers a tool to understand and be part of the decision making about future infrastructure and to support the diversity of users. It also provides a dashboard allowing stakeholders to follow the use of such a tool in a design fiction or real scenario. It can enable immutability of records that concern ownership of property of natural resources and land and enable stakeholders to start important conversations about commons, climate exchange, and other pressing issues.

Section 2: Current process

Current Solutions
There are plans to use blockchain and satellite data in land registries with real-time data on conditions etc., but there are no PoC we could discuss. There is a company offering infrastructure for crypto-spatial coordinates that will support future services based on Ethereum https://foam.space/ , but no use cases, only a protocol. The existing blockchain satellite solutions work mainly on the issue of a resilient and alternative blockchain infrastructure, such as https://blockstream.com/satellite/ or https://spacechain.com/ . The independent space-based imagery and satellite data analytics companies (for example http://skylabanalytics.com/ , https://www.rezatec.com/ , https://www.planet.com/) offer aerial or satellite data collection platforms used for natural disasters monitoring, business intelligence, digital farming, real estate, retail and tourism intelligence, etc. None of them, however, uses or offers blockchain services. Their market is still rather niche, they have to educate their clients on the type of information, and automation satellite data offer. We claim that the blockchain solutions are necessary for satellite data because of the possible forgeries made by AI/machine learning algorithms that can simulate aerial images in the future. Furthermore, satellite data do not need to be only passive, but an active channel of communication and expression of communities and individuals through interventions. There are no current solutions that use

interventions on specific sites to generate satellite data except fake cardboard cutouts of planes and military gear in cases of military intelligence.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Satellite data analytics company uses data generated by their satellites or buys data from satellite providers to offer custom made analytics to different companies and stakeholders (agriculture, insurance, tourism, etc.).	There are closed API's for satellite imagery and data which the clients buy or they buy reports based on these data, but there is no blockchain currently involved in managing their accuracy and transfer.
2.		

Process scheme (as-is)

Data and information (as-is)		
Data	Type	Description
1		
2		

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Satellite data provider	An entity that sells satellite data
2	Satellite data analytics provider	An entity that analyzes and provides reports
3	Company or stakeholder	An entity that buys the data or reports

Other Notes
The emerging satellite data and analytics market will need to use blockchain technologies to guarantee the accuracy of the offered data. Accurate data are essential for any attempts to automatize processes and use the strategic value of such information in smart contracts and actionable intelligence.

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	A company, NGO or policy actor requests data about a specific location/time which they use for their analytics or as a trigger for smart contracts they created on the DLT.	DLT checks if there are free data about the given location available (in the example we have it is an API service for open data from Sentinel 2A where we can use get and post commands http://anonette.net:8000/summary/). If the information is not open/free, a call to satellite data providers to post their offers is issued by the DLT. DLT emits<call for price and data/offer>
2.	The satellite providers offer the service (data) in various cryptocurrencies.	The interledger integration enables payment in different cryptocurrencies which DLT accepts. DLT emits <payment event>. The satellite providers register the payment and provide access to their data (API) with info on the metadata which are based in the ledger via some queries (timestamp proving the authenticity of the data).
3.	The satellite providers use the DLT when uploading their data on the cloud to timestamp the files and to be able to prove their authenticity. They offer their services and data in various cryptocurrencies on the DLT.	The satellite providers cloud or system updates the ledger continuously with uploaded data to authenticate their origin and provenance. The notary, records keeper, proof of existence type of contract provides a link to authenticate the data when offered to the users and clients. DLT emits<record proof>
4.	Trigger event: marker visible on the GPS location that triggers a smart contract on the DLT	When a visual marker is visible on the location (or other satellite provided data marker), the DLT updates the info on the assets and participants based on the contract.

Process scheme (to-be)

Participants and their roles		
Actor	Type/Role	Description
1	Satellite data providers	Authenticates data on the DLT, provides offers of data and services.
2	Stakeholders, NGOs, clients	Clients are seeking information or trigger data from satellites for their contracts on the DLT.

Data and information		
Data	Type	Description
1	Documents and data	Visual information or data timestamped on the DLT at the time of their upload on the server or cloud of the satellite providers.
2	Interledger payment transactions	Transfer of money between satellite data providers and their clients.
3	Request for satellite data	GPS location, image resolution and DN value, spectrum (visible, infrared etc.)

Security and privacy
1. Data authenticity and privacy are two requirements, which permissioned DLTs guarantee. All data is encrypted and protected;
2. DLT system should be able to provide mechanisms of DLT data integrity control (link to check the timestamp of a file);
3. DLT system should provide interledger integration for payments.
4. DLT system enables smart contracts with satellite data (over REST API).

Main Success Scenario + expected time line
1. All information timestamping, exchange and payments occur in DLT in automatic mode;
2. Payments are transferred using digital currency over interledger integration without human verification;

Conditions (pre- or post-)
1. The satellite data providers have a contract with the user interested in their service;
2. Users and providers must be registered in the identity solution on the DLT;
3. The data and services used in the transactions must be registered as assets;
4. Smart contracts must be deployed;
5. All parties are connected to DLT-network.

Performance needs
1. Transactions processing near real time;
2. 24/7/365 availability;

Legal considerations
1 Regulation (EC) 45/2001. The parties in the DLT, have to sign that they are aware of the limits and will not break the law.
2. Data from International intergovernmental organizations such as the European Space Agency (ESA) are not subject to EU law, including the GDPR (we are using Sentinel 2A).

Risks
1. Security risks;

- | |
|-------------------------------------|
| 2. Interledger vulnerabilities; |
| 3. Risks related to DLT immaturity. |

Special Requirements

- | |
|--|
| <ul style="list-style-type: none">1. More mature market for satellite data;2. Better awareness about current satellite technologies and their capabilities. |
|--|

External References and Miscellaneous
--

Blockchain application within a multi-sensor satellite architecture, 2018

<http://adsabs.harvard.edu/abs/2018amos.confE..25M>

<https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180006549.pdf>

The Game Changer of Geospatial Systems — Blockchain, 2017

<https://www.geospatialworld.net/article/blockchain-geospatial-systems/>

How ConsenSys's Latest Acquisition Puts Blockchain at the Center of the Booming Commercial Space Race, 2018

[https://medium.com/p/how-consensys-acquisition-of-planetary-resources-puts-the-blockchain-at-the-99d781f6d359?fbclid=IwAR3zwNc5KeZ736V4KUoenpnAseRxfTbeCwqZCi8DnJAGzudDg1exfSirV1M](https://medium.com/p/how-consensys-acquisition-of-planetary-resources-puts-the-blockchain-at-the-center-of-the-99d781f6d359?fbclid=IwAR3zwNc5KeZ736V4KUoenpnAseRxfTbeCwqZCi8DnJAGzudDg1exfSirV1M)

The Impact of Blockchain Technology on the Surveying Industry, Cadastre and Land Registry Systems, 2019

<https://medium.com/@johndeanmarkunas/the-impact-of-blockchain-technology-on-the-surveying-industry-cadastre-and-land-registry-systems-32ade8a8bbfd>

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)
-

Custodian Accounting of Electronic Mortgage

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-001	Use Case Type:	Vertical
Submission Date:	December 28, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Custodian accounting of electronic mortgage	Domain:	List 8 Appendix 2
Status of Case	Pilot	Sub-Domain	1. Finance a. Financial management & accounting b. interbank payments c. Reduction of Fraud d. Financial messaging e. Asset lifecycles and history
Contact information of person submitting/managing the use-case	Full Name: Dergachev Ivan Job Title: Project manager, Fintech Association E-mail address: ivan.dergachev@fintechru.org Telephone number: +7 926 773 77 74 Full Name: Alexander Chuburkov Job Title: Expert GOST R * Russian TC 26 Cryptography and security mechanisms * ISO TC 307 Blockchain & DLT * Fintech Association (RUS) * Chair WG4 FG DLT ITU-T E-mail address: chuburkovalex@gmail.com Telephone number: +7 965 336 62 92		
Proposing Organization	Fintech Association Address: 4 Shlyuzovaya Embankment, Moscow, 115114, Russia Web site: http://fintechru.org/		
Short Description	Masterchain is a P2P-network with access control. The communications between the nodes of this network are based on the modified Ethereum protocol. Masterchain provides for safe record of information in a distributed ledger. The copies of this ledger are kept at each node of the network. Here you can see the white paper of the Masterchain: http://fintechru.org/documents/Masterchain_whitepaper_v1.1_en.pdf		
Long description	Masterchain is: <ul style="list-style-type: none"> • System using blockchain, hierarchical, with a restriction on the addition of information; • Ledger type is replicated; 		

- | | |
|--|--|
| | <ul style="list-style-type: none">• Financial organization included in the Masterchain-authorized user of the information system, which can be both a user-validator (confirming the creation of a new block) or a user-controller, and as a result of the consensus procedure - user-registrar of the information system;• Conventional unit (token) - technological units of account/ specialized units of account;• User-registrar's resource - the computing power of the node (pool) of the user-registrar, expressed in the number of calculations of the hash function per second.• Type of consensus procedure - PoW. |
|--|--|

Decentralized Depository system is a platform implemented in the Masterchain.

- Decentralized Depository system including electronic mortgages aims to combine the accounting systems of the depositories of the Russian Federation in the unified ledger . The DDS application is part of the initiative, which aims to translate the entire process of buying property from the selection of the object to the registration of mortgages and obtaining rights to real estate in the "online" and to make maximum transparency at all stages.
- DDS provides depositories with the ability to perform the functions of storage and (or) accounting and confirmation of rights to electronic mortgagees to owners of mortgages or other persons exercising rights to electronic mortgages, conducting Depository operations, ensuring the accounting of mortgage parameters, as well as receiving reports on the status of mortgage registration in the Depository at any time.
- DDS allows exchanging information messages between depositories, including orders, keeping records of electronic mortgages on accounts provided by the Bank of Russia acts, storing files of electronic mortgages, as well as documents that can be created/issued in pursuance of electronic mortgages.
- Is necessary for conducting Depository accounting of electronic mortgages in connection with changes in the legislation of Russia, which introduces the concept of electronic mortgages - a non-documentary security, the rights of which are fixed in the form of an electronic document signed by an enhanced qualified electronic signature, which is stored in the Depository, in accordance with article 13.2 of the Federal law of 25.11.2018 No. 328-FL.

General principles of Depository accounting in DDS:

- Depository accounting of mortgage certificates is in pieces.
- Mortgages on Deposit accounts are accounted for on a double entry basis (in accordance with clause 5.1. Bank of Russia Regulation No. 503-P). Each mortgage in the Depository account must be recorded twice: once in the passive account and once in the active account for mortgages recorded in the Depository, the balance must be kept: the total number of mortgages recorded in the passive accounts of the depot must be equal to the total number of mortgages recorded in the active accounts.
- Depository operations are carried out on the principle of "two hands": the operator (it is possible to use the "technical user" in the system) and the controller.
- It is not allowed to have a negative balance of mortgages recorded on the depot account.

	Document accounting system: <ul style="list-style-type: none"> • A system of accounting for documents related to Depository accounting, as well as documents related to the storage, recording and transfer of rights to electronic mortgages should be organized within the framework of the DDS. Records of documents that have been received (incoming documents) or sent (outgoing documents) by the Depository shall be accessible. • Document accounting system may include software hardware designed to generate, send and receive electronic documents. 		
SDG in Focus (when applicable)			
Value Transfer:	Reduce of the mortgage business process costs by 30%	Number of Users:	10
Types of Users:	Business roles of DDS users: <ul style="list-style-type: none"> • Record-keeping Depository - the Depository carries out the storage of the mortgage, that is, performs the function of storage information contained in the electronic mortgage and agreements to the electronic mortgage, as well as interaction with Rosreestr during registration, amendments in the mortgage, cancelling the mortgage. • Record-entry Depository - depositary carrying out accounting and transfer of mortgage rights. Does not store the mortgage, provides services for the accounting and transfer of rights for the mortgage. • Role combining the roles of the Depository of storage and Depository of accounting rights. 		
Stakeholders	Fintech Association, Banks.		
Data:	There are two different kinds of data stored in Masterchain. The first is open data, that is stored in ledger and is available for all users in network. The second type is confidential data. It is stored in special storage. Access rights to confidential data are configured in smart-contract called "Role Model".		
Identification:	Addresses in network are calculated using certified cryptographic methods. These addresses within roles and access rights of users are stored in special smart-contract called "Whitelist". Each operation in network should pass an authorization using this contract.		
Predicted Outcomes:	<ul style="list-style-type: none"> • Elimination of the risks inherent in a paper mortgage: the risks of loss of the mortgage and the need for a procedure for the mortification of rights under the lost mortgage. • Increasing transparency of interaction between mortgage market participants and regulators. • Acceleration of securitization: the process of portfolio valuation and sale of the fixed volume of mortgages. 		

Overview of the Business Problem or Opportunity

The objectives of the project:

- Switching from paper documents to digital form due to Russian law
- Optimization of the business process by dint of DLT

- Simplification of the procedure of securitization

For all participants of the business process it means a significant reduction of time (in 3-5 times). Process reduces the risk of falsification of the document. For Depository, it means a reduction of operating costs by 30% and simplification of furnishing of documents for the Regulator. The process of document verification is simplified for the Regulator.

Why Distributed Ledger Technology?

The Blockchain and smart-contracts make this interaction trustworthy, transparent and understandable. The implementation of DLT solution, which allows tracking electronic mortgages, can eliminate paperwork and shorten the time of transaction.

Section 2: Current process

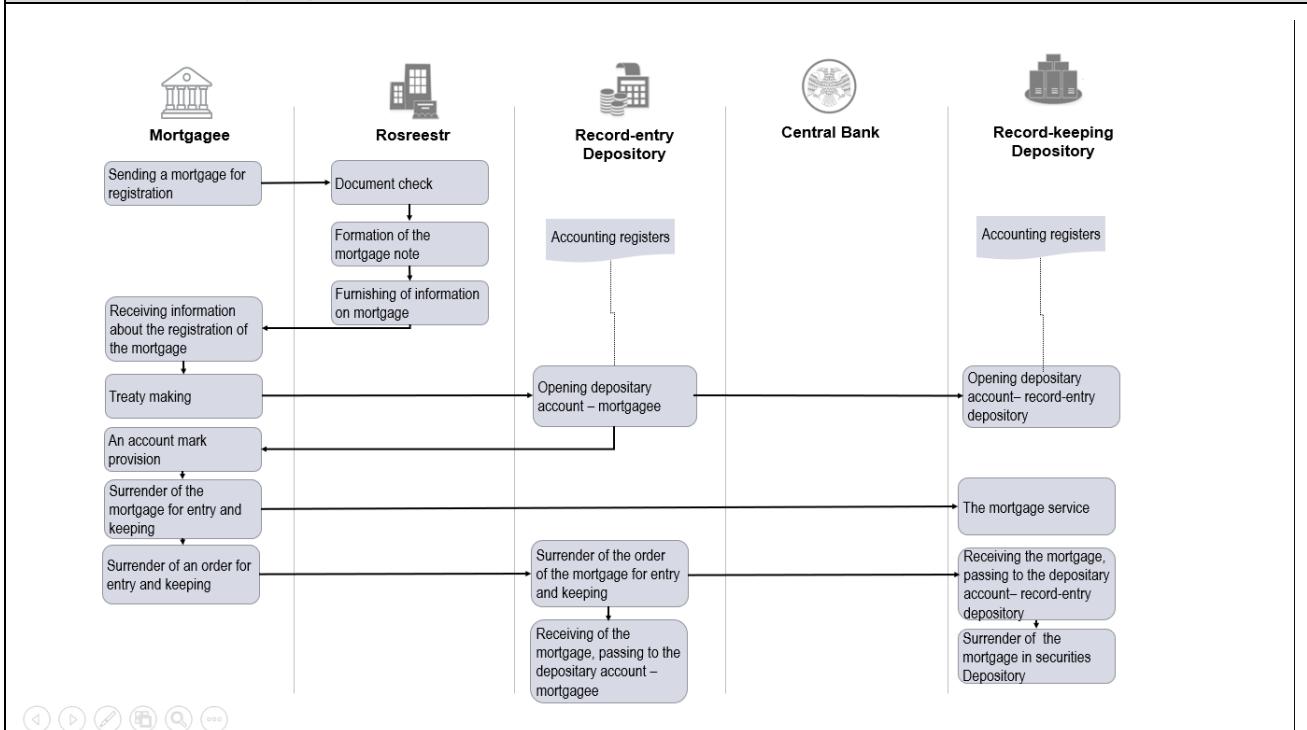
Current Solutions

Documents exist in paper form.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Mortgage servicing	n/a
2.	Record-entry Depository receiving/sending information about the mortgage	n/a
3.	Mortgage expired	n/a

Process scheme (as-is)



Data and information (as-is)

Data	Type	Description
1	Documents	Mortgage, agreements
2	Payment transactions	Payment of the fee

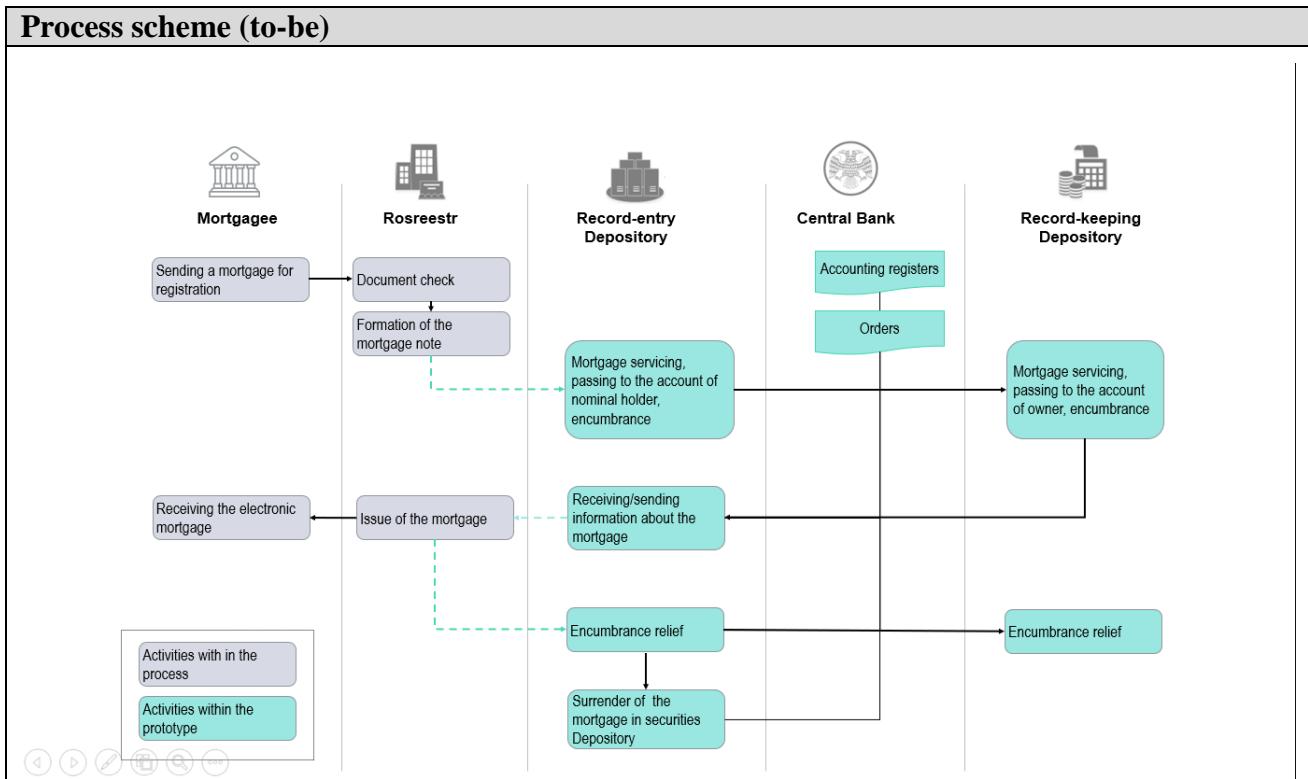
Participants and their roles (as-is)

Actor	Type/Role	Description
1	Mortgagee	Pledge holder
2	Rosreestr	Federal executive authority
3	Record-entry Depository	Participant of the securities market
4	Record-keeping Depository	Participant of the securities market
5	Central Bank	Central Bank of Russian Federation, Regulator

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Mortgagee	Pledge holder
2	Rosreestr	Federal executive authority
3	Record-entry Depository	Participant of the securities market
4	Record-keeping Depository	Participant of the securities market
5	Central Bank	Central Bank of Russian Federation, Regulator

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Mortgage servicing	System writes smart contract to the blockchain and save the contract to the distributed storage
2.	Depository validates mortgage data from the blockchain and the distributed storage	System marks the smart contract and the contract from the distributed storage as validated by Depository
3	Receiving/sending information about the mortgage	System marks the smart contract as active
4	The extension of the mortgage	System marks the smart contract as active. System saves hash of the documents to the blockchain and the consignment to the distributed storage
5	Changing conditions of the mortgage	System saves the data into distributed storage and blockchain
6	Mortgage expired	System finalizes the smart contract



Participants and their roles		
Actor	Type/Role	Description
1	Mortgagee	Pledge holder

Participants and their roles		
Actor	Type/Role	Description
2	Rosreestr	Federal executive authority
3	Record-entry Depository	Participant of the securities market
4	Record-keeping Depository	Participant of the securities market
5	Central Bank	Central Bank of Russian Federation, main top-tier Bank

Data and information		
Data	Type	Description
1	Documents	Documents hashes exchange in DLT-network
2	Payment transactions	Payment of the fee

Security and privacy
1. The mortgage conditions should be confidential to other blockchain network participants. 2. DLT-system should be able to provide mechanisms of mortgage documents and payments data integrity control; 3. Mortgage documents and payments data and related services (System Actions) should be available in 24/7/365 mode.

Main Success Scenario + expected time line
1. Mortgage comes into force; 2. Mortgage conditions adhered; 3. Mortgage expired.

Conditions (pre- or post-)
1. All parties are connected to DLT-network

Performance needs
1. Volume of transactions > 700 Tx/day. 2. Network participants > 150

Legal considerations
Switching from paper documents to digital form.

Risks

- | |
|--|
| <ol style="list-style-type: none">1. Legal risks;2. Security risks;3. Risks related to DLT immaturity. |
|--|

External References and Miscellaneous
--

GOST R 34.11-2012 (Streebog);

GOST R 34.10-2012;

GOST 28147-89 (Magma);

Appendix 1: Domains and subdomains for use cases categorization

Vertical:

2. 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
3. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
4. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
5. 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)
-

Digital Letter of Credit

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-002	Use Case Type:	Vertical
Submission Date:	December 28, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Digital Letter of Credit	Domain:	List 8 Appendix 2
Status of Case	<i>Pilot</i>	Sub-Domain	<ul style="list-style-type: none"> 1. Finance <ul style="list-style-type: none"> a. Financial management & accounting b. International & interbank payments c. Reduction of Fraud d. Financial messaging e. Asset lifecycles and history f. Trade finance g. AML/KYC
Contact information of person submitting/managing the use-case	<p>Full Name: Dergachev Ivan Job Title: Project manager, Fintech Association E-mail address: ivan.dergachev@fintechru.org Telephone number: +7 926 773 77 74</p> <p>Full Name: Alexander Chuburkov Job Title: Expert GOST R * Russian TC 26 Cryptography and security mechanisms * ISO TC 307 Blockchain & DLT * Fintech Association (RUS) * FOCUS GROUP DLT ITU-T E-mail address: chuburkovalex@gmail.com Telephone number: +7 965 336 62 92</p>		
Proposing Organization	Fintech Association Address: 4 Shlyuzovaya Embankment, Moscow, 115114, Russia http://fintechru.org/		
Short Description	Development and implementation of a software package to opening and implementation of a digital letter of credit based on a distributed ledger platform.		
Long Description	<p>The goals of the project are the creation and implementation of the application, improvement of legal regulation of digital letter of credit.</p> <p>The objectives of the project are:</p>		

	<ul style="list-style-type: none"> • <i>the formation of requirements and hypotheses for testing</i> (business requirements, functional requirements, hypothesis for testing on the prototype of the system, the target scheme of the system node and integration requirements); • <i>the development of a prototype system</i> (the prototype system, the test system prototype, the testing protocols of the prototype system); • <i>the development of the pilot system and its integration with external systems</i> (the pilot system, the script /test reports of the pilot system, reports on the testing of hypotheses, the program of activities/reports on the readiness of the transition to experimental-industrial exploitation system); • the introduction of the system/launch of the pilot (reports on the results of the commercial operation system, acts of transition to the commercial operation system, plan / report on the distribution of the system); • <i>the identification of obstacles/opportunities to improve the base of the regulatory legal act for digital letter of credit, the preparation of proposals and the organization of their adoption</i> (a list of regulatory legal act in digital credit for development/change, proposals in digital credit for the enactment of the PPA digital credit enacted). <p>Projected effect:</p> <ul style="list-style-type: none"> - reduction the duration of information exchange processes from 4 days to 0.5 days; - reduction of labor costs of the Bank's involved employees - up to 20%; 			
SDG in Focus (when applicable)				
Value Transfer:	<table border="1" style="width: 100%;"> <tr> <td style="width: 30%;"></td> <td style="width: 40%;">Number of Users:</td> <td style="width: 30%;">10</td> </tr> </table>		Number of Users:	10
	Number of Users:	10		
Users:	Exporters, Importers, Banks, Shipping companies			
Types of Users:	Buyer, Buyer's Bank, Supplier's Bank, Supplier.			
Stakeholders	Exporters, Importers, banks			
Data:	Electronic documents, accounts in DLT			
Identification:	Full identification of participants required			
Predicted Outcomes:	Automation of document and supply tracks involved into a Letter of Credit implementation. Reduction in the term of implementation of a letter of credit with a 15 days' cover.			

Overview of the Business Problem or Opportunity

The letter of credit transaction may involve a large number of participants of the business process that do not know and do not trust each other.

The first stage of project addresses the issue of eliminating paper work, by shifting it into digital form. At the second stage, it is expected to transfer payments between the counterparties using digital currency (CBDC).

The objectives of the project-automation of document flow, which are involved in the design of the letter of credit; eliminate paperwork and related time delays in the application of transactions.

Paper work elimination could be possible solution to problem of distributed data storage.

For customers it means significantly reduced time for registration and processing of documents (from 10 days to 4 hours). For Banks it means that they will be able to reduce transaction costs for processing transactions.

Project boundary:

Start: the buyer forms a business documents for issuance of the letter of credit (the condition of the contract for a bargain).

End: the buyer and the supplier are notified of the payment of the transaction.

Why Distributed Ledger Technology?

The Blockchain and smart-contracts make this interaction trustworthy, transparent and understandable for each one of them. The implementation of DLT solution, which allows tracking paid LoC issuance, can eliminate paperwork and shorten the time of transaction.

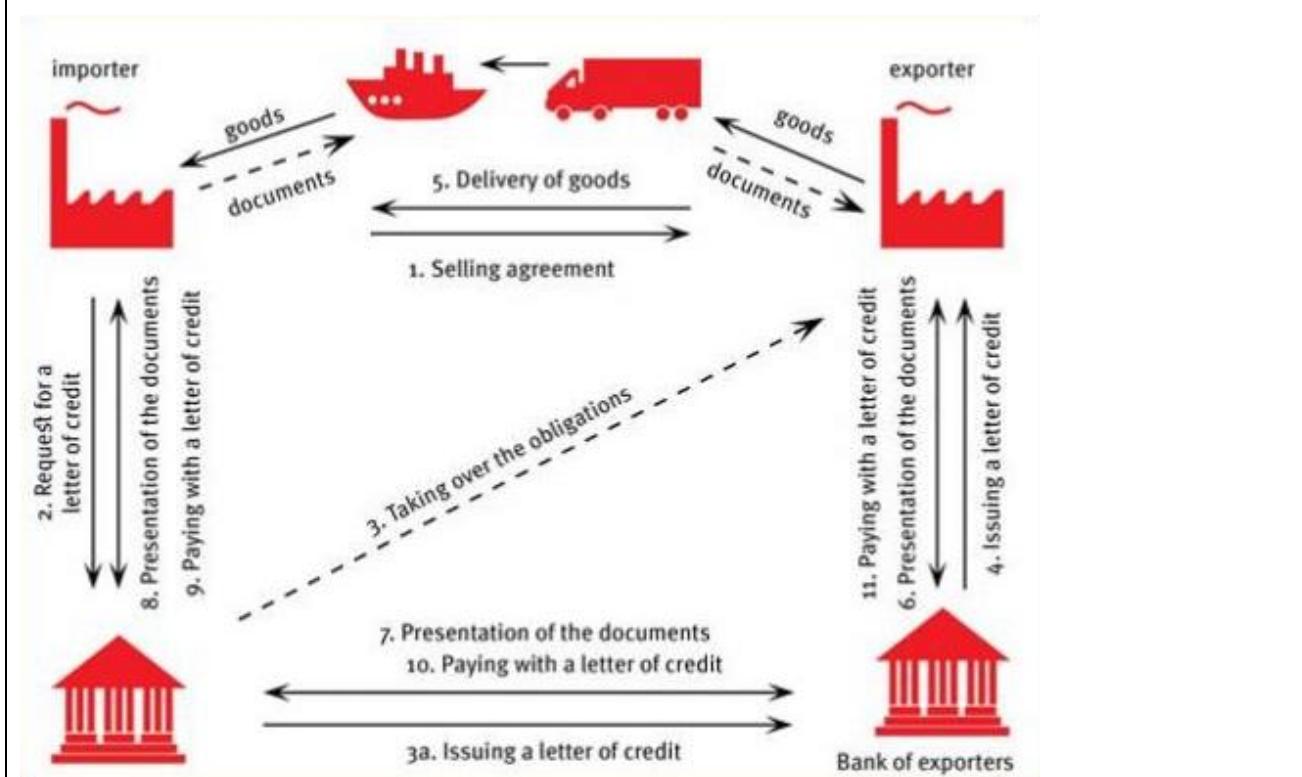
Section 2: Current process

Current Solutions

Documents exist in paper form; funds are transferred by corresponding bank.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Importer contacts bank for a LoC issuance	n/a
2.	Importer's bank checks if Importer is able to pay for goods	n/a
3.	Exporter receives LoC and checks that it matches with the contract	n/a
4.	Once the goods have been shipped, the Importer's bank pays to Exporter	n/a

Process scheme (as-is)



Data and information (as-is)

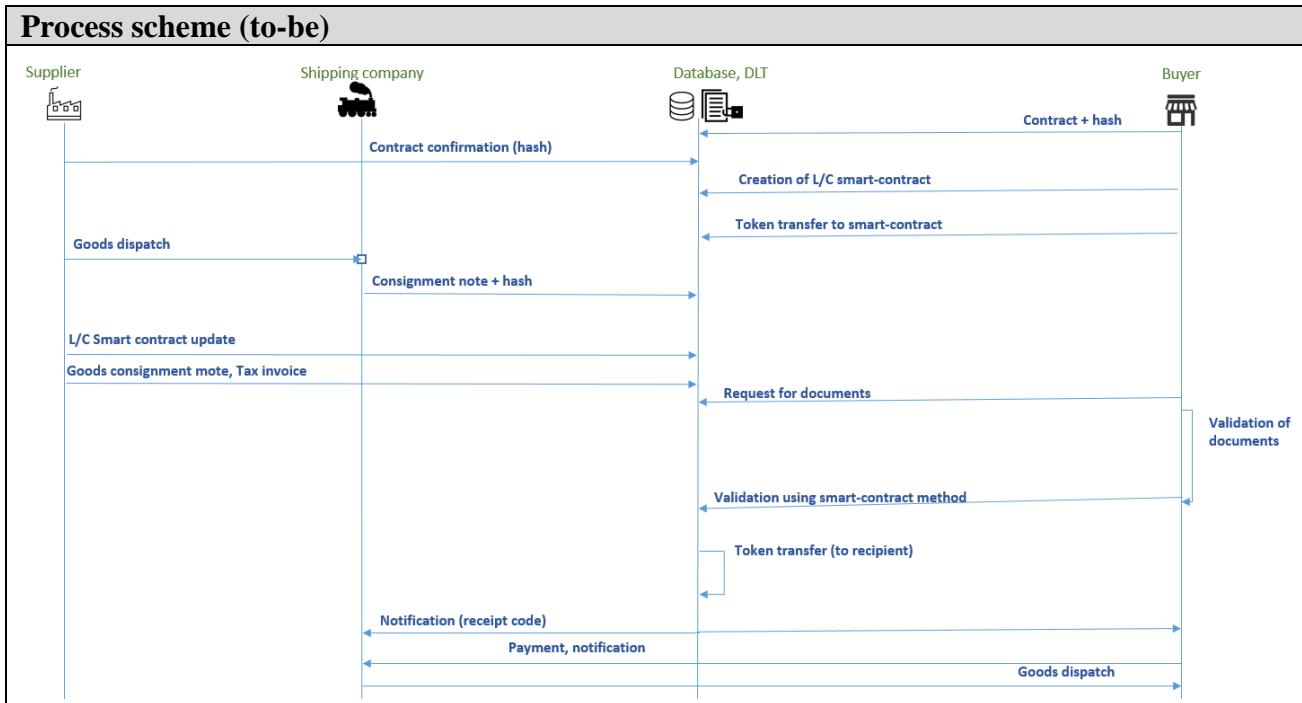
Data	Type	Description
1	Documents	Documents (Contract, Letter of credit, Transportation documents, Agreements)
2	Payment transactions	Letter of Credit payments

Participants and their roles (as-is)

Actor	Type/Role	Description
1	Exporter	Supplier of goods or services
2	Exporter's bank	Bank of supplier (letter of credit issuance)
3	Importer	Consumer of goods or services
4	Importer's bank	Bank of consumer (letter of credit payments)
5	Shipping company	The companies which delivers and stores the goods to the Importer (contracts and other documents validation, consignment forming, shipment)

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	The Importer writes Contract's public hashes to the blockchain and Contract's private data to the distributed storage	The System writes the smart contract to the blockchain and saves files with private data to the distributed storage
2.	The Exporter uses Contract's public identifiers and his private keys to access and validate the Contract's data	Marks the smart contract state and/or files in the distributed storage as validated by the Exporter
3	The Importer deposits tokens in amount specified in the Contract	Increases tokens amount on the account of smart-contract
4	The Exporter handles goods to the shipping company, the shipping company writes hash of the goods consignment to the blockchain and the private goods consignment to the distributed storage	Saves hash of the goods consignment to the smart contract and private consignment files to the distributed storage
5	The Exporter writes private goods consignment notes and Tax invoice to the distributed storage and their hashes to the blockchain	Saves the data into distributed storage and blockchain
6	The Importer validates the goods consignment	Marks the goods consignment as validated by the Importer and the smart contract sends tokens to the Exporter's account
7	Informing the shipping company about tokens sent to the Exporter account.	Shipment of goods to the Importer.



Participants and their roles		
Actor	Type/Role	Description
1	Importer	The Importer of the goods
2	Exporter	The Exporter of the goods
3	Shipping company	The companies which delivers and stores the goods to the Importer (contracts and other documents validation, consignment forming, shipment)

Data and information		
Data	Type	Description
1	Documents	Documents' hashes exchange in DLT-network
2	Payment transactions	Letter of Credit payments

Security and privacy		
1.	The contract conditions and payment transactions should be confidential to other blockchain network participants;	
2.	DLT-system should be able to provide mechanisms of L/C documents and payments data integrity control;	
3.	L/C documents and payments data and related services (System Actions) should be available in 24/7/365 mode.	

Main Success Scenario + expected time line

1. All information exchange and payments occur in Distributed Ledger in automatic mode;
2. Payments are transferred using digital currency (CBDC).

Conditions (pre- or post-)

All parties are connected to DLT-network

Performance needs

1. Payment transactions processing (near real time, 24/7/365)
2. Volume of transactions > 700 Tx/day.
3. Network participants > 150

Legal considerations

Eliminating paper documents shifting them to digital form.

Risks

1. Legal risks, including regulation of CBDC and cryptocurrencies, documents in digital form;
2. Security risks;
3. Risks related to DLT immaturity.

Special Requirements

Hypotheses are tested in the framework of the implemented functional prototype Digital letter of credit system.

The buyer and the supplier of the customers of one Bank (buyer's Bank=supplier's Bank), connected or have access to the digital letter of credit system

Appendix 1: Domains and subdomains for use cases categorization

Vertical:

2. 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
3. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
4. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
5. 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)

Digital Bank Guarantee

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-003	Use Case Type:	Vertical
Submission Date:	December 5, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Digital Bank Guarantee	Domain:	List 6 Appendix 2
Status of Case	Pilot	Sub-Domain	Financial
Contact information of person submitting/managing the use-case	Full Name: Dergachev Ivan Job Title: project manager E-mail address: ivan.dergachev@fintechru.org Telephone number: +7 926 773 77 74 Full Name: Alexander Chuburkov Job Title: Expert GOST R * Russian TC 26 Cryptography and security mechanisms * ISO TC 307 Blockchain & DLT * Fintech Association (RUS) * FOCUS GROUP DLT ITU-T E-mail address: chuburkovalex@gmail.com Telephone number: +7 965 336 62 92		
Proposing Organization	FinTech Association Address: 4 Shlyuzovaya Embankment, Moscow, 115114, Russia http://fintechru.org/		
Short Description	Development and implementation of a software package for the organization of work with Digital Bank guarantees (DBG) based on the distributed ledger platform (blockchain platform "Masterchain").		
Long description	The market is ready to move from paper bank guarantees to digital ones, and it has already come to the realization that the digitization of paper documents and further work with digital copies of paper documents is a non-optimal approach and it is necessary to move to a system where the digital document will be primary; The potential availability of CBG solutions currently being developed by individual Banks is limited to the clients of the respective Bank, which reduces the possible effect of their implementation (the Buyer and the Seller, as residents of the Russian Federation, are not always clients of the same Bank). The System (solution, set of services) developed in the project is an interbank platform that is not tied to one Bank and, therefore, is devoid of the mentioned restriction.		
Project goals:			

	<ul style="list-style-type: none">• Creation and implementation of the System• Improvement of legal regulation of CBG <p>Project objective:</p> <ul style="list-style-type: none">• Generation of requirements and hypothesis to test• Development of a prototype System and test the hypothesis• System pilot development and integration with "external" systems• System implementation/Start-up of pilot <p>Key assumption:</p> <ul style="list-style-type: none">• the technological platform for the project implementation is the infrastructure of the distributed Masterchain network, which includes the functionality for its administration and support of the role model of the system participants,• technological implementation of the system involves two stages: 1) creation of a prototype System and 2) creation of a pilot System,• openID Connect 1.0 is proposed as a technology for authorization of users of the developed system (user ID is signed by the authorization center, and can also be signed by the client in the browser through the EDS plug-in),• to store scans of documents (accompanying release, entry into force, change of conditions, termination of the warranty, etc.), it is planned to use a local document Storage integrated with the node of the distributed Masterchain network. <p>Beyond the scope of the project</p> <ul style="list-style-type: none">• Approval by the Principal and the Bank of the conditions for issuing a Bank guarantee,• Verification of the conditions for the entry into force of the Bank guarantee (except for the agreed date),• Check the conditions of termination of the Bank guarantee (except for the expiry of the guarantee),• Payment by the Principal of the Commission to the Bank for the issuance of a Bank guarantee,• Transfer of funds to the Beneficiary of the Bank guarantee when paying for it,• Integration with government agencies for the exchange of information on transactions with Bank guarantees.		
SDG in Focus (when applicable)			
Value Transfer:	Stage 1: no value transfer;	Number of Users:	
	Stage 2: payments in DLT allowed (CBDC)		10
Types of Users:	Principal, Guarantor bank, Beneficiary.		
Stakeholders	Principal, Beneficiary, Bank. Central Bank as observer		

Data:	Electronic documents, such as BG and contract, accounts in DLT
Identification:	Full identification of participants required
Predicted Outcomes:	<ul style="list-style-type: none">• Reduction of terms and reduction of costs to ensure document flow under Bank guarantees (According to Bain&Company, 2016, more than 50% of operating costs of banks to conduct transactions of Bank guarantees goes to the implementation of paper document flow).• Reducing the cost of storage and risks of loss of information on paper (Distributed ledger guarantees the technical safety of information on the documents).• Increasing the availability/reducing the time for obtaining information on the Bank guarantee and its status for all stakeholders through the use of a single information environment, in the future integrated with national electronic trading platforms.

Overview of the Business Problem or Opportunity

The objectives of the project:

- Switching from paper documents to digital form
- Protection of confidential data by limiting the visibility of the issued document

For all participants of the business process it means a significant reduction of time (1-2 days).

Process reduces the risk of falsification of the document, for economy that means increase of origin BG market. For banks, it means a reduction of operating costs by 10-15%. For Beneficiary, there is no reason to waste time on letters to Bank to verify authenticity of the issued bank guarantees. The process of document verification is simplified for the Regulator.

Why Distributed Ledger Technology?

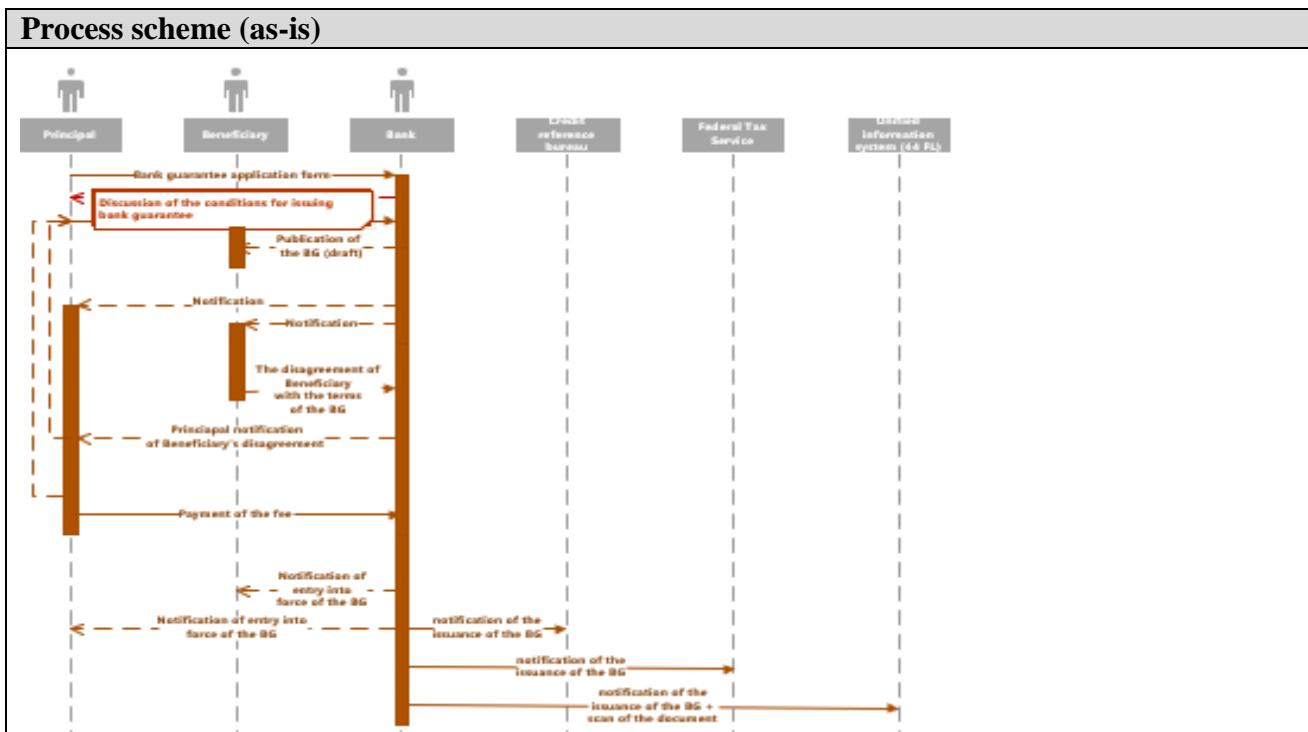
The Blockchain and smart-contracts make this interaction trustworthy, transparent and understandable for each one of them. The implementation of DLT solution, which allows tracking paid bank guarantees, can eliminate paperwork and shorten the time of transaction.

Section 2: Current process

Current Solutions		
Documents exist in paper form; funds are transferred by corresponding bank; procedure of verification of the BG is manual, confidential data of issued BG is not protected.		

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Principal contacts bank for a BG issuance	n/a

Existing Flow (as-is)		
Step	User Actions	System Actions
2.	Beneficiary receives BG and checks that it matches with the contract	n/a
3.	BG has expired	n/a

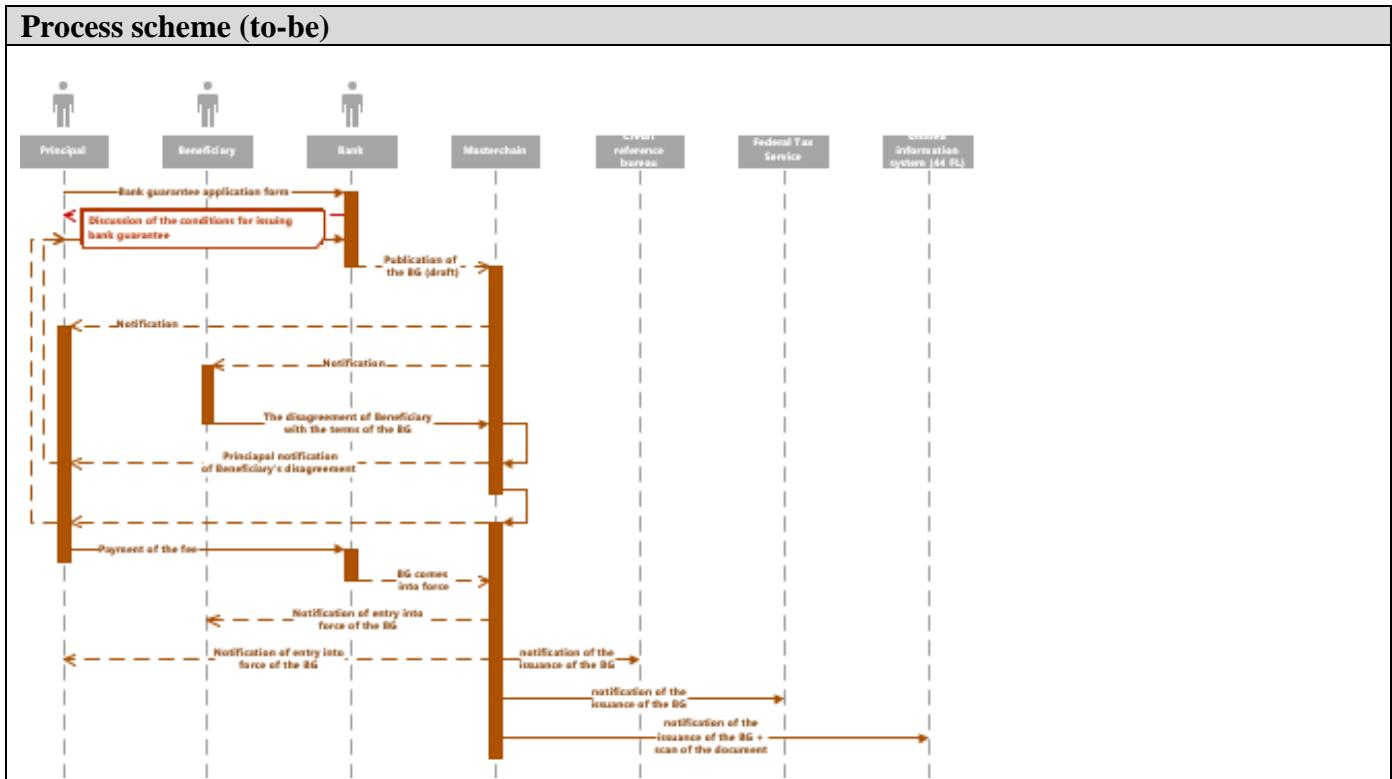


Data and information (as-is)		
Data	Type	Description
1	Documents	Contract, bank guarantee, agreements
2	Payment transactions	Payment of the fee for issue of bank guarantee

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Principal	Principal of bank guarantee
2	Beneficiary	Beneficiary of bank guarantee
3	Bank	Bank that issues the bank guarantee

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Bank writes BG's data to the blockchain and the distributed storage	System writes smart contract to the blockchain and save the contract to the distributed storage
2.	Beneficiary validates BG's data from the blockchain and the distributed storage	System marks the smart contract and the contract from the distributed storage as validated by the Beneficiary
3	BG comes into force	System marks the smart contract as active
4	The extension of the BG	System marks the smart contract as active. System saves hash of the documents to the blockchain and the consignment to the distributed storage
5	Changing conditions of the BG	System saves the data into distributed storage and blockchain
6	BG expired	System finalizes the smart contract



Participants and their roles		
Actor	Type/Role	Description
1	Bank	Bank that issues the bank guarantee
2	Principal	Principal of bank guarantee
3	Beneficiary	Beneficiary of bank guarantee

Data and information		
Data	Type	Description
1	Documents	Documents' hashes exchange in DLT-network
2	Payment transactions	Payment of the fee for issue of bank guarantee

- | Security and privacy |
|---|
| <ol style="list-style-type: none"> 1. The bank guarantee conditions should be confidential to other blockchain network participants. 2. DLT-system should be able to provide mechanisms of BG documents and payments data integrity control; 3. BG documents and payments data and related services (System Actions) should be available in 24/7/365 mode. |

- | Main Success Scenario + expected time line |
|---|
| <ol style="list-style-type: none"> 1. Principal furnishes documents to Bank 2. Bank approves loan 3. Principal accepts Bank conditions 4. Beneficiary accepts the text of BG 5. Principal pays fee 6. BG comes into force; 7. BG conditions adhered; 8. BG expired. |

Conditions (pre- or post-)
All parties are connected to DLT-network
Performance needs
<ol style="list-style-type: none"> 1. Volume of transactions > 700 Tx/day. 2. Network participants > 150
Legal considerations
Switching from paper documents to digital form
Risks
<ol style="list-style-type: none"> 1. Legal risks; 2. Security risks; 3. Risks related to DLT immaturity.

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)
-

88 InsurTech Insurance and BlockchAIn for Good

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-005	Use Case Type:	Vertical 1. Finance j Insurance Horizontal 1;3;4
Submission Date:	March 31, 2019	Is Use Case supporting SDGs	Yes
Use Case Title:	88 InsurTech Insurance and BlockchAIn for Good	Domain:	Finance
Status of Case	In Production (Live in BR)	Sub-Domain	Insurance
Contact information of person submitting/managing the use-case	<p>Full Name: Rodrigo Messias Ventura Job Title: Founder and CEO E-mail address: ventura@88i.io Telephone number: +5511995555001 Social media: https://www.linkedin.com/in/rodrigoventura/ https://singularityuglobal.org/profile/rodrigo-ventura https://www.youracclaim.com/badges/41f84027-9eaf-4f80-a191-9a79f890f720/linked_in_profile https://courses.dcurr.unic.ac.cy/user/profile.php?id=18091</p> <p>https://www.linkedin.com/company/11549784/admin/ https://www.facebook.com/88Insurtech.io/ https://twitter.com/88insurtech https://open.spotify.com/playlist/0oIkK6Y3icfFnBqwm3SWX2 https://www.youtube.com/channel/UC2AZZ_loumldrNsKz5jypBzQ https://github.com/88insurtech/ethereum https://github.com/88insurtech/hyperledger</p> <p>Web site: https://88i.io https://play.google.com/store/apps/details?id=io.insurtech88i</p>		
Proposing Organization	Legal name, Country and national registration number (as applicable) 88 Insurtech Serviços Digitais e Intermediação Ltda., Av. Angélica, 2529 - Bela Vista São Paulo - SP, 01227-200 Brazil National Registration Number: CNPJ 29.846.286/0001-02 UNGM number: 551162		
Short Description	<i>88i is reinventing insurance, Uberizing the industry to democratize insurance, ultimately making it for free and promoting social impact at global scale.</i>		
Long description	88 INSURTECH is a startup company with a disruptive business model based in blockchain that revolutionize the insurance market. The company presents a cheaper, more practical, faster and more transparent way to buy and sell insurance. The interface is simplified by the use of a		

	digital platform (app) that gives full transparency to the consumer and operated in a 24/7 shift to guarantee a faster path to contract and acquire insurance. In exchange of a cash-back, 88i is planning to have the active support of its clients to sell insurance products. Without the standard physical costs of distribution, it is expected to reduce the insurance cost up to -30% and make insurance for free. Another important feature of the business model is the possibility to customize the product. On Demand Company has won an important blockchain competition in Brazil promoted by Google (Startup Weekend Blockchain TechStars) UNICEF has been shortlisted 88INSURTECH as a Blockchain Startup for Social Impact with Global Scale at the Innovation Fund. And UNGM has listed 88i as a SUPPLIER NUMBER 551162, Additionally 88i was approved by Singularity University at their Global Startup Program GSP.		
SDG in Focus (when applicable)	<p><i>Enter one or more number (1-17) and specific corresponding indicator/s as applicable</i></p> <p><i>See https://www.un.org/sustainabledevelopment/sustainable-development-goals/</i></p> <p>1;2;3;4;5;8;10;11;17</p>		
Value Transfer:	<i>The solution allows to transfer any value (e.g. assets and or tokens, etc.)</i>	Number of Users:	<i>Over 1400 at the moment - We aim 1 Billion people</i>
Types of Users:	We are building ecosystems of protection in Mobility (Taxi, Car-sharing, Bikes, Scooters), Fintech (Digital Banking, Credit Lending) and Crypto/Fiat Exchanges		
Stakeholders	Drivers and Passengers - anyone who use a mobile phone		
Data:	<p>The first step is to register a transaction as a time-stamp in a PKI to prove immutability. (refereeing to a PDF insurance policy)</p> <p>The second step is to register a series of events, related to the insurance policy. (Like sales commissions paid, register of co-insurance, reinsurance, FNOL)</p> <p>The third step would be a self executing policy in real time via a smart contract. (instant claim settlement)</p> <p>All personal data should be preserved outside the ledger complying with the PDGR. The ledger would have the information about the financial scope of insurance and what binary information should try to obtain from an oracle.</p>		
Identification:	In the case of insurance, to be compliant with the insurance regulations, its necessary to have a KYC process during the app on-boarding. The client wants to identify him-self to be able to receive the insurance coverage.		
Predicted Outcomes:	<p>We want to democratize insurance, making it more simpler, easier and cheaper, ultimately for free in a member-get-member process.</p> <p>And subsidize micro-insurance with traditional insurance premiums not claimed. Our purpose is to impact 1 billion people worldwide</p>		

Overview of the Business Problem or Opportunity

The experience of buying insurance is awful, bureaucratic and time-consuming.

The millennial client of today represents 54% of the world's population and demands experience via digital channels and mobile apps;

The blockchain technology has vanished from the map the only 2 main entrance barriers from the insurance market (Regulation and Capital Intensive via ICOs, STOs)

Tech GIANTS had entered into the insurance market like

Lemonade with Google Capital; Sequoia and SoftBank);

Acko with Amazon or

ZhongAn with Tencent, Alibaba and PingAn

The world has changed to customer centric and the insurance industry still only focus in the product and the distribution channel.

There is a unique opportunity now to reinvent insurance while at the same time bring social impact at global scale.

Why Distributed Ledger Technology?

The improvement would happen by transforming the whole management life-cycle of an insurance policy. From entrance by enabling clients to buy from an app but also in the instant claim settlement in real time.

Immutability, No Arbitrage, No conflict of interests, Full transparency, Solvency rules like Basileia, Sarbanes Oxley; Instant Claim Settlement

Section 2: Current process

Current Solutions

Traditional Insurance carriers still remains with process from the industrial revolution. Everything is manual, bureaucratic, time-consuming, full of paper. The industry focus the distribution channel and the product, but not the customer. Furthermore it is expensive and excludes a number of people from having a protection from when they most need it.

Brokers, also don't have interest to sell microinsurance. We are changing that for good.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	You have to search for a insurance broker	
2.	Once with the broker you have to ask for a quote	The assessment is performed by the broker in paper.

Existing Flow (as-is)		
Step	User Actions	System Actions
3.	Do simulations	Simulations are made manually with a printed price / factor table
4	Get a quote	A quote than is provided by the broker to the client in paper
5	Ask to a proposal	The client verify the price; Accept the price and than ask the broker to formalizing to the insurer his proposal
4.	Insurer Acceptance	There is no guarantee that your proposal is going to be accepted by the insurer. In fact by law they have
5.	KYC Process	Inform 1. Tax ID + Birth date 2. Full address
6.	Receive the insurance policy	Policy issue 1. Mail 2. Via PDF e-mail

Process scheme (as-is)		
Client <=> Broker <=> Insurer		

Data and information (as-is)		
Data	Type	Description
1	Documents	1. Mobile phone number, IMEI, Model, Manufacturer 2. Tax ID, Birth date, Full Address 3. Credit card number
2	Payment transactions	Via Credit Card; Invoice

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Lawyers	Insurance regulation
2	Insurers and Assurances	Provide traditional insurance products for destitution and Risk coverage in case of a claim.
3.	Retailers	Physical Distribution channels to reach the client.

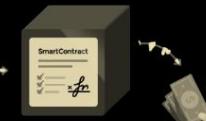
Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
0.	Share the Good with others	Member-get-member via social media to earn progressive discounts, until you get your insurance for free
1.	Download 88i app from Google play	Install the app https://play.google.com/store/apps/details?id=io.insurtech88i
2.	Login (ID)	Login with Google or Facebook
3.	Get a quote	<ol style="list-style-type: none">1. Inform your telephone number2. Select the coverage value \$3. Choose the types of coverages4. Receive a proposal
4.	Purchase your Protection	Select the type of payment <ol style="list-style-type: none">1. Credit Card2. Invoice3. Crypto
5.	KYC Process	Inform <ol style="list-style-type: none">3. Tax ID + Birth date4. Full address
6.	Receive the insurance policy	Policy issue <ol style="list-style-type: none">3. Inside the app insurance wallet4. Via PDF e-mail
7.	Share the Good with others	Member-get-member via social media to earn progressive discounts, until you get your insurance for free

Process scheme (to-be)

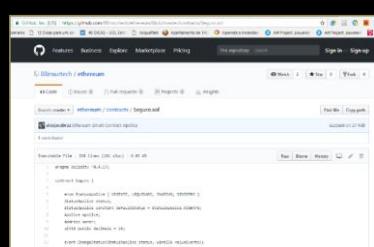
MOBILE INSURANCE – CREDIT CARD PAYMENT



© 88 InsurTech AG. Commercial In Confidence

28

MOBILE INSURANCE – CRYPTO PAYMENT



© 88 InsurTech AG. Commercial In Confidence

31

Participants and their roles		
Actor	Type/Role	Description
1	Documents	4. Social media ID; Name, e-mail, picture 5. Mobile phone number, IMEI, Model, Manufacturer 6. Tax ID, Birth date, Full Address 7. Credit card number
2	Payment transactions	Via Credit Card; Invoice or Crypto payment

Data and information		
Data	Type	Description
1	Lawyers	Insurance regulation Blockchain regulations
2	Insurers and Assurances	Provide tradition insurance products for destitution and Risk coverage in case of a claim.
3.	Taxi App Digital banks Exchanges	Digital Distribution channels to reach the client.

Security and privacy
<i>1. Depends of the network in use. It may vary between R3 Corda, Hyperledger, Etherium, RSK and NEM (each one of them according to the insurance product. Parametric or not) And type of use.</i>

Main Success Scenario + expected time line
Operate our 3 major taxi app platforms and Reach 1 million clients by Dez./2020

Conditions (pre- or post-)
1.

Performance needs
TBD

Legal considerations
1. We could disrupt the whole industry however playing with the rules we must have the traditional players in the game and make alliances with them, broker and insurers to be legally complaint. 2. Circular 294 SUSEP the electronic insurance sales. We provide the feedback inside the app.

Risks

1. Legal. Insurance is extremely regulated and we have a formal insurance layers to help us with that.
2. Tech, We are creating something with no precedent and good technical resources a hard to find. Accelerate the development of new products already mapped by the business team.
3. Human resources. Need to increase the seniority and professionalize to further investment rounds

Special Requirements

Business and technical requirements of use case

External References and Miscellaneous

Other Notes

Unifying Economies of Goods & Services and of Information

Section 1: Summary

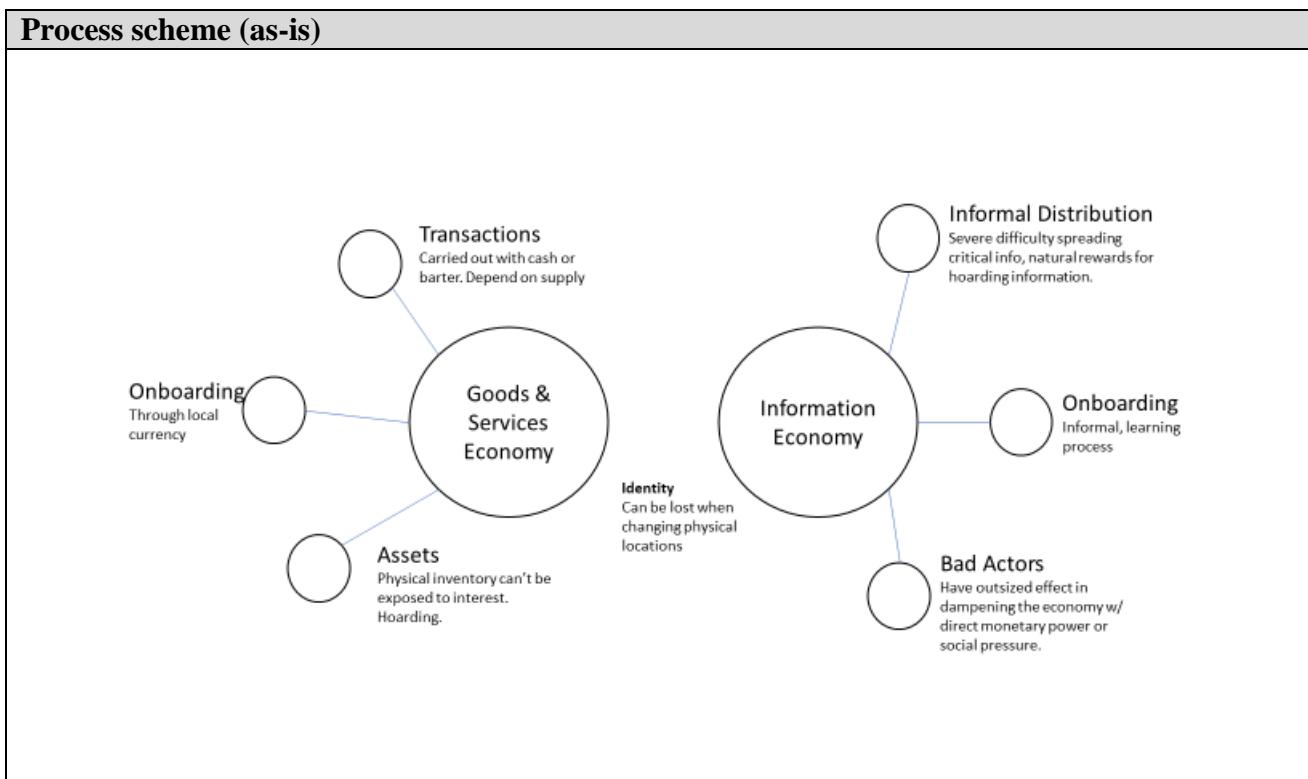
Use Case Summary			
Use Case ID:	FIN-006	Use Case Type:	Vertical
Submission Date:	April 1, 2019	Is Use Case supporting SDGs	Yes
Use Case Title:	Unifying Economies of Goods & Services and of Information	Domain:	Financial
Status of Case	Proof of Concept	Sub-Domain	F,K
Contact information of person submitting/managing the use-case	Bradley Clarke bradley@rsr.dev twitter.com/bradleyc	CEO, rsr.dev +1 714 604 8332 https://rsr.dev	
Proposing Organization	Resurgence Dev		
Short Description	We use DLT to formalize economies of goods and services and of information within a single system in the context of a refugee camp, using both social and financial leverage to create new opportunities for targeted delivery of aid and create a scaffold for enduring growth.		
Long description	<p>A major problem of informal economies is that assets within the economy have no way to be exposed to leverage or interest based investments. Tying physical inventories to a virtual currency opens an avenue for goods to also be leveraged.</p> <p>Formalizing a goods & services economy on the blockchain also allows for the pinpoint delivery of aid via community incentives. In other contexts, this would be called "gamification".</p> <p>Tying aid to "interest" on goods stored helps ensure that the amount of aid injected into the economy does not overwhelm organic growth of the economy, serving as scaffold for growth rather than creating a dependence on aid.</p> <p>We propose the formalization of the information economy on a microblogging platform, where participants in the network are able to reward each other for efforts in creation and curation of content. This economy would share the same currency as the layer for goods & services.</p> <p>By adding a social layer, good actors can visibly identify themselves as participants in both the goods & services and the information economies. Gamification can be used to coordinate incentivized behavior. Each transaction can optionally be broadcast on the network for visibility.</p>		

SDG in Focus (when applicable)	1) No Poverty 8) Decent Work & Economic Growth 10) Reduced inequalities		
Value Transfer:	Virtual token to track value of economies of goods & services and of information	Number of Users:	50,000 – 100,000
Types of Users:	Residents of a refugee camp		
Stakeholders	Residents of camp Camp administration Governing body that issues / certifies identity		
Data:	<p>The DLT would store and track a digital token for a given camp. It would also store references to actions taken by system actors in the real world and in the social layer.</p> <p>The social application layer would store content outside the DLT with immutable references to the content (via a hash) stored on the DLT.</p>		
Identification:	A public / private keypair will be issued to each resident involved in the study. This is be tied to either a retinal scan or a phone's IMEI number / SIM card, depending on available technology.		
Predicted Outcomes:	<p>Formalizing the goods & services economy through virtual currency allows smoother flows of capital within the cap, ability to measure aid utilization and target future aid, and potentially expose physical assets to interest bearing instruments.</p> <p>Formalizing the information economy exerts social pressure to encourage participation of good actors and counter the influence of bad actors and create tangible rewards for creating / curating useful information. The social layer can also serve as irrefutable proof of reputation if it is needed as residents exit the camp.</p>		

Overview of the Business Problem or Opportunity	
Why Distributed Ledger Technology?	DLT allows secure, immutable, and transparent registry of real-world goods tied to virtual currency. It brings the same level of security, immutability, and transparency to the information economy. The currency can also be verifiable if it becomes portable / convertible to any other currencies. Moving every transaction to the DLT creates transparency in the economy at large, removing dark areas in which bad actors prefer to act.
Section 2: Current process	

Current Solutions	
Currently, the most advanced solution we are aware of uses iris scanning in the distribution of aid resources. (see reliefweb page listed under external resources).	

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Transactions	Transactions must be carried out either with cash or barter. Supply issues can become a severe bottleneck in the economy
2.	Idle state of assets	Any physical inventory can't be exposed to interest
3.	Informal organization of information	Severe difficulty in spreading critical information to those who need it; natural rewards to those who hoard information.
4.	Dampening effect of bad actors	Bad actors can have an outsize effect in the economy through exerting direct monetary power or indirectly by creating social pressure toward



Data and information (as-is)		
Data	Type	Description
1	Paper money	Fiat currency

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Vendors	In context – any individual that engages in goods-for-currency trades

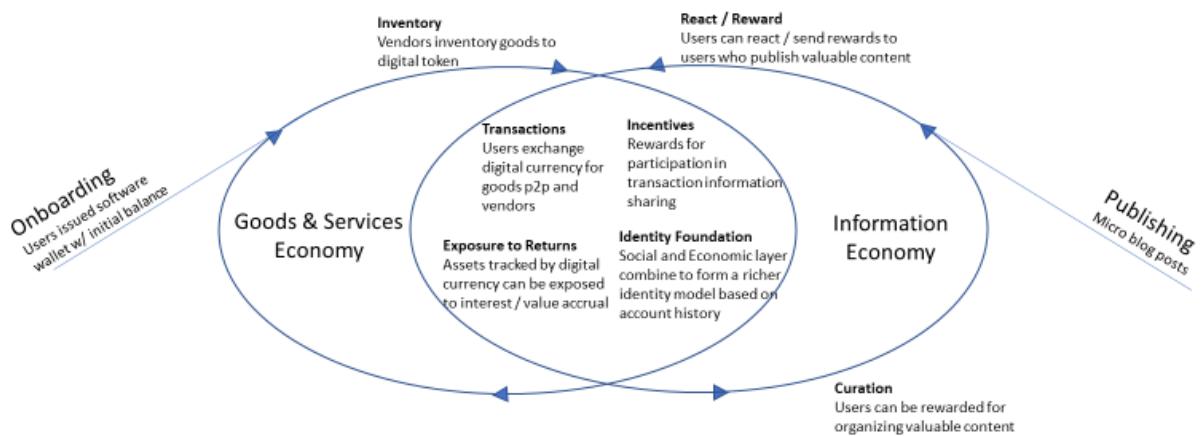
Participants and their roles (as-is)		
Actor	Type/Role	Description
2	Consumers	In context – transacts via barter or service exchange, or makes currency-for-goods purchases.

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Onboarding	Users issued software wallets with a small starting balance.
2.	Inventory	Vendors inventory their goods to be tied to digital tokens.
3.	Transactions	Users can transact using digital currency, either peer to peer or customer to vendor. Tokenized goods get transferred from seller to purchaser
4.	Incentives	As users transact, they can publish their transactions to a micro blogging service. Rewards for system participation can be issued on the basis of transaction quantity, value, or any dimension which could foster adoption.
5.	Publishing	Any user of the social layer can publish a micro blog post.
6.	React / Reward	Any user of the social layer can react to a published post and may choose to send a reward to the user who published the content. This should reinforce positive behavior.
7.	Curation	Users who choose to curate valuable social information in their published posts may be able to accrue substantial value.
8.	Exposure to returns	Digital currency or tokenized assets can be exposed to interest bearing investments / “savings accounts”, or interest might be simulated via direct aid payments as a percentage of assets tracked in the system.
9.	Identity foundation	An individual user’s activity in the social layer and the goods and services layer can use their account history while establishing documented identity in a future host country.

Process scheme (to-be)



Transaction Flow



User A stakes to post message

User B interacts with the message, sending a tip to User A

User C gets useful information from User A's post, and sends a moderate donation to User A

After receiving positive interactions, User A's initial stake is returned

After several high performing posts, User A buys bread from User B, transacting in Ethique.

Participants and their roles

Actor	Type/Role	Description
1	End Users	Participate in both the goods / services layer of the economy and the social layer
2	Program Administrators	Workers who help educate about and facilitate the program.

Data and information		
Data	Type	Description
1	Wallets	A software that stores basic identity information about the bearer of the wallet and keypairs that hold the assets in the system.
2	Tokenized Assets	Durable goods can be tracked by virtual non-fungible tokens and potentially used as collateral for financial services
3	Microblog posts	User submitted posts related to transactions or created entirely by users.
4	Virtual Currency	Both goods / services layer and social layer are tied to the same virtual currency.

Security and privacy
<ol style="list-style-type: none">1. Privacy is a major concern. We recommend that security / stability data science driven monitoring of the system be performed anonymously, and that network topology approaches be preferred in locating bad actors over watching the transactions of targeted users.2. It will be critical to establish that devices used to access wallet services have some level of security, such as passcode enabled.

Main Success Scenario + expected time line
Success will be met when the vast majority (80%) of camp transactions take place via online currency. Timeline: 4 weeks – requirements gathering, interviews, on-site inspection 12 weeks – software implementation 4 weeks – on site deployment, on site instruction, begin inventory 12 weeks – rollout of system across camp 12 weeks – monitored / incentivized adoption

Conditions (pre- or post-)
Requires internet or SMS access for end users.

Performance needs
Needs to be on a DLT that can handle high throughput. A RAFT-like consensus algorithm would suffice. End users would need devices capable of connecting to either an SMS or Web-based interface.

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.

Risks

Legal issues that have not yet been defined will likely emerge from this process.

Bad actors frequently resist attempts at economic formalization and could stall adoption.

Special Requirements

N/A

External References and Miscellaneous

<https://ethique.link>

<https://reliefweb.int/sites/reliefweb.int/files/resources/68256.pdf>

<https://www.technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/>

<https://www.un.org/sg/en/content/sg/personnel-appointments/2018-11-29/task-force-digital-financing-sustainable-development>

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)
-

Moeda's Global Ecosystem for Financial Inclusion and Sustainable Development Growth

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-007	Use Case Type:	<i>Horizontal</i>
Submission Date:	March 3, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Moeda's Global Ecosystem for Financial Inclusion and Sustainable Development Growth	Domain:	Cross-domains: Finance, Industries, Government and Public Sector, Identity Management, Security Management, Data Processing, Storage and Management
Status of Case	<i>Operating</i>	Sub-Domain	<i>Finance (Financial management & Accounting, International and Interbank Payments, Clearing and Settlement, Reduction of Fraud, Asset Lifecycles and History, Trade Finance, Regulatory and Compliance, AML/KYC, peer-to-peer transactions) Industries (Manufacturing, Supply chain Management, Agriculture) Government and public sector (Government and non-profit transparency, legislation, compliance and regulatory) Identity Management, Security Management, Data Processing Storage and Management</i>
Contact information of person submitting/managing the use-case	<i>Taynaah Reis taynaah@moeda.in @taynaahreis</i>	<i>President and CEO +1 347 8229423 www.moedaseeds.com</i>	
Proposing Organization	Moeda Semente Brasil – Desenvolvimento de Software e Serviços Financeiros S/A CNPJ 30.669.919/0001-33		
Short Description	<i>Moeda is an ecosystem of companies (Fintech, Accelerator, Crypto Exchange, Marketplace and BLOC Impact Fund Ventures) that uses blockchain technology to revolutionize finance by connecting mission-driven investors with community-owned enterprises and providing the means for alternative financing, knowledge, resource exchange, and collective action.</i>		

Long description	<p><i>Moeda's ecosystem of companies (Fintech, Accelerator, Crypto Exchange, Marketplace and BLOC Impact Fund Ventures) is effectively leapfrogging some of the most common challenges such as: lack of transparency, a preponderance of middlemen, and inefficiency.</i></p> <p><i>The system's architecture design through Blockchain allows the creation of trustworthy, immutable records, as well as cost-saving tackling social problems through innovative and scalable solutions in a secure way around the globe to achieve sustainable development.</i></p> <p><i>Moeda's ecosystem removes three key barriers that have plagued effective public financing of the Sustainable Development Goals (SDGs)</i></p> <ul style="list-style-type: none"><i>. Insufficient Transparency</i> <i>Impact lenders have little visibility into sustainable investments. This makes it risky to manage a large portfolio because there's no way to see where the money is going.</i><i>. Insufficient Access to Capital</i> <i>Due to the lack of transparency, borrowers have limited options for investment. Moeda gives borrowers a way to establish reputation, document project status, and to collaborate with others in the community.</i><i>. Investment Bias</i> <i>Statistics have shown that investors have a gender bias against women-led projects, despite having historically higher success ratios and repayment rates than projects run by men. Brazil has the largest gap, whereby 45 percent of women-owned SMEs identify access to finance as a major constraint in operating and growing their businesses.</i> <p><i>In August 2017, Moeda raised US\$ 20 million in an Initial Coin Offering (ICO) and its proprietary digital token, the MDA, has been listed on several exchanges including Binance, one of the largest in the world. Until today, Moeda has deployed over R\$ 4.7 million in impact investments that supports 7.500 direct beneficiaries.</i></p> <p><i>In March 2019, Moeda has created BLOC, alongside Bamboo Capital Partners ("Bamboo"), an impact investing platform, the Government of Togo and Smart Africa, a bold and innovative commitment from African Heads of State and Government to accelerate sustainable socioeconomic development on the continent, ushering Africa into a knowledge economy through affordable access to Broadband and usage of Information and Communications Technologies. The Smart Africa Alliance has since grown to include</i></p> <p><i>BLOC is the first impact fund in the world which uses blended finance to exclusively invest in companies that use new technologies, in particular blockchain, to benefit the low- and middle income populations in emerging markets.</i></p> <p><i>It demonstrates the joined ambition from public and private investors to tackle social and environmental challenges, leveraging innovative business models</i></p>
-------------------------	--

	<i>leapfrogging emerging markets and poverty. The Fund allocation of €100 million from a combination of public and private sector investors will focus on five key sectors: energy, education, financial inclusion and healthcare. Bamboo Capital is asset manager of BLOC Fund ventures in Luxembourg and Moeda's technology expertise provides investors on Bloc Fund Ventures full traceability of their investments. It is innovative because accepts investment in both hard currencies (EUR, USD) and cryptocurrencies (MDA, MDAB), using a KYC platform to convert the latter into either EUR or USD..</i>		
SDG in Focus (when applicable)	<i>Our initial focus are 6 of the Sustainable Development Goals – 1. No Poverty, 2. Zero Hunger 5. Gender Equality, 13. Climate Action 10. Reducing Inequalities and 17. Partnerships for the Goals.</i>		
Value Transfer:	<i>Assets, Tokens (cryptocurrency public traded MDA, stable/reserves coins MDABRL, MDAUSD, MDAEURO, debenture coin MDADIB, loyalty/rewards coins MDAB, MDALOYAL, MDAX)</i>	Number of Users:	<i>100.000+</i>
Types of Users:	<i>Borrowers (Individuals, Entrepreneurs, SME's, Cooperatives) Investors (Individuals, Private Institutions and Impact Funds, Financial Institutions Agencies, Government and Public Sector), International Development Organizations and Research Academic Institutions</i>		
Stakeholders	<i>Borrowers (Individuals, Entrepreneurs, SME's, Cooperatives) Investors (Individuals, Private Institutions and Impact Funds, Financial Institutions Agencies, Government and Public Sector)</i>		
Data:	<p><i>Types of Data: Attributes to ID and Authentication, Payment Transactions (Wallet Account, Balance, Transfer, Exchange, Swype, Split) Documentation (Projects Accountability, Supply chain, Wiki)</i></p> <p><i>Moeda Impact Ecosystem Platforms Hybrid Architecture Infrastructure</i></p> <p><i>The Moeda Impact Ecosystem Platforms are a combination of software programs built on four blockchain protocols, i.e. Hyperledger, Stellar network, Ethereum and the Binance Chain protocol and Moeda's API legacy systems.</i></p> <p><i>Moeda has built a partnership with IBM and DACS (Digital Asset Custody Services) and leverages IBM's LinuxOne servers and Crypto Express6S HSMs to provide the strongest possible security environment. Crypto Express6S is the highest commercially rated HSM in the world (FIPS 140-2 Level 4). Private keys are always encrypted and cannot be extracted or imported.</i></p> <p><i>All on-chain data related to Moeda's Platforms token transactions are kept private, such as documentation related to identity and authentication, confidential contracts and other agreements with sensitive information are managed through Hyperledger Fabric. Users retain sole custody of their</i></p>		

private keys throughout the transaction process, this gives full control to investors over their own funds without having to rely on an exchange.

Stellar network performs as a gateway for Fiat-Crypto transactions on Moeda's platforms. Stellar network allows easy and fast conversions of almost any fiat currencies into MDA-Fiat cryptocurrencies. Also it supports smart contracts which will ensure the whole Moeda's platforms to run smoothly.

On the other hand, in order to bring more scalability, decentralization and security to the software and more liquidity to token holders, Crypto-Crypto transactions on Moeda's platforms happen on Binance chain.

At Moeda's platforms, interchain swap tools and protocols were developed in conjunction with other transaction performance-enhancing tools both on Binance chain and Stellar network.

Moeda cryptocurrencies (stable/reserves coins MDABRL, MDAUSD, MDAEURO, debenture coin MDADIB, loyalty/rewards coins MDAB, MDALOYAL, MDAX) are deployed on both Stellar network and Binance chain. The tokens on Stellar network function as the actual utility tokens, while those on Binance chain can be exchanged with other cryptocurrencies. The token ownerships on both Stellar network and Binance chain are synchronized on a real-time basis thanks to interchain swap technologies.

Moeda's BLOC Impact Fund Ventures Investment Platform

The Moeda's BLOC platform aims to provide high quality and standardized impact fund service where investors have the opportunity to invest in top impact funds, not only to obtain considerable returns, but also to create global social benefits. The platform is joining forces with a number of well-known fund institutions to launch multiple funds, including Bamboo Capital, UNDP, etc.

Moeda's BLOC Platform aggregates liquidity across token exchanges by treating the entire landscape as a potential reserve. Bloc reserves provide a supply and demand of various tokens that are readily available to be executed based on the reserve's quoted buy and sell prices for that token. These reserves are created by on-chain smart contracts (Moeda's Chain) that enforce the trade execution and settlement process. The trade price is also programmatically determined by a smart contract. The reserve model enables Bloc users to enter trades more easily given that the supply and demand sides have fixed terms and are readily available to trade upon those terms. This removes the potential friction involved in discovering counterparties and negotiating.

Automated order filling

With an automated order filling Bloc Reserve Managers feed dynamic exchange rates into the Moeda's smart contract and orders are filled at the current exchange rate, an algorithm will match orders automatically. Automated order

	<p><i>filling reduces the amount of user time and effort needed to identify suitable trades, thereby reducing order filling latency.</i></p> <p><i>Moeda's BLOC Transaction Settlement</i></p> <p><i>On-chain settlement helps users publicly verify on the ledger that their trades were settled according to their desired terms.</i></p> <p><i>Moeda's BLOC Consensus</i></p> <p><i>Bloc has a flexible governance model MDAB-weighted delegated voting system where voting power is directly proportional to the amount of MDAB you have. Validator will be able to choose to stake its own token into the smart contract. Any holder of the MDAB token will have the option of proxying the held MDAB token to some Validator Node for Staking.</i></p> <p><i>Moeda's API (Legacy Systems)</i></p> <p><i>MOEDA API</i></p> <p><i>The MOEDA API is hosted on Microsoft Azure and deployed using Docker containers, which give us increased confidence that our development, staging, and production environments are consistent.</i></p> <p><i>MOEDA API microservices architecture consists of a collection of autonomous services: Authentication, Wallet, Exchange and Projects. Each service module is self-contained and implements a single business capability. Microservices are a popular architectural style for building applications that are resilient, highly scalable, independently deployable, and able to evolve quickly.</i></p> <p><i>The services are deployed independently. A team can update an existing service without rebuilding and redeploying the entire application.</i></p> <p><i>The Services are responsible for persisting their own data or external state. This differs from the traditional model, where a separate data layer handles data persistence.</i></p> <p><i>The Services communicate with each other by using well-defined APIs. Internal implementation details of each service are hidden from other services.</i></p> <p><i>MOEDA's API Languages and Tools</i></p> <p><i>The MOEDA API and Frontend are both built using JavaScript. We use next-generation JavaScript through Babel to take advantage of improved language features such as async/await and modules. All tests are built using Jest. The frontend integrates with the API using Apollo's GraphQL Client. The application data is stored within a PostgreSQL database, also hosted by Azure.</i></p>
Identification:	<i>Moeda's Identity Blockchain and Legacy Systems Inter-operability</i>

	<p>Authentication API</p> <p><i>In the Authorization API all the information is secured by a token present in each requisition. All the requisitions are logged and the given token is discarded after used. A new one is generated after each requisition.</i></p> <p><i>A hash is designed to act as a one-way function: A mathematical operation that turns readable data into a scrambled cipher and cannot be reversed. In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" the password.</i></p> <p><i>The user's login password is not saved. Instead, in the database is saved the resulting mathematical operation of the password mixed with the salt, guaranteeing the user's privacy.</i></p> <p><i>When a new account is created, an configurable e-mail and a SMS is sent with a random unique code to confirm the user ownership and block robots.</i></p> <p><i>The user's account balances are not stored in a local database, they are retrieved live from the blockchain real network.</i></p> <p>Moeda's Wallet API</p> <p><i>In Moeda's Wallet, the private key is automatically generated whenever a new user is created. This key is then encrypted using script algorithm and each information needed to decrypt this private is stored in separated servers. The raw private key is not stored anywhere.</i></p> <p><i>The address, as said, is generated from the public key and the public key is generated from the private key, so, indirectly, the address is generated from the private key. As the own name suggest, the public key can be publicly distributed, as it is possible to recover the private key with this information.</i></p>
Predicted Outcomes:	<p><i>For Investors (Individuals, Private Institutions and Impact Funds, Financial Institutions Agencies, Government and Public Sector):</i></p> <ul style="list-style-type: none">• <i>Access to SDG-aligned investment portfolio opportunities</i>• <i>Greater transparency into SDG-aligned Impact Investments</i>• <i>Trust of cryptographically assured blockchain records and contracts</i>• <i>Increased auditability</i>• <i>Decreased Risk</i> <p><i>For Borrowers (Individuals, Entrepreneurs, SMEs, Cooperatives)</i></p> <ul style="list-style-type: none">• <i>Provide a multi-purpose digital identity and opportunities to build credit-worthiness and reputation</i>• <i>Access to affordable capital</i>• <i>Facilitate to efficiently scale community investments</i>• <i>Facilitate payment transactions</i>• <i>Business education</i>

- | | |
|--|---|
| | <ul style="list-style-type: none">• Enhance access to other financial services• Access to online marketplace |
|--|---|

Overview of the Business Problem or Opportunity

According to the World Bank, approximately 2 billion people of the world are not included on the financial system, don't have access to a banking account, or worse, they have negative credit and are in debt.

In regards to the under banking of women, a recent Goldman Sachs research report states that the global credit gap for women is estimated at \$300B. Closing that gap could increase per capita income in emerging markets by an average of 12 percent by 2030, and could be as large as 25-28 percent for Brazil.

This moves us into impact investing where investments made with the intention to generate positive, measurable social and environmental impact alongside a financial return. In this way, we can align the interest of sustainability with that of investing – financial returns.

Moeda's Ecosystem removes three key barriers that have plagued effective public financing of the Sustainable Development Goals (SDGs):

Insufficient Transparency

Impact lenders have little visibility into sustainable investments. This makes it risky to manage a large portfolio because there's no way to see where the money is going.

Insufficient Access to Capital

Due to the lack of transparency, borrowers have limited options for investment. Moeda gives borrowers a way to establish reputation, document project status, and to collaborate with others in the community.

Investment Bias

Statistics have shown that investors have a gender bias against women-led projects, despite having historically higher success ratios and repayment rates than projects run by men. Brazil has the largest gap, whereby 45 percent of women-owned SMEs identify access to finance as a major constraint in operating and growing their businesses.

Why Distributed Ledger Technology?

Distributed Ledger Technology is a powerful tool that is already shaping the future of the Internet with simple, safe and secure transactions, bringing a new wave of Economic Opportunity and Digital Innovation.

The blockchain technology facilitates the exchange of value without the need for intermediaries, enables transparent interactions of parties through a trusted and secure network that distributes certified and auditable access to data, simplifying the existing processes lowering the costs and increasing the capital efficiency.

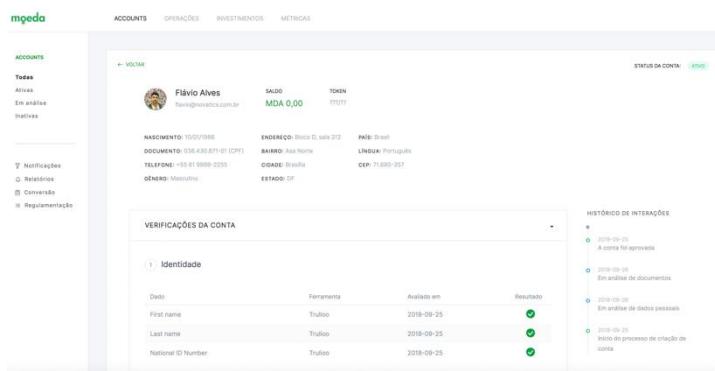
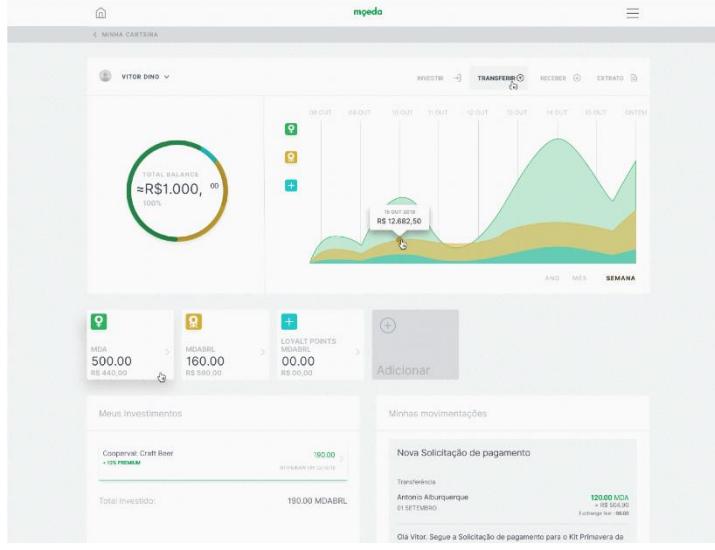
Section 2: Current process

Current Solutions

Moeda's Ecosystem utilizes DLT based trust of cryptographically assured blockchain records and contracts to provide the following solutions:

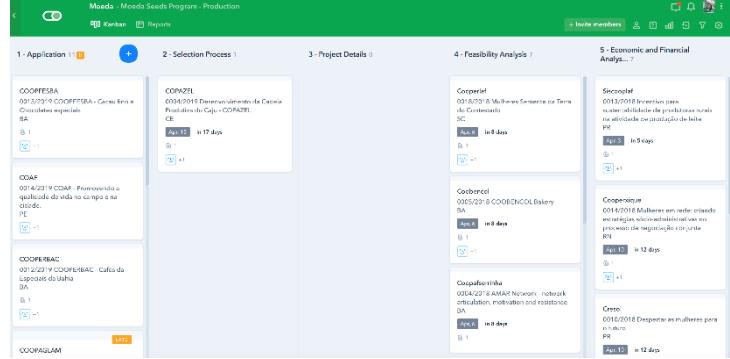
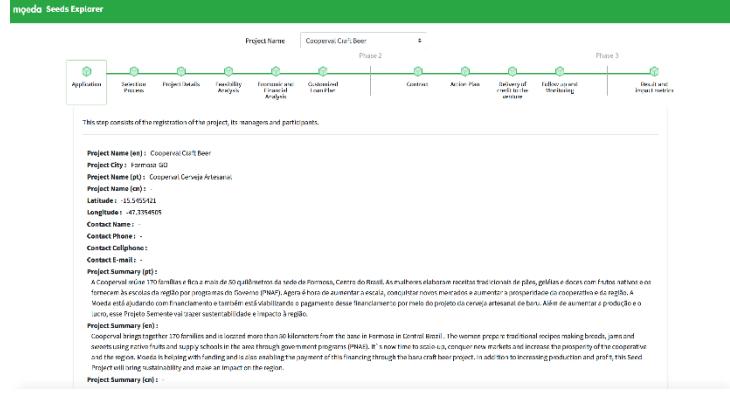
- *Access to SDG-aligned investment portfolio opportunities*
- *Greater transparency into SDG-aligned Impact Investments*
- *Increased auditability*
- *Decreased Risk*
- *Provide a multi-purpose digital identity and opportunities to build credit-worthiness and reputation*
- *Access to affordable capital*
- *Facilitate to efficiently scale community investments*
- *Facilitate payment transactions*
- *Access to online marketplace*

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	<p><u><i>Account Sign Up</i></u></p> <p><i>User is required to submit personal information (name, age, country..) ID images, proof of address, acknowledge terms of use) to have access to a Moeda ID and Account</i></p>	
2.	<p><u><i>ID Authentication (Global KYC/AML)</i></u></p> <p><i>User is required to submit personal information ID images, proof of address, acknowledge terms of use to have access to a Moeda Wallet and access to Investments)</i></p>	

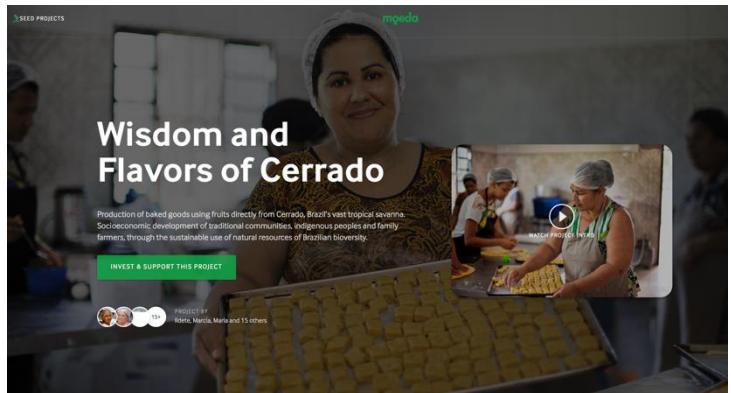
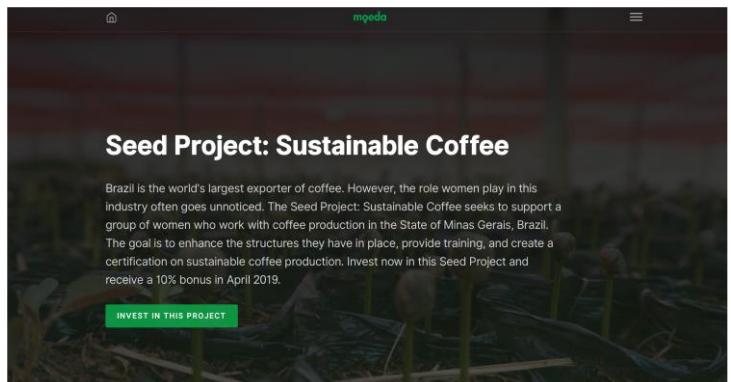
Existing Flow (as-is)		
Step	User Actions	System Actions
2.	<p><u>Backoffice Analysis of Accounts for KYC and AML with Global coverage</u></p> <p><i>Account Analysis uses both automatic machine learning process (Trulioo Global API and IDWall Brazil) and Manual process through Moeda's compliance team approval.</i></p> <p><i>Account approval takes from 3min to 3 days.</i></p>	
2.	<p>Moeda's Wallet</p> <p><i>Upon user's KYC/AML account approval, user is allowed to access it's Moeda's Wallet (Balance overview, investments portfolio, p2p payments Transfer, currency exchange)</i></p>	
	<p>Moeda Seeds Accelerator Program Project/Loan Submission</p> <p><i>To enter the Moeda Seeds Accelerator Program, Individuals/entrepreneurs are encourage to fill an application to submit it's Project/Loan</i></p>	

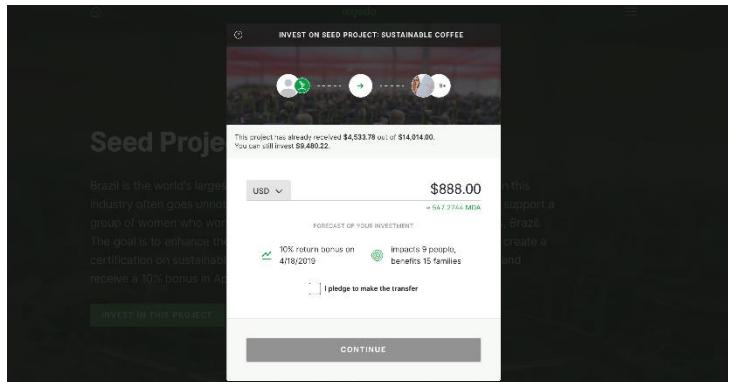
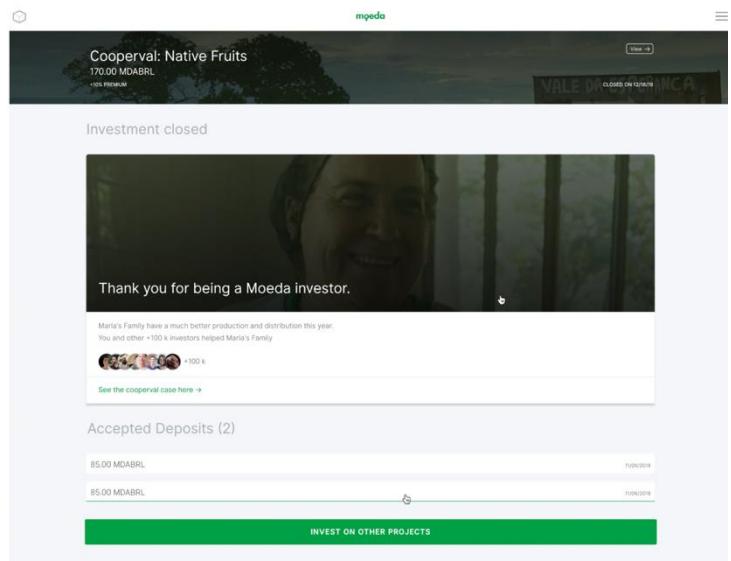
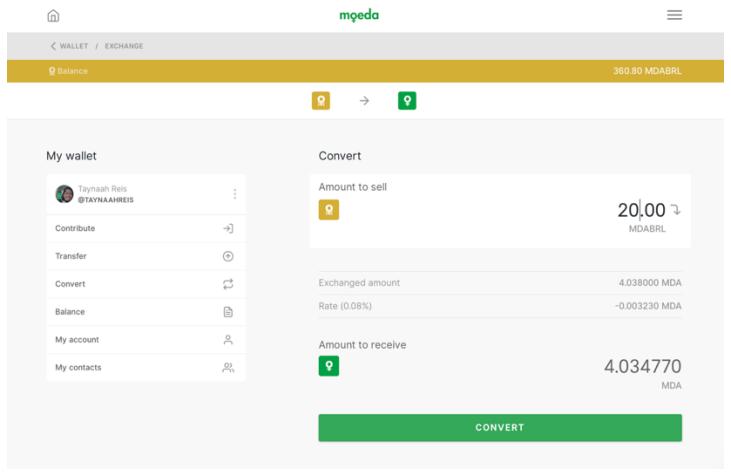
Existing Flow (as-is)																																							
Step	User Actions	System Actions																																					
	<p><i>Moeda Seeds Accelerator Program Project/Loan Submission</i></p> <p><i>The application allows Moeda's compliance team to curate projects in alignment with the programs objectives.</i></p>	<p>15+ Qual das Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas seu projeto ajudará a alcançar? *</p> <p>Pode selecionar várias opções</p> <ul style="list-style-type: none"> 1 ERADICAR A POBREZA A Objetivo 1: Erradicar a pobreza 2 ERADICAR FOME B Objetivo 2: Erradicar a fome 3 SAÚDE DE QUALIDADE C Objetivo 3: Saúde de qualidade 4 EDUCAÇÃO DE QUALIDADE D Objetivo 4: Educação de qualidade 5 IGUALDADE DE GÉNERO E Objetivo 5: Igualdade de gênero 6 ÁGUA POTÁVEL E SANEAMENTO F Objetivo 6: Água potável e saneamento 7 ENERGIAS RENOVÁVEIS E ACESSÍVEIS G Objetivo 7: Energias Renováveis e Acessíveis 8 TRABALHO DIGNO E CRESCIMENTO ECONÔMICO H Objetivo 8: Trabalho Digno e Crescimento Econômico 																																					
	<p><i>Moeda Seeds Accelerator Program Project/Loan Response</i></p> <p><i>Upon completing the application the individuals/entrepreneurs receive within 3 min an automatic analysis and estimate simulation of the loan and is encourage to provide more details to work on a customized loan plan.</i></p>	<p>Cadastro Projeto Semente</p> <p>Obrigado por enviar o cadastro inicial do seu projeto para a Moeda.</p> <p>Para dar continuidade ao processo, por favor, clique no botão abaixo. Ele dá acesso a um formulário mais completo, que vai ajudar a entender melhor seus objetivos e necessidades.</p> <p>Preencher formulário complementar</p> <p>Agradecemos sua confiança!</p> <p>Para você conhecer um pouco mais sobre nossas taxas e condições fizemos uma simulação baseada nas informações que você nos passou, veja só:</p> <table border="1"> <thead> <tr> <th colspan="2">Simulação de empréstimo</th> </tr> </thead> <tbody> <tr> <td>Valor Financiado</td> <td>R\$ 30.000,00</td> </tr> <tr> <td>Carência</td> <td>0 meses</td> </tr> <tr> <td>Prazo</td> <td>6 meses</td> </tr> <tr> <td>Juros</td> <td>1,60 %am</td> </tr> <tr> <td>Valor Total</td> <td>R\$ 33.287,33</td> </tr> <tr> <td>Juros Totais</td> <td>R\$ 1.787,33</td> </tr> <tr> <td>Fundo Moeda</td> <td>R\$ 1.500,00</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Parcela</th> <th>Mes</th> <th>Valor</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1</td> <td>R\$ 5.547,89</td> </tr> <tr> <td>2</td> <td>2</td> <td>R\$ 5.547,89</td> </tr> <tr> <td>3</td> <td>3</td> <td>R\$ 5.547,89</td> </tr> <tr> <td>4</td> <td>4</td> <td>R\$ 5.547,89</td> </tr> <tr> <td>5</td> <td>5</td> <td>R\$ 5.547,89</td> </tr> <tr> <td>6</td> <td>6</td> <td>R\$ 5.547,89</td> </tr> </tbody> </table>	Simulação de empréstimo		Valor Financiado	R\$ 30.000,00	Carência	0 meses	Prazo	6 meses	Juros	1,60 %am	Valor Total	R\$ 33.287,33	Juros Totais	R\$ 1.787,33	Fundo Moeda	R\$ 1.500,00	Parcela	Mes	Valor	1	1	R\$ 5.547,89	2	2	R\$ 5.547,89	3	3	R\$ 5.547,89	4	4	R\$ 5.547,89	5	5	R\$ 5.547,89	6	6	R\$ 5.547,89
Simulação de empréstimo																																							
Valor Financiado	R\$ 30.000,00																																						
Carência	0 meses																																						
Prazo	6 meses																																						
Juros	1,60 %am																																						
Valor Total	R\$ 33.287,33																																						
Juros Totais	R\$ 1.787,33																																						
Fundo Moeda	R\$ 1.500,00																																						
Parcela	Mes	Valor																																					
1	1	R\$ 5.547,89																																					
2	2	R\$ 5.547,89																																					
3	3	R\$ 5.547,89																																					
4	4	R\$ 5.547,89																																					
5	5	R\$ 5.547,89																																					
6	6	R\$ 5.547,89																																					
	<p><i>Moeda's Project Tracking Dashboard</i></p> <p><i>Moeda Seeds Accelerator Program team and its partners are equipped with a unique system that allows to track each stage of a enterprise/individual loan/project submission (from application selection process, feasibility and economic analysis, payments, results and impact)</i></p>	<p>Moeda</p> <p>Pipes Databases Reports Automations</p> <p>My pipes</p> <ul style="list-style-type: none"> 1 Assigned to you 2 Associação de cooperativas 3 Bloc & cards 4 BNDES / Unicafes 5 Indicação de consultor para projeto 6 Moeda Seeds Program - Projetos 7 Programa Moeda Semente - Web Application 8 Add new pipe 																																					

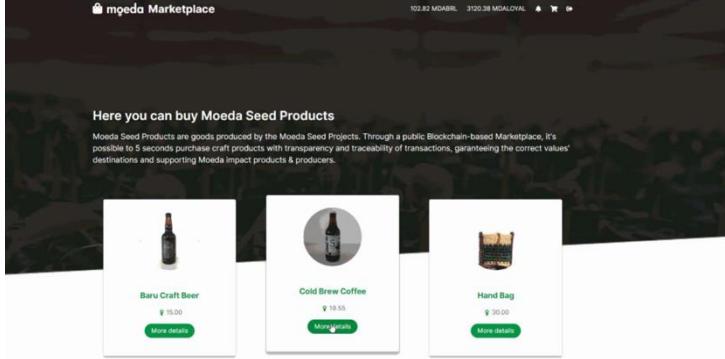
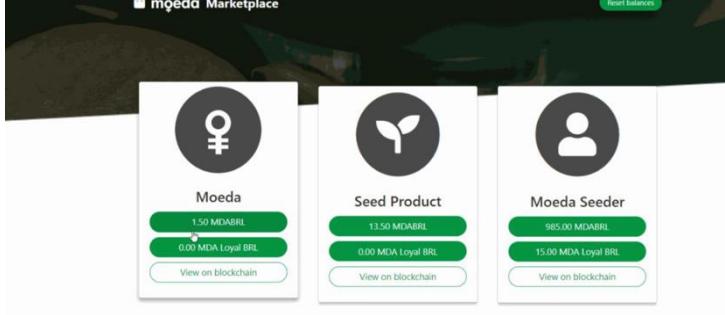
Existing Flow (as-is)

Step	User Actions	System Actions
	<p><i>Moeda's Project Tracking Dashboard</i></p> <p><i>Moeda Seeds Accelerator Program team and it's partners are equipped with a unique system that allows to track each stage of a enterprise/individual loan/project submission (from application selection process, feasibility and economic analysis, payments, results and impact)</i></p>	
	<p><i>Moeda's Project Explore using Hyperledger Fabric</i></p> <p><i>Moeda's share public information related to the project tracking system on it's website</i></p>	<p>Where the project is at this moment?</p> <p>Every project at Moeda goes thru a Technical Assistance team that will help from the qualification until the issuance of outcomes. Every transaction on these steps are registered via Blockchain so the information is secure. The projects themselves will be tradable blockchain assets on a future exchange to provide more liquidity and a lower cost of capital for entrepreneurs.</p> <p>Wisdom and Flavors of Cerrado is at Phase 2 · Contract</p> 
	<p><i>Moeda Seeds Accelerator Program Explore using Hyperledger Fabric</i></p> <p><i>Moeda's share public information related to the projects tracking system on it's websites</i></p>	
	<p><i>Moeda's APP</i></p> <p><i>Users are allowed to access the platform to an Android App available on Google Play Store</i></p>	

Existing Flow (as-is)		
Step	User Actions	System Actions
	<p><i>Moeda's Investment Portfolio</i></p> <p><i>Upon selection on the Moeda Seeds Program Accelerator, projects are showcased on the website (www.moedaseeds.com.br/projects) and can be open for co-investment and it's progress can be monitor online</i></p>	<p>Central Cerrado: Eco-social Products</p> <p>Copajas: Minimally Processed Foods</p> <p>Cooperfamiliar: Milk and Dairy</p> <p>COOPEREDÉ: Community Production</p> <p>Smart Water: Clean Water</p> <p>Cooperval: Native Fruits</p>

Existing Flow (as-is)					
Step	User Actions	System Actions			
	<p><i>Moeda's Investment Portfolio Project Details</i></p> <p><i>Upon selection on the Moeda Seeds Program Accelerator, projects are showcased on the website and can be open for co-investment and it's progress can be monitor online</i></p>	 <p>The History behind Wisdom and Flavors of Cerrado</p> <p>Wisdom and Flavors of Cerrado was first established in 2004, as an informal collective of 19 community-based projects based in the Federal District of Brazil, where Brasília is located. They were beneficiaries of the Small Social Projects Program (PPPEcos), operated by the Institute for Society, Population and Nature—ISPn, which together sought an alternative for products. At present, the Central has 21 community organizations in its framework, located in the states of Maranhão, Tocantins, Mato Grosso, Pára, Goiás, Piauí, Mato Grosso do Sul and Minas Gerais and operates in the development of 25 value chains from extractivism, agroextractivism and of traditional family agriculture, among them the babassu chain.</p>    <p>Impact this project is generating</p> <p>Every project lists at Moeda is generating great impact. Wisdom and Flavors of Cerrado was first established in 2004, as an informal collective of 19 community-based projects based in the Federal District of Brazil, where Brasília is located.</p> <table> <tr> <td>DIRECT BENEFICIARIES 2,350 people</td> <td>INDIRECT BENEFICIARIES 500,000 people</td> <td>NEW JOBS 50 positions</td> </tr> </table> <p>SUSTAINABLE DEVELOPMENT GOALS</p> <p>This project covers 6 goals of social and economic development issues agenda created by United Nations.</p>  	DIRECT BENEFICIARIES 2,350 people	INDIRECT BENEFICIARIES 500,000 people	NEW JOBS 50 positions
DIRECT BENEFICIARIES 2,350 people	INDIRECT BENEFICIARIES 500,000 people	NEW JOBS 50 positions			

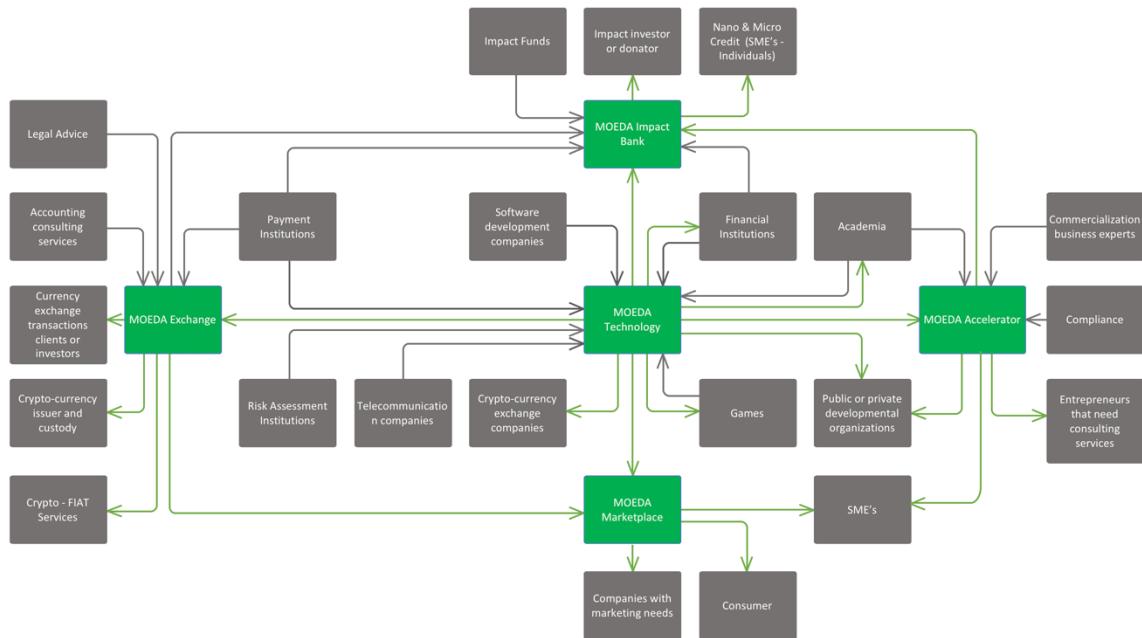
Existing Flow (as-is)		
Step	User Actions	System Actions
	<p><i>Moeda's Investment Portfolio</i></p> <p><i>Projects accept the following cryptocurrencies: MDA, MDABRL, MDALOYAL, BNB and MDAX</i></p>	
	<p><i>Moeda's Development Impact Bond</i></p> <p><i>Co-Investors at the Moeda Seeds Program Accelerator Portfolio of Projects receive a Moeda's Development Impact Bond (MDADIB) to track it's investments on the dashboard.</i></p>	
	<p><i>Moeda's Wallet</i></p> <p><i>User is allowed to exchange cryptocurrencies within the ecosystem</i></p>	

Existing Flow (as-is)		
Step	User Actions	System Actions
	<p><i>Moeda's Marketplace</i></p> <p><i>With pioneering and singularity initiative in construction an e-commerce platform with built-in cross-blockchain-based technology, especially related to an ecosystem of positive impact and sustainable generation, Moeda Market Place establishes the last mile of sales' and distribution of an entire chain of production, selection and development of social products, confirming its commitment with the circular and creative economy, corroborating its capacity to generate social impact and positive transformation.</i></p>	
	<p><i>Moeda's Marketplace</i></p> <p><i>Performing split transparent payments. Initially, through MDABRL, the use of the Stellar protocol allows the tracking of financial resources. It grants transparency in the ability of the user to verify how much is coming to the producer in relation to that purchase, and the amount that remains for the operation for Moeda Seeds.</i></p> <p><i>In addition, for each MDABRL transaction held in Moeda Market Place, Stellar protocol establishes a direct relationship with the Moeda Loyalty Program, which instantly generates MDALOYAL (XLM) points for users. Outside the incentive system, in case of purchasing products using PayPal, for</i></p>	

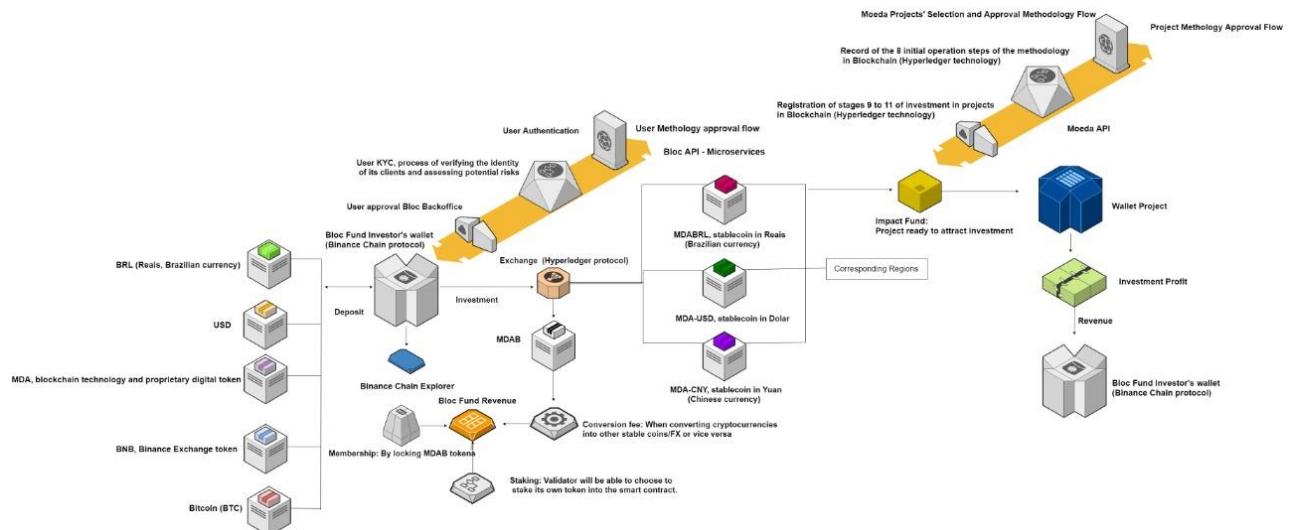
Existing Flow (as-is)		
Step	User Actions	System Actions
	<p><i>example, the user does not receive points.</i></p> <p><i>With Moeda ecosystem integrated user login and also direct integration with the Moeda Stellar Wallet already registered by the user, it is possible to use his own current balance to buy products at Market Place.</i></p> <p><i>All transactions performed at Moeda Market Place are registered in the Stellar public network, and its information can be observed in real time.</i></p>	

Process scheme (as-is)

Moeda's Ecosystem flow of Assets and Services



Moeda's Ecosystem Hybrid Architecture (Developed by the main system's Architect Taynaah Reis)



Data and information (as-is)

Data	Type	Description
1	Attributes to ID and Authentication	All on-chain data related to Moeda's Platforms token transactions are kept private, such as documentation related to identity and authentication, confidential contracts and other agreements with sensitive information are managed through Hyperledger Fabric. Users retain sole custody of their private keys throughout the transaction process, this gives full control to investors over their own funds without having to rely on an exchange.

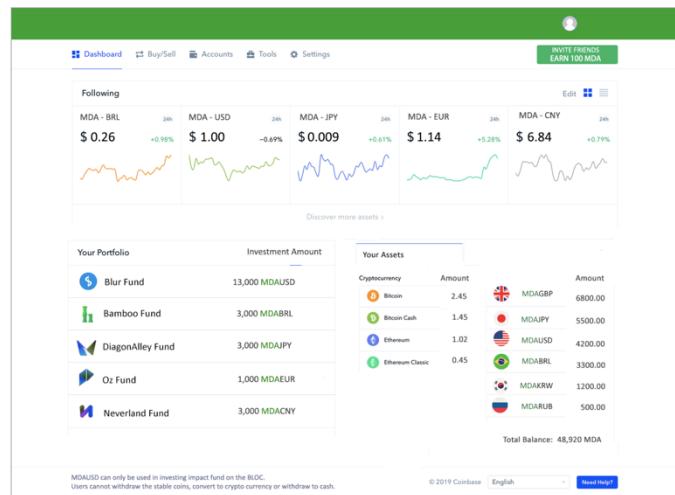
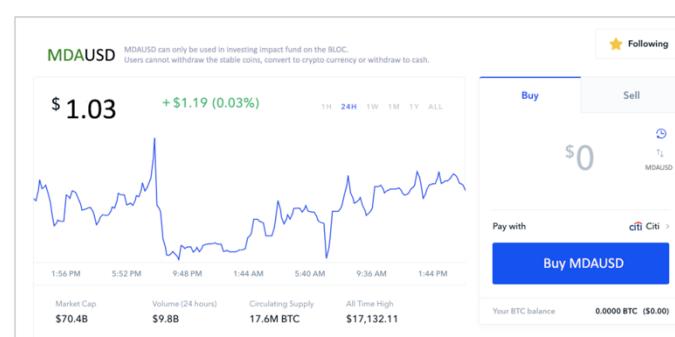
2	<p>Payment Transactions (<i>Wallet Account, Balance, Transfer, Exchange, Swap, Split</i>)</p>	<p><i>Stellar network performs as a gateway for Fiat-Crypto transactions on Moeda's platforms. Stellar network allows easy and fast conversions of almost any fiat currencies into MDA-Fiat cryptocurrencies. Also it supports smart contracts which will ensure the whole Moeda's platforms to run smoothly.</i></p> <p><i>On the other hand, in order to bring more scalability, decentralization and security to the software and more liquidity to token holders, Crypto-Crypto transactions on Moeda's platforms happen on Binance chain.</i></p> <p><i>At Moeda's platforms, interchain swap tools and protocols were developed in conjunction with other transaction performance-enhancing tools both on Binance chain and Stellar network.</i></p> <p><i>Moeda cryptocurrencies (stable/reserves coins MDABRL, MDAUSD, MDAEURO, debenture coin MDADIB, loyalty/rewards coins MDAB, MDALOYAL, MDAX) are deployed on both Stellar network and Binance chain. The tokens on Stellar network function as the actual utility tokens, while those on Binance chain can be exchanged with other cryptocurrencies. The token ownerships on both Stellar network and Binance chain are synchronized on a real-time basis thanks to interchain swap technologies.</i></p> <p><i>Moeda's BLOC Platform aggregates liquidity across token exchanges by treating the entire landscape as a potential reserve. Bloc reserves provide a supply and demand of various tokens that are readily available to be executed based on the reserve's quoted buy and sell prices for that token. These reserves are created by on-chain smart contracts (Moeda's Chain) that enforce the trade execution and settlement process. The trade price is also programmatically determined by a smart contract. The reserve model enables Bloc users to enter trades more easily given that the supply and demand sides have fixed terms and are readily available to trade upon those terms. This removes the potential friction involved in discovering counterparties and negotiating.</i></p> <p><i>Automated order filling</i></p> <p><i>With an automated order filling Bloc Reserve Managers feed dynamic exchange rates into the Moeda's smart contract and orders are filled at the current exchange rate, an algorithm will match orders automatically. Automated order filling reduces the amount of user time and effort needed to identify suitable trades, thereby reducing order filling latency.</i></p> <p><i>Moeda's BLOC Transaction Settlement</i></p>
---	--	--

Data and information (as-is)		
Data	Type	Description
		<p><i>On-chain settlement helps users publicly verify on the ledger that their trades were settled according to their desired terms.</i></p> <p><i>Moeda's BLOC Consensus</i></p> <p><i>Bloc has a flexible governance model MDAB-weighted delegated voting system where voting power is directly proportional to the amount of MDAB you have. Validator will be able to choose to stake its own token into the smart contract. Any holder of the MDAB token will have the option of proxying the held MDAB token to some Validator Node for Staking.</i></p>
3	<i>Documentation (Projects Accountability, Supply chain, Wiki)</i>	<p><i>Moeda's Hyperledger Fabric Application</i></p> <p><i>By establishing a changeless record database on all financial transactions, Hyperledger's use in Moeda's Ecosystem goes beyond its financial aspect. As well as in the Projects Approval Flow of Moeda Seed Projects, in Market Place Hyperledger keeps track of all steps of approval of the product until its entrance to commercialization. In this way, all the steps that classify products to be socially responsible for their availability become transparente and unalterable. Hyperledger Fabric's modular capability gives Moeda a chance to separate products from Moeda Seed projects or outside.</i></p> <p><i>Another fundamental aspect of Hyperledger is related to traceability the application in the productive process of the respective commercialized products. Initially applied and available for only a few specific products within Market Place, the full history of the product, its certificates of origin, quality and working conditions will be recorded and displayed. These products will receive a traceability and uniqueness ID, granting the new Moeda certification for socially responsible products in the New Economy Blockchain Market and beyond. In medium term, with optimized processes of selection and evaluation, also counting on the modular aspect of the used protocol, it will be possible to apply this certification not only for entry into the Market Place, but also for other similar environments.</i></p> <p><i>As a database of immutable records and with calibrated business rules, Hyperledger also prints transparency in the ability to see split payments also made via PayPal.</i></p> <p><i>With a separate node in the Currency network, but permeating its entire environment, Hyperledger Fabric connects and integrates with the Backoffice both the Moeda administrative portal and the Backoffice of the respective Projects (Producer</i></p>

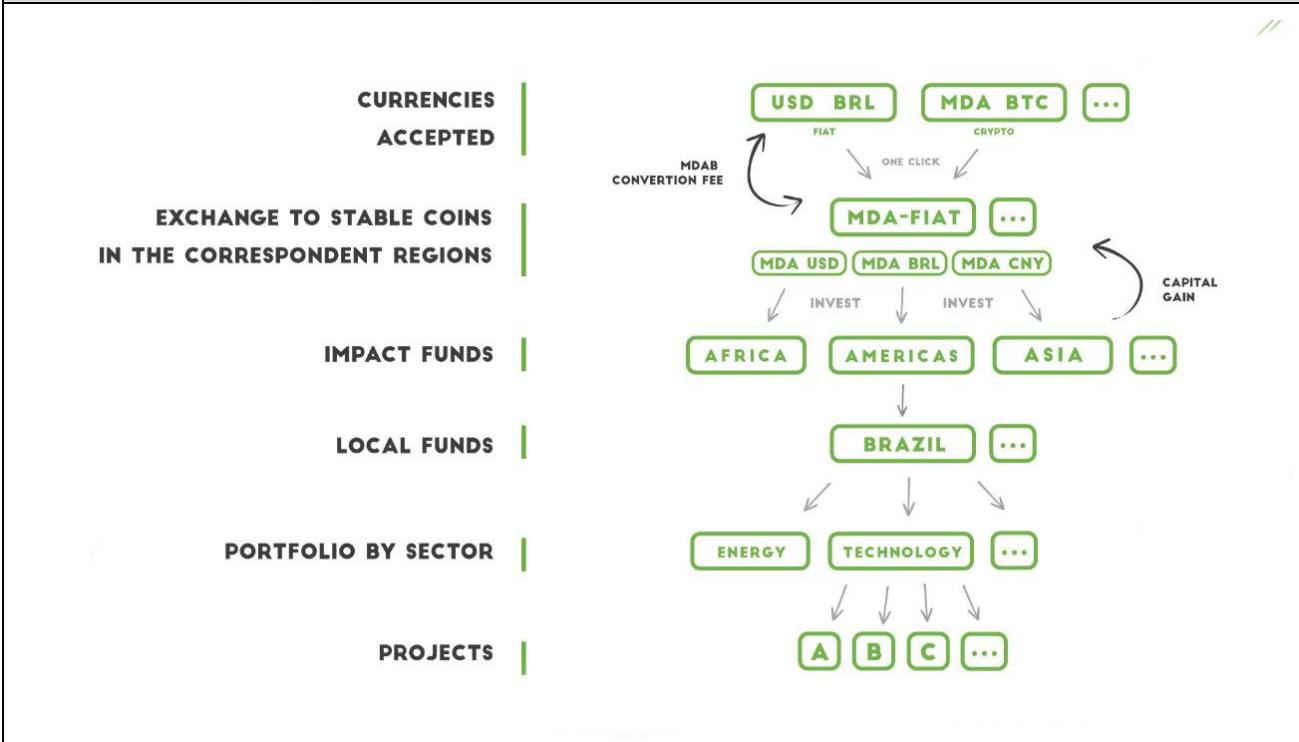
Data and information (as-is)		
Data	Type	Description
		<i>Portal) to follow up on its movements, deliveries and product approvals, among many others.</i>

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Borrowers</i>	<i>Individuals, Entrepreneurs, SME's, Cooperatives</i>
2	<i>Investors</i>	<i>Individuals, Private Institutions and Impact Funds, Financial Institutions Agencies, Government and Public Sector</i>
2	<i>Research and Academia</i>	<i>International Development Organizations and Academic Institutions</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	<i>Users will be allowed to invest in other Impact Investment Funds and Global portfolios with both FIAT and Cryptocurrencies.</i>	
2.	<i>Moeda will provide other services like insurance and currency-hedge</i>	

Process scheme (to-be)



Security and privacy

Transaction history, digital bank account information, and customer credit card credentials, investment preferences are a few examples of data that needs to be secured from unauthorized access. Unauthorized exposure is often prevented using data encryption and that's is the reason why we have been using blockchain Hyperledger, Stellar, Ethereum and Binance protocols through our systems to significantly increasing data availability and integrity, reducing paperwork handling, storage and loss, and other process improvements related.

Blockchain allows for the creation of trustworthy, immutable records, as well as cost-saving operational efficiencies that then lower the cost of lending while increasing safety.

Offering financial services also require specific approach with backup systems, to guarantee our systems will continue running in case of an incident. Backup schedules and tools are outlined in relevant policies and regularly reported on by functional managers. Awareness training includes how to establish whether backups have effectively been made of organizational data and how to securely store backups on the systems provided.

Moeda has built a partnership with IBM and DACS (Digital Asset Custody Services) and leverages IBM's LinuxOne servers and Crypto Express6S HSMs to provide the strongest possible security environment. Crypto Express6S is the highest commercially rated HSM in the world (FIPS 140-2 Level 4). Private keys are always encrypted and cannot be extracted or imported.

Main Success Scenario + expected time line

We aim to significantly improve Impact Results, by funneling sustainable development investments into local communities across the globe.

We started in Brazil with and plan to expand the ecosystem to LATAM and Africa in 2019 to reach 1 million associates by 2020 and 10 million by 2022.

Performance needs

Moeda's ecosystem platforms have achieved:

- Low cost of transaction (~0)
- Transaction cost <\$0.00001
- Funds cleared 3-5 seconds
- transactions per second 1.000+
- Energy per transaction 0.03Wh
- Scale capacity to analyse and approve 200 projects weekly (from wallet to projects, investors to results)
- Firmness MDABRL parity with The Fiat Brazilian Reais
- Easiness Hyperledger Fabric Projects token flow integration to Moeda Seed Projects transparent accountability
- Hyper-secure from the top down: Private keys are always encrypted and cannot be extracted, imported or compromised
- Decentralized architecture: Transactions require multiple layers of authentication via key signing. No single point of failure

Legal considerations

To achieve MOEDAs mission of connecting disadvantaged entrepreneurs to modern financial systems we aim to license our proprietary technologies and operate our fiat-crypto services in a global scale. That's why we have established Moeda's Exchange company in Uruguay free-trade zone, a special economic zone part of the Latin America Free Trade Association (LAFTA).

We are encouraged by the Uruguayan governments business-friendly environment and we have many advantages, including tax exemptions, unfettered foreign currency trading and logistical support. Also, the introduction and trade of foreign currency, gold, precious metals, and public values, is completely free.

Like in the rest of the Uruguayan territory, inflow and outflow of foreign currency is free.

U.S. investment bank Merrill Lynch, India's Tata Consulting and copier maker Ricoh are among international companies that have established operations in Uruguay's free-trade zones, according to published reports.

Moeda plans to maximize its use by being established in free-trade zones in Uruguay and other countries to improve the overall trade efficiency of its clients and partner organizations.

MOEDA has pledged to the Brazilian Central Bank, Brazilian tax authorities and regulatory bodies that it will maintain a transparent-and-compliant digital banking venture that will regularly provide information about its seed projects and other operations in the country.

External References and Miscellaneous

www.moedaseeds.com

Emoney Token Standard

Section 1: Summary

Use Case Summary			
Use Case ID:	FIN-008	Use Case Type:	<i>Vertical</i>
Submission Date:	July 19, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Emoney Token Standard	Domain:	<i>1</i>
Status of Case	<i>In Production, ready.</i>	Sub-Domain	B- International & interbank payments
Contact information of person submitting/managing the use-case	<i>Full Name: Ismael Arribas Web site: https://emoneytokenstandard.org/ standards@alastria.io</i>		
Proposing Organization	Iobuilders (Kingdom of Spain). B-88104054		
Short Description	A proposed standard for e-money, bank and central bank money issued tokens		
Long description	<p>Financial institutions work today with electronic systems which hold account balances in databases on core banking systems. In order for an institution to be allowed to maintain records of client balances segregated and available for clients, such institution must be regulated under a known legal framework and must possess a license to do so. Maintaining a license under regulatory supervision entails ensuring compliance (i.e. performing KYC on all clients and ensuring good AML practices before allowing transactions) and demonstrating technical and operational solvency through periodic audits, so clients depositing funds with the institution can rest assured that their money is safe</p> <p>here are only a number of potential regulatory license frameworks that allow institutions to issue and hold money balances for customers (be it retail corporate or institutional types). The most important and practical ones are three:</p> <p>Electronic money entities: these are legally regulated vehicles that are mostly used today for cash and payments services, instead of more complex financial services. For example prepaid cards or online payment systems such as PayPal run on such schemes. In most jurisdictions, electronic money balances are required to be 100% backed by assets, which often entails holding cash on an omnibus account at a bank with 100% of the funds issued to clients in the electronic money ledger</p>		

	<p>Banking licenses: these include commercial and investment banks, which segregate client funds using current and other type of accounts implemented on core banking systems. Banks can create money by lending to clients, so bank money can be backed by promises to pay and other illiquid assets</p> <p>Central banks: central banks hold balances for banks in RTGS systems, similar to core banking systems but with much more restricted yet critical functionality. Central banks create money by lending it to banks, which pledge their assets to central banks as a lender of last resort for an official interest rate</p> <p>Regulations for all these types of electronic money are local, i.e. only valid for each jurisdiction and not valid in others. And regulations can vary dramatically in different jurisdictions - for example there are places with no electronic money frameworks, on everything has to be done through banking licenses or directly with a central bank. But in all cases compliance with existing regulation needs to be ensured, in particular:</p> <p>Know Your Customer (KYC): the institution needs to identify the client before providing them with the possibility of depositing money or transact. In different jurisdictions and for different types of licenses there are different levels of balance and activity that can be allowed for different levels of KYC. For example, low KYC requirements with little checks or even no checks at all can usually be acceptable in many jurisdictions if cashin balances are kept low (i.e. hundreds of dollars)</p> <p>Anti Money Laundering (AML): the institution needs to perform checks of parties transacting with its clients, typically checking against black lists and doing sanction screening, most notably in the context of international transactions</p> <p>Beyond cash, financial instruments such as equities or bonds are also registered in electronic systems in most cases, although all these systems and the bank accounting systems are only connected through rudimentary messaging means, which leads to the need for reconciliations and manual management in many cases. Cash systems to provide settlement of transactions in the capital markets are not well connected to the transactional systems, and often entail delays and settlement risk.</p> <p>The EM Token builds on Ethereum (Corda and others is under study), standards currently in use such as ERC20, but it extends them to provide few key additional pieces of functionality, needed in the regulated financial world:</p> <p>Compliance: EM Tokens implement a set of methods to check in advance whether user-initiated transactions can be done from a compliance point of view. Implementations must `require` that these methods return a positive answer before executing the transaction</p>
--	---

	<p>Clearing: In addition to the standard ERC20 `transfer` method, EM Token provides a way to submit transfers that need to be cleared by the token issuing authority offchain. These transfers are then executed in two steps: 1. transfers are ordered 1. after clearing them, transfers are executed or rejected by the operator of the token contract</p> <p>Holds: token balances can be put on hold, which will make the held amount unavailable for further use until the hold is resolved (i.e. either executed or released). Holds have a payer, a payee, and a notary who is in charge of resolving the hold. Holds also implement expiration periods, after which anyone can release the hold. Holds are similar to escrows in that they are firm and lead to final settlement. Holds can also be used to implement collateralization</p> <p>Funding requests: users can request for a wallet to be funded by calling the smart contract and attaching a debit instruction string. The tokenizer reads this request, interprets the debit instructions, and triggers a transfer in the bank ledger to initiate the tokenization process</p> <p>Payouts : users can request payouts by calling the smart contract and attaching a payment instruction string. The (de)tokenizer reads this request, interprets the payment instructions, and triggers the transfer of funds (typically from the omnibus account) into the destination account, if possible. Note that a redemption request is a special type of payout in which the destination (bank) account for the payout is the bank account linked to the token wallet</p> <p>The EM Token is thus different from other tokens commonly referred to as "stable coins" in that it is designed to be issued, burnt and made available to users in a compliant manner (i.e. with full KYC and AML compliance) through a licensed vehicle (an electronic money entity, a bank, or a central bank), and in that it provides the additional functionality described above so it can be used by other smart contracts implementing more complex financial applications such as interbank payments, supply chain finance instruments, or the creation of EM-Token denominated bonds and equities with automatic delivery-vs-payment</p>
SDG in Focus (when applicable)	<i>SDG9 and SDG17</i>
Value Transfer:	We will transfer claims off-chain with on-chain proofs. Ponderation of attributes by causality. Verified authority to attest and authenticate an attribute.
Types of Users:	People, Organizations, E.money entities, Banks, Central Banks

Stakeholders	<p><i>As we are proposing a money standards issuer and token holders are involved, that means any stakeholder is applied,</i></p>
Data:	<p>https://github.com/ethereum/EIPs/pull/2020 https://emoneytokenstandard.org</p> <p>All the data flow is fully detailed at</p> <p>https://github.com/IoBuilders/holdable-token</p> <p>https://github.com/IoBuilders/payoutable-token</p> <p>https://github.com/IoBuilders/clearable-token</p> <p>https://github.com/IoBuilders/fundable-token</p>
	<p>Privacy by design: unlinkable actions.</p>
Identification:	<p><i>On next releases the idea is to link the identity to SSI schemas. Having said that all the information, balances, accumulates etc, want to be kept confidential. The standard workgroup is actively working on a confidential token approach, researching and implementing homomorphic encryption, range proofs, nnd pedersen commitments.</i></p> <p>https://crypto.stanford.edu/bulletproofs/</p>
Predicted Outcomes:	<p>Urion.io (IoBuilders project) is already live and shows a production ready application, working under the Alastria network, managing real tokenized euros. Other uses cases have deployed under Pegasys Pantheon and JP Morgan Quorum based networks.</p> <p>Adhara, has already deployed the standard under a Singapore, Philippines payment corridor project.</p> <p>Adhara is going to deploy a use case with the South African Reserve Bank in Q4 2019.</p> <p>IoBuilders is going to deploy a use case with the BME, the Spanish CSD, on a bond issuing platform in Q4 2019.</p>

Overview of the Business Problem or Opportunity
Blockchain technology is starting to be seen with huge potential to speed up the fintech innovation. Banks and financial institutions, are envisioning smart money and payments scenarios leveraged by blockchain and smart execution. To enable fully regulated payment scenarios, with

fiat tokenized money, tokens must be issued under e-money/ bank / central bank rules, and directives.

Standardization is key to enable interoperability and cross use case integration. The standard has been started and developed with the aim of enable global interoperability, on tokenized fiat money issuances and payments..

Why Distributed Ledger Technology?

Advantages of fiat money tokenization on the blockchain are as following:

- Use of the universal blockchain protocol based on a continuous and interconnected chain of blocks that provides unification and universality of interactions for various market participants;
- High level of security due to inability to post-factum change the chain of blocks / tamper proof)
- Token issuers can directly communicate with parties interested in any payment use case
- Traceability
- Unique source of truth
- Auditability and transparency (by regulators)

Section 2: Current process

Current Solutions

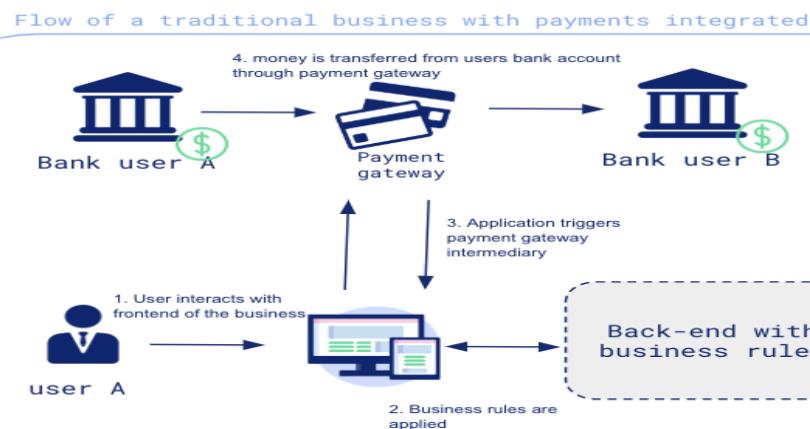
On [Eurion.io](#) lowest KYC level, has been implemented, allowing to have a yearly 1000 € limit and 250 per operation

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	User Identification (KYC)	As money holders, all users need to be identified. Either central banks, banks or e-money entities need to identify users, following the established KYC rules. Based on the level of identification, users are able to manage different amounts of money.
2.	Cashin	Cashin is done via the banking system, either using payment gateways or SEPA, SWIFT communication

Existing Flow (as-is)

Step	User Actions	System Actions
3.	Transfer	SEPA, SWIFT communication based on ISO 20022 payments standards and bank integrations
4,	Transfer with Hold	SEPA, SWIFT communication with ISO 20022 payments standards and bank integrations
5.	Cashout	SEPA, SWIFT communication with ISO20022 payments standards and bank integrations

Process scheme (as-is)



Data and information (as-is)

Data	Type	Description
1	Documents	All the identification process has important documents associated: KYC0: OTP validated mobile phone KYC1: Validated ID document KYC2: Biometric patterns linked to ID, income data, and personal IBAN Information KYC4: KYC template
2	Payment transactions	Cashin, Transfer and cashout

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Lawyers</i>	Kyc and AML process definition
2	<i>Bank, Central Bank, and Emoney License</i>	Money issuer
3	<i>User</i>	Money holder
4	<i>Clearing Agent</i>	Allows a clearable operation to be fulfilled

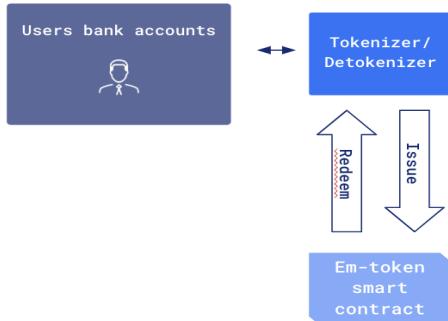
Other Notes
<i>No.</i>

Section 3: Expected process

Expected Flow (TO BE)		
Step	User Actions	System Actions
1.	User Identification (KYC)	As money holders, all users need to be identified. Either central banks, banks or e-money entities need to identify users, following the established KYC rules. Based on the level of identification, users are able to manage different amounts of money. On Eurion.io lowest KYC level, has been implemented, allowing to have a yearly 1000 € limit and 250 per operation. On chain configuration is done via EIP 2009
2.	Cashin	Once users have been identified, they can start using tokenized cash. There are 2 ways of being able to receive tokenized money, via an existing user that natively transfers money, or via baking system based cashin operation, either via credit card or SEPA transfer. All Eurion users, have an unique IBAN associated to its ethereum address. This cashin operation, can be executed on a centralized or decentralized way, via the funding method provided by the standard. On invocation, the token issuer, will read the payment transaction and mint the required tokens (EIP 2019)
3.	Transfer	A native transfer between token holders.
4,	Transfer with Hold	In some cases, native transfer want to be validate or cleared by a third party, On this case mixing the hold and clearing capabilities of the standard, such kind of transactions can be easily implemented.(EIP 2019)
5.	Cashout	An cashout operation, can be executed on a centralized or decentralized way, via the payout method provided by the standard. On invocation, the token issuer, will read the payment transaction and burn the required tokens. (EIP 2021)

Process scheme (to-be)

Money tokenization explanation



- When money reaches the account of a user of ioCash, the bank/EME notifies us.
- The tokenizer issues the corresponding amount of tokens over the decentralized ledger into our Em-token smart contract
- Now, money is digital, programmable and interoperable
- When the user orders a redemption, the detokenizer burns the tokens on the smart contract
- Money is moved from the client ioCash account to the destination

Participants and their roles

Actor	Type/Role	Description
1	<i>Lawyers</i>	Kyc and AML process definition
2	<i>Bank, Central Bank, and Emoney License</i>	Money issuer
3	<i>User</i>	Money holder
4	<i>Clearing Agent</i>	Allows a clearable operation to be fulfilled
5	<i>Hold Operator</i>	Allows a held operation to be fulfilled

Data and information

Data	Type	Description
1	<i>Documents</i>	All the identification process has important documents associated: KYC0: OTP validated mobile phone KYC1: Validated ID document KYC2: Biometric patterns linked to ID, income data, and personal IBAN Information KYC4: KYC template
2	<i>Payment transactions</i>	Cashin, Transfer and cashout

Security and privacy

All the standard is based on current ethereum capabilities and ourion.io has been developed following all the security and ISO standards and specifications.

Main Success Scenario + expected time line

[Ourion.io](#) (IoBuilders project) is already live and shows a production ready application, working under the [Alastria](#) Ecosystem, managing real tokenized euros. Other use cases have deployed under Pegasys Pantheon and JP Morgan Quorum based networks.

[Adhara](#), has already deployed the standard under a Singapore, Philippines payment corridor project.

Adhara is going to deploy a use case with the South African Reserve Bank in Q4 2019.

[IoBuilders](#) is going to deploy a use case with the BME, the Spanish CSD, on a bond issuing platform in Q4 2019.

Conditions (pre- or post-)

Non applicable.

Performance needs

Current Ethereum landscape is totally focused on scalability, due the low transnationality, throughput available either on private or public networks..

Legal considerations

Electronic Money License, Anti-money laundering compliance and KYC regulation.

Risks

Scalability and confidentiality. (mentioned before)

Special Requirements

Financial institutions share a common platform and data overview.

External References and Miscellaneous

<https://io.cash/product/>

Other Notes

It is possible to be tested for free by the ITU-T FG DLT experts and members.

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)
-

Public Sector Lending Transparency

Section 1 Summary

Use Case Summary			
Use Case ID:	GOV-001	Use Case Type:	Vertical
Submission Date:	May 28, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Public sector lending transparency	Domain:	Government and public sector
Status of Case	Pilot	Sub-Domain	Government and non-profit transparency
Contact information of person submitting/managing the use-case	Full Name: Suzana Mesquita de Borba Maranhão Moreno (BNDES) Job Title: Software Engineer E-mail address: suzana@bndes.gov.br Telephone number: 55-21-993056325 Social media: https://www.linkedin.com/in/suzana-moreno/ Web site: https://www.bndes.gov.br		
Proposing Organization	BNDES, Brazil		
Short Description	This use case is a proposal for changing the process of lending projects in The Brazilian Development Bank using a stable coin with DLT technology. The main goal is achieve more transparency of the public money allocation. However, the new proposal achieve other benefits like operational costs reduction and the generation of data to support aggregate analysis of the benefits arising from the bank's loans.		
Long description	This use case is a proposal for changing the process of lending projects in The Brazilian Development Bank using a stable coin with DLT technology. The stable coin is used when disbursing money from BNDES to the client and from the client to contractors. Then, the contractor can redeem to get its fiat money. It is a closed ecosystem between BNDES, clients and contractors in order to avoid regulatory risks. In order to achieve the desired transparency, it is necessary to identify everyone who do transactions using the stablecoin. In future view, there is also important to identify services and products offered from contractors to clients. The main goal is achieve more transparency of the public money allocation. However, the new proposal achieve other benefits like operational costs reduction and the generation of data to support aggregate analysis of the benefits arising from the bank's loans.		
SDG in Focus (when applicable)	16 – Peace, Justice and Strong Institutions		

Value Transfer:	Tokens representing fiat money	Number of Users:	20+
Types of Users:	Development bank, Lender, Contractor, Society		
Stakeholders	Government, Development bank (or Public agency), Commercial banks, Lender, Contractor, Society, Auditor		
Data:	<p>=> Use case shared data (ideally stored in DLT):</p> <ul style="list-style-type: none">- Entity identification (link between DLT account and real world entity identification)- Product or service type identification (Future Vision only) <p>=> Use case specific DLT data:</p> <ul style="list-style-type: none">- Account- Token balance to each account- Project identification- Instances of use case shared data identification <p>=> External data - not stored in DLT:</p> <ul style="list-style-type: none">- Entity additional information (number of employees, revenue, geographic region, industry, sector etc.) <p>=> All public information (see Security and privacy section).</p>		
Identification:	Full identification of Lenders and Contractors required by the development bank		
Predicted Outcomes:	<p>The predicted outcomes of adopting the new process are to:</p> <ul style="list-style-type: none">- increase transparency of public money allocation- make clients' proofing of their spending simpler- reduce audit and compliance costs- improve public money allocation by postponing fiat money lending- minimize time to publish lending information- produce data to do aggregate analysis of the benefits arising from the development bank's loan		

Overview of the Business Problem or Opportunity

- In general, society demands more transparency in the use of public money.
 - The development bank uses public money to finance projects that adhere to government

development policies priorities.

- The society does not trust the development bank.

- The development bank needs to verify that the public money is being used as planned.

- Periodically, lenders need to prove each money spending, including transfer to contractors.

- The development bank needs to verify that lenders' proof correctly demonstrates that the public money was used as planned.

- Auditors verify that the development bank indeed has assessed lenders' money spending.

- Maximizing process automation would increase processes efficiency, while reducing the development bank's verification and audit costs.

- The process information of lending is fragmented.

- The development bank owns the projects and disbursements data. Each lender or contractor has its transfer data.

- Transfer data is protected by commercial banks - financial privacy.

- The development bank has to collect transfer data in order to publish lending information to society.

- The development bank does not have contractor's registry.

- The development bank has to collect and group data to demonstrate benefits arising from the development bank's loans.

- Integrating data would improve the process efficiency, while minimizing cost.

- In order to minimize paperwork, the development bank disburses to lenders large amounts of money.

- Lenders take some time to spend all the money so they have to invest the funds. If the value of investment interest rate is bigger than the value of the lending interest rate, lenders may have an incentive to postpone the project schedule.

- To make disbursement date and money spending date closer would improve the process efficiency and improve fiat money allocation.

Why Distributed Ledger Technology?

DLT would improve the current solution because it is possible to achieve public money loans transparency without trusting the development bank. Transfer data become easily accessible and can be used to make the underlying processes of lender's proof of money spending and the process of collecting and publishing loans benefits simpler and more efficient.

In addition, the use of DLT token enables the development bank to disburse fiat money just-in-time. Many times the money can flow to contractors directly.

Section 2 Current process

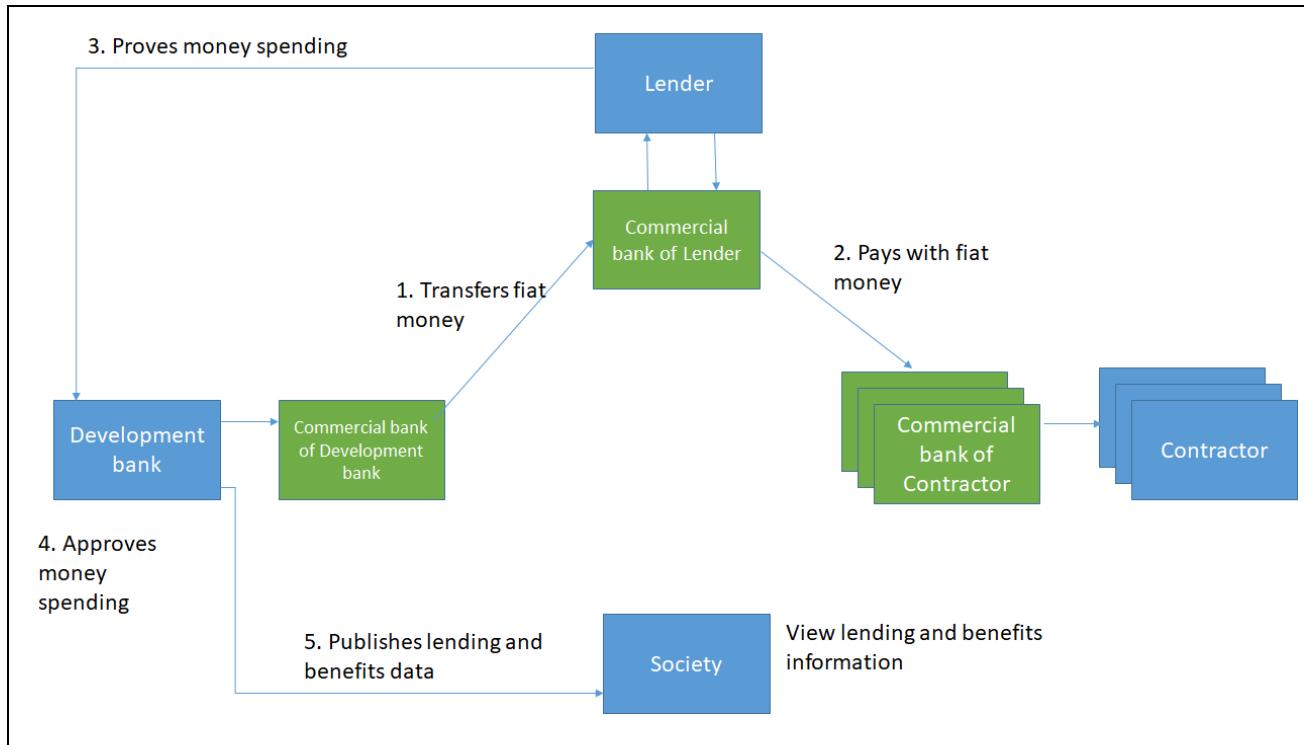
Current Solutions

Value is transferred by corresponding banks; There is a lot of manual work to prove and validate money spending; There is a lot of manual work to publish lending and benefits data; Lending and benefits data can be manipulated by the development bank; There is no data publication in real time.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	The development bank makes a transfer of fiat money to lender using the service of commercial banks.	The development bank's internal system registers the transfer Each commercial bank updates its ledger The lender's internal system registers the transfer
2.	The lender pays some contractors using a service of commercial banks. It can take a while to spend all money.	For each payment: The lender's internal system registers the payment Each commercial bank updates its ledger The contractor's internal system registers the payment
3.	The lender proves his money spending to the development bank.	The development bank system register the lender's spending proof
4.	The development bank approve lender's money spending. It can involve a lot of manual work.	The development bank system changes disbursement status
5.	The development bank publishes lending and benefits data	N/A

Process scheme (as-is)



Data and information (as-is)		
Data	Type	Description
1	Fiat money transactions	The way value is transferred between: (a) the development bank and the lender and (b) the lender and contractors
2	Money spending proof	Documents, images etc used to proof the money was used as planned. It must include commercial bank statements to proof that the lender paid contractors and what products or services type were commercialized.
3	Lending data	Detailed information about each transaction, including who the lender and the contractors were, what time each transaction happened and what the value of each transaction was, what product or service type was commercialized in each transaction.
4	Benefits data	Aggregate information about transactions joined with entities additional information. Examples: How many transactions involved companies with small revenues? How much money was transferred in a geographic region or an industry?

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Development bank	Financial institution designed to provide medium- and long-term capital for productive investment

2	Commercial bank	Financial institution to provide transfer/payment between parts
3	Lender	Entity who takes the loan with the development bank
4	Contractor	Entity who sells a product or service to the lender
5	Society	Everyone who is interested to know how the public money was allocated and what were the benefits of that

Other Notes

Some steps must occur before the described use case but are not relevant to the description:

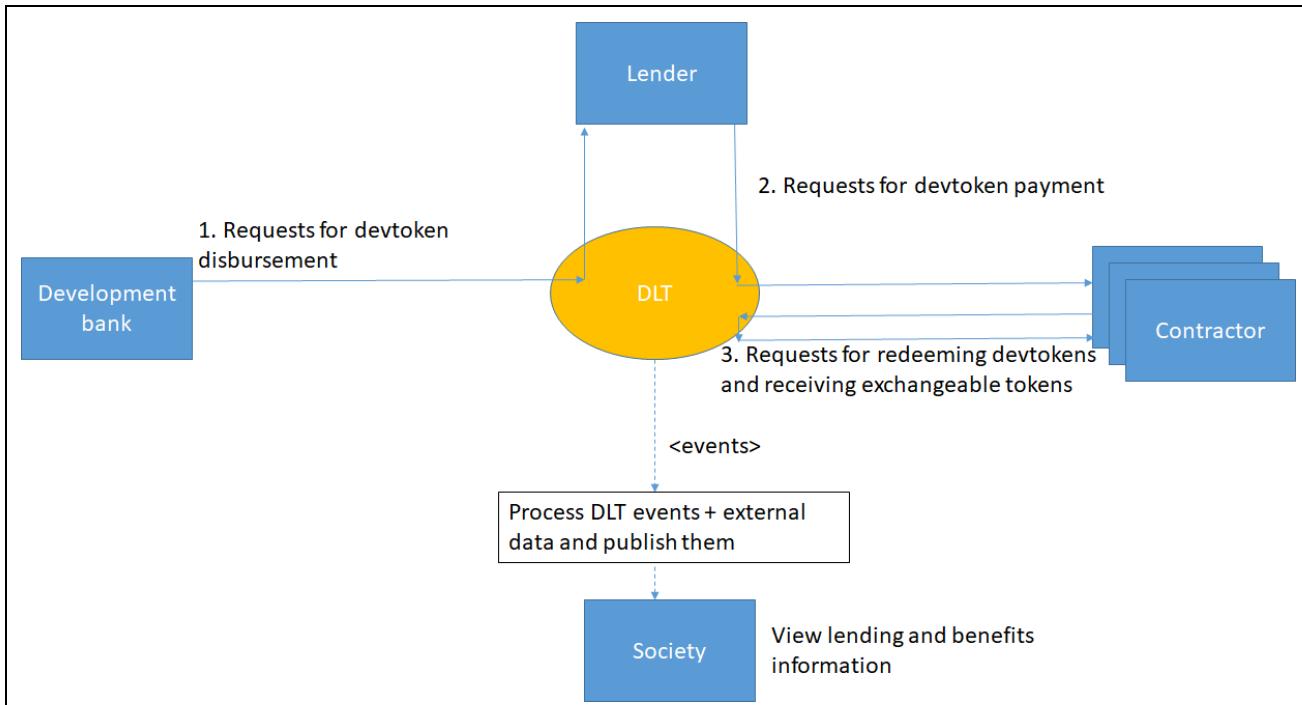
- The development bank must approve a development project within a contract. The contract must state the conditions of each public money disbursement;
- The lender must ask for a disbursement to the development bank;
- The development bank approves disbursement to the lender.

Section 3 Expected process

Future Vision

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	The development bank requests for devtoken disbursement.	<p>DLT checks the development bank is authorized and the lender is enabled to receive devtokens. If true, DLT mints new devtokens and transfers them to the lender's address.</p> <p>DLT emits <disbursement event>.</p>
2.	The lender request for devtoken payment	<p>DLT checks the lender is authorized and has enough balance and the contractor is enabled to receive devtokens.</p> <p>If true, DLT transfers devtokens to the contractor. This transfer demonstrate what the product or service commercialized are. In addition, it has legal value to be used as lender's proof of money spending.</p> <p>DLT emits <payment event>.</p>
3.	A contractor requests for redeeming devtokens and receiving exchangeable tokens * At some point before, the development bank must input enough exchangeable token in DLT.	<p>DLT checks the contractor is authorized and has enough balance and the smart contract has enough exchangeable tokens.</p> <p>If true, DLT burns the received devtokens, makes the conversion between the devtoken value and the exchangeable token value and transfers the corresponding exchangeable token value.</p> <p>DLT emits <redemption event>.</p>
Trigger event	N/A	When a trigger event of DLT is observed, a system updates the lending and benefits information.

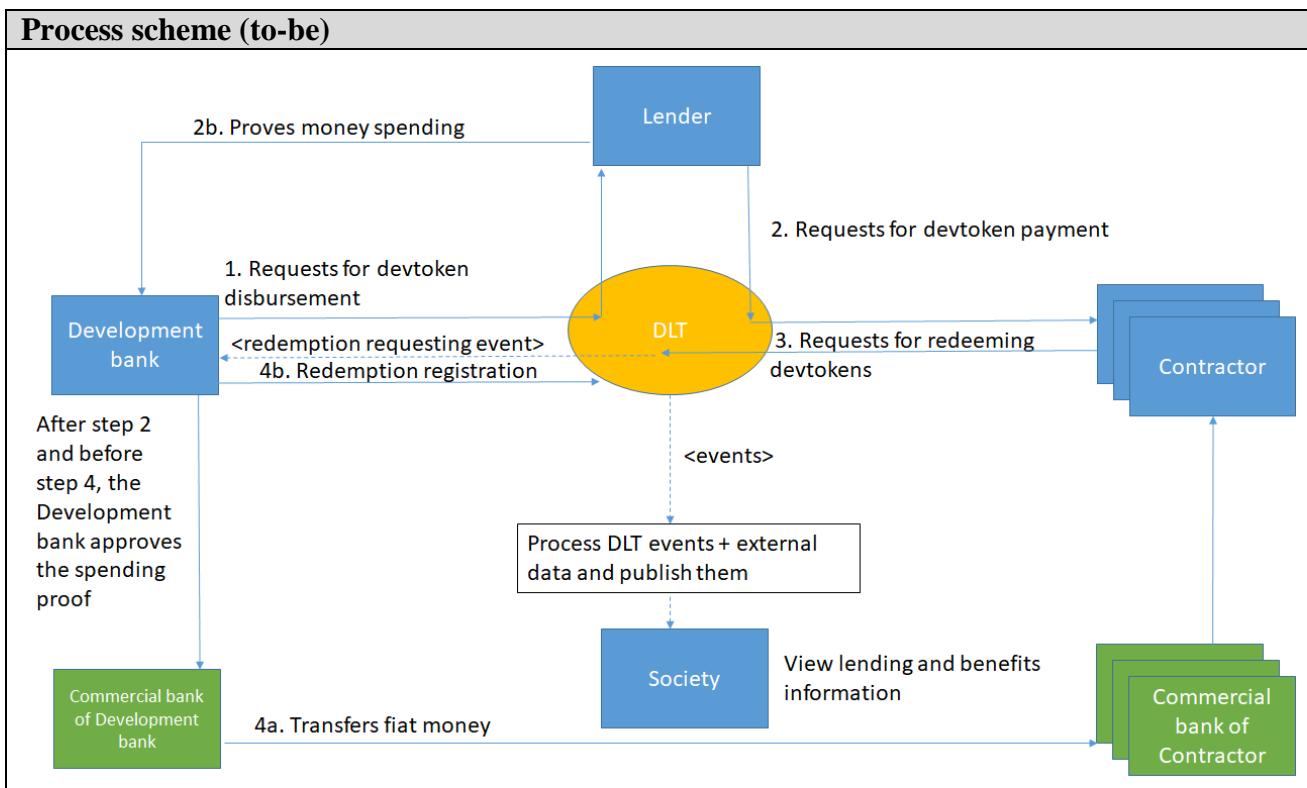
Process scheme (to-be)



Transition Vision

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	The development bank requests for devtoken disbursement.	<p>DLT checks the development bank is authorized and the lender is enabled to receive devtokens. If true, DLT mints new devtokens and transfers them to the lender's address.</p> <p>DLT emits <disbursement event>.</p>
2.	<p>The lender request for devtoken payment. (2a)</p> <p>At the same time, proves his money spending to the development bank. (2b)</p>	<p>DLT checks the lender is authorized and has enough balance and the contractor is enabled to receive devtokens.</p> <p>If true, DLT transfers devtokens to the contractor. (2a)</p> <p>This transfer does not demonstrate what the product or service commercialized. Then, although the transfer contains devtoken values*, it cannot be used as <u>complete</u> spending proof.</p> <p>* Since devtoken values are available to DLT, it is possible to update published lending and benefits data when trigger event is fired.</p> <p>DLT emits <payment event>.</p> <p>The development bank system register the lender's money spending proof. (2b)</p>
3.	A contractor requests for	DLT checks the contractor is authorized and has

	redeeming devtokens	enough balance. If true, DLT burns the received devtokens and emits <redemption request event>.
After step 2 and before step 4	The development bank approves the money spending proof.	The development bank system changes disbursement status.
4.	The development bank observe that a redemption request event has occurred. The development bank pays the contractor using a service of commercial banks. (4a)	The development bank's internal system registers the payment (4a) Each commercial bank updates its ledger (4a) The contractor's internal system registers the payment (4a) DLT emits <redemption event>. (4b)
Trigger event	N/A	When a trigger event of DLT is observed, a system updates the lending and benefits information.



Future and Transition Vision

Participants and their roles		
Actor	Type/Role	Description

1	Development bank	Financial institution designed to provide medium- and long-term capital for productive investment
2	Commercial bank	Financial institution to provide transfer/payment between parts
3	Lender	Entity who takes the loan with the development bank
4	Contractor	Entity who sells a product or service to the lender
5	Society	Everyone who is interested to know how the public money was allocated and what were the benefits of that

Data and information		
Data	Type	Description
1	Devtoken	Token representing fiat money value. It is used to transfer value between: (a) the development bank and the lender and (b) the lender and contractors. It cannot be transferred to a entity who is not registered and enabled to receive devtoken. The token should only be used to execute the associated development project.
2	Fiat money transactions	The way fiat money is transferred between: (a) the development bank and contractors in the transitional vision
3	Money spending proof	Documents, images etc used to proof the money was used as planned in the transitional vision. It must include what products or services type were commercialized. It does not need to include commercial bank statements since this information is available at DLT.
4	Exchangeable token	A token that can be exchanged by fiat money or other cryptocurrency without use the devtoken smart contract.

Security and privacy
<ol style="list-style-type: none"> 1. Since transparency is the main requirement, the ideal information visibility is public; 2. If business privacy prevent public visibility, this critical subset of data can be encrypted or protected; 3. DLT system should be able to provide mechanisms of DLT data integrity control; 4. DLT data and related services (System Actions) should be available in 24/7/365 mode; 5. The entity identity solution should prevent identity fraud. 6. The products and services type identification solution should prevent fraud. (Future Vision only)

Main Success Scenario
<ol style="list-style-type: none"> 1. All information exchange and payments occur in Distributed Ledger in automatic mode; 2. Payments are transferred using digital currency (either devtoken or an exchangeable token);

- | |
|--|
| 3. Money spending proof occurs without human verification; |
| 4. Lending and benefits data published without human intervention. |

Conditions (pre- or post-)

- | |
|---|
| 1. The development bank must have established a financial contract with lenders; |
| 2. Lenders and contractors who receive devtokens must be registered in the identity solution and enabled to receive devtoken; |
| 3. Products and services types used in devtoken transactions must be registered in Product or service type identification (Future Vision only); |
| 4. Devtoken smart contract must be deployed; |
| 5. All parties are connected to DLT-network. |

Performance needs

- | |
|---|
| 1. Transactions processing near real time; |
| 2. 24/7/365 availability; |
| 3. Volume of disbursements > 1000 Tx/day, volume of transactions > 10.000 Tx/day; |
| 4. Lending and benefits data published in the moment they are available (near real time). |

Legal considerations

Changing how a lender proves his money spending has legal impacts.
--

Risks

- | |
|---|
| 1. Legal risks, including regulation of cryptocurrencies, money spending proofing and taxation; |
| 2. Security risks; |
| 3. Contractors do not accept devtokens; |
| 4. Lenders do not want devtokens; |
| 5. Risks related to DLT immaturity. |

Special Requirements

N/A

External References and Miscellaneous

- | |
|-----------------------------------|
| 1. Project using this use case => |
|-----------------------------------|

Brazilian State Bank to Tokenize Brazilian Real on Ethereum's Public Blockchain - https://www.trustnodes.com/2018/03/06/brazilian-state-bank-tokenize-brazilian-real-ethereums-public-blockchain
--

Other Notes

1. For simplicity, this use case does not describe a scenario where:

- Lender can request for redemption
 - Contractor can transfer devtoken again
-

Trubudget for the Amazon Fund

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-002	Use Case Type:	<i>Vertical</i>
Submission Date:	March 22, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Trubudget for the Amazon Fund	Domain:	<i>4. Government and public sector</i>
Status of Case	<i>Pilot</i>	Sub-Domain	<i>b. Government and non-profit transparency</i>
Contact information of person submitting/managing the use-case	<p><i>José Nogueira D'Almeida Jr.</i> <i>Software Engineer</i> <i>nogueiradalmeida@gmail.com</i> <i>+55 (21) 97189-2811</i> <i>https://www.linkedin.com/in/nogueiradalmeida/</i> <i>www.bnDES.gov.br</i></p>		
Proposing Organization	<i>BNDES – Brazilian Development Bank</i>		
Short Description	<p><i>Trubudget for the Amazon Fund is a blockchain system that improves the reliability of the information providing the money tracking for the investments of Amazon Fund in Brazil.</i></p>		
Long description	<p><i>The Amazon Fund is a REDD+ mechanism created to raise donations for non-reimbursable investments in efforts to prevent, monitor and combat deforestation, as well as to promote the preservation and sustainable use in the Brazilian Amazon.</i></p> <p><i>The Amazon Fund is managed by BNDES, the Brazilian Development Bank, which is responsible for raising and investing funds, monitoring the projects supported, rendering accounts and communicating results obtained.</i></p> <p><i>Germany is one of the main donors of Amazon Fund. The Germany's Development Bank KfW and BNDES are cooperating to use the blockchain technology to record how funding is spent. The Trubudget is a generic blockchain system that allows to register workflows. The Trubudget for the Amazon Fund is an use case that registers the money flow. It started in 2017, it had a Proof-of-Concept Phase in 2018 which consisted in simulations with real clients and in 2019 is in the Pilot Phase, which consists in real disbursement monitored and controlled by the blockchain. The payments process from BNDES to its Clients was the choice to be recorded on Trubudget blockchain in the Pilot Phase.</i></p>		

SDG in Focus (when applicable)	<i>Goal 6 – Clean Water and Sanitation Goal 13 – Climate Action Goal 15 – Life on Land Goal 16 – Peace, Justice and Strong Institutions Goal 17 – Revitalize the global partnership for sustainable development</i>		
<i>All these objectives are related to the Amazon Fund and the Trubudget aims to improve the management of it.</i>			
Value Transfer:	<i>There is no value transfer in the blockchain solution described. This is a declarative ledger.</i>	Number of Users:	<i>30+</i>
Types of Users:	<i>BNDES Business Analyst BNDES-Clients Business Analyst Auditors Donors Government agencies</i>		
Stakeholders	<i>BNDES, KfW(Germany), Petrobras, TCU (government agency), Norway</i>		
Data:	<i>Users Projects Subprojects Workflow items</i> <i>There is a communication between Trubudget and the ERP System, which every disbursement that occurs in the ERP, it makes a new record in the respective Trubudget Subproject.</i>		
Identification:	<i>Every user has credentials (login and password) to use the system. Some users have admin power, which means that they can create other credentials. Projects, Subprojects and Workflows items need permission of its owner to read/write.</i>		
Predicted Outcomes:	<i>Trubudget aims to be an additional source of information in a blockchain for the stakeholders monitor the Amazon Fund projects. The system is able to provide the Client's, BNDES and Donors access to the same data at any time. This is similar to the Circularization technique commonly used by Audit companies, when the auditor sends a letter directly to a third party to confirm an information about the audited organization. In a future phase, it can replace some process/report that is currently made offchain.</i>		

Overview of the Business Problem or Opportunity

The donors of Amazon Fund and BNDES could be concerned about the correct use of the disbursements for the projects executed by their clients, generally NGOs. This system can improve the timing of the information and the reliability of it.

Why Distributed Ledger Technology?

Every stakeholder (Donor, BNDES, Clients/NGOs) has its system and provide the information of money expenditure using the traditional ways (emails, documents, spreadsheets, receipts, etc).

The Trubudget for the Amazon Fund integrates this information in one blockchain system, where

the data is immutable, secure, verifiable and transparent.

Section 2: Current process

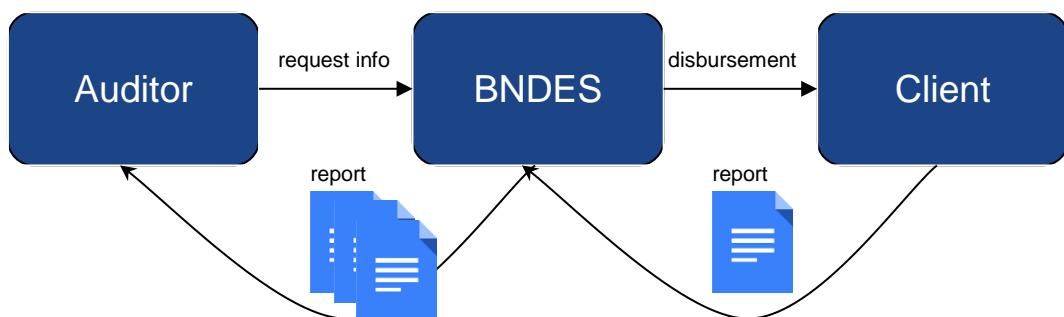
Current Solutions

The disbursements of BNDES are made to its Clients using the traditional Brazilian Payment System (SPB). The Clients executes the project according to the Amazon Fund principles and then reports the expenditure to BNDES. BNDES aggregates all its Clients reports and make its reports to the donors periodically.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	BNDES Analyst submits a disbursement in the ERP system	The ERP system sends a disbursement through the Brazilian Payment System
2.	The Client checks the project bank account	No system action
3	BNDES periodically reports to the Auditor how and when the money was spent	No system action

Process scheme (as-is)



Data and information (as-is)

Data	Type	Description
1	Documents	A report of project ongoing results must be send to BNDES, who manages the Amazon Fund. BNDES collects all those results from its clients, make analysis and then produce its reports to the auditors (donors and government agencies).

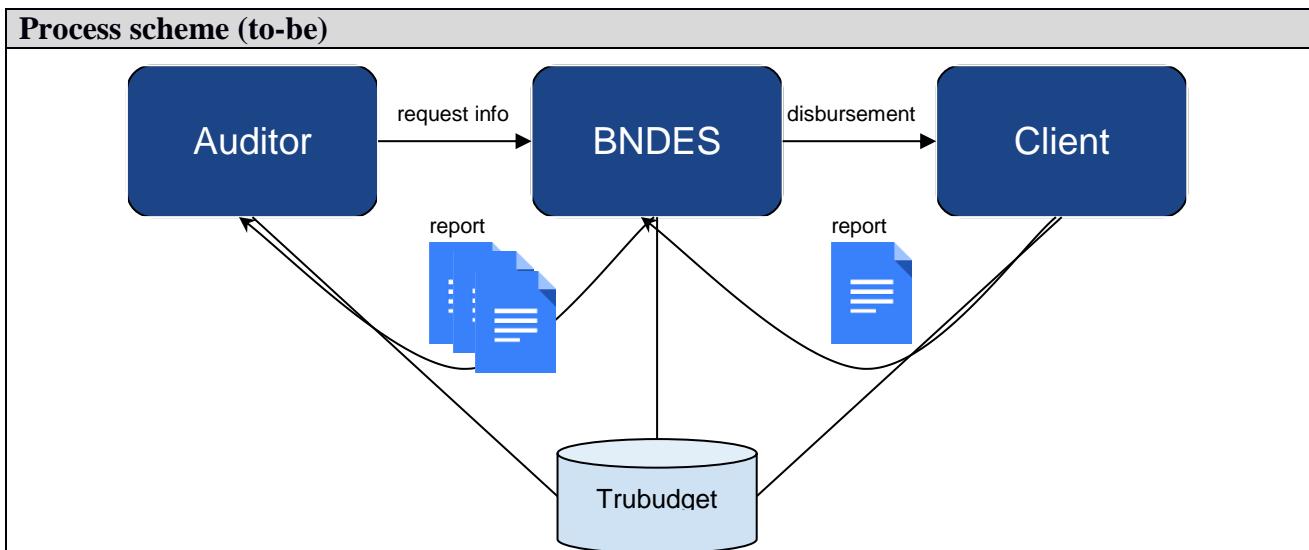
2	<i>Payment transactions</i>	The Clients' expenditures receipts must be send to BNDES.
----------	-----------------------------	---

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>BNDES</i>	Manages the Amazon Fund and evaluate the results of ongoing projects and approves/rejects new projects
2	<i>KfW/Norway</i>	Monitor their donations and audit the BNDES management
3	<i>TCU (as example)</i>	Audit the BNDES Amazon Fund management
4	<i>BNDES Clients</i>	Executes the projects and report the results

Other Notes
N/A

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	BNDES Analyst submits a disbursement in the ERP system	The ERP system sends a disbursement through the Brazilian Payment System and this payment is loaded into Trubudget Ledger. Trubudget sends an email to the Clients
2.	The Client checks the project bank account and then approves the receipt in the Trubudget Ledger.	Trubudget sends an email to BNDES team
3	The Auditor logs on Trubudget at any time and check the money flow for every iteration described in the steps 1 and 2	Trubudget shows every money step through the ledger



Participants and their roles		
Actor	Type/Role	Description
1	BNDES	Manages the Amazon Fund and evaluate the results of ongoing projects and approves/rejects new projects
2	KfW/Norway	Monitor their donations and audit the BNDES management
3	Auditor	Audit the BNDES Amazon Fund management
4	BNDES Clients	Executes the projects and report the results

Data and information

Data	Type	Description
1	<i>Documents</i>	A report of project ongoing results must be send to BNDES, who manages the Amazon Fund. BNDES collects all those results from its clients, make analysis and then produce its reports to the auditors (donors and government agencies).
2	<i>Payment transactions</i>	The Clients' expenditures receipts must be send to BNDES.
3	<i>Trubudget Workflow</i>	All the stakeholders can access Trubudget at any time to check daily the status of each project of the Amazon Fund.

Security and privacy
<i>Application security:</i> <i>The Trubudget has access control to login into the system, as well it offers specific permission for each project, subproject and workflow item.</i>
<i>Network security:</i> <i>The Trubudget network is a permissioned blockchain based on Multichain. Therefore only the approved nodes have the grants to join on this. Currently there are two nodes: BNDES and KfW. Norway and Petrobras were invited to join. The Clients uses the BNDES frontend node.</i>

Main Success Scenario + expected time line
<i>Description of DLT-based solution, which potentially will be created</i>

Conditions (pre- or post-)
<i>Not applicable</i>

Performance needs
<i>Trubudget is based on Multichain permissioned blockchain technology.</i>
<i>The confirmation time in a permissioned networked can vary according to the consensus mechanism, number of nodes, etc. Trubudget does not require real-time update for all nodes. It is desired and viable a few minutes of confirmation time.</i>
<i>Trubudget already contains a Restful API, which supports external calls from other systems.</i>
<i>A few transactions per day are expected on Amazon Fund and since Trubudget is based on Multichain permissioned blockchain technology, the transaction throughput is not an issue.</i>
<i>"In MultiChain you can set the block size limit much higher (up to 1 GB) and the block time much lower (down to 2 seconds), so based on this calculation it could process over 2 million tx/second. But for now the codebase itself can handle a little over 1000 tx/second on mid-range hardware, using either the multichain or bitcoin protocol. (In reality you would also have to consider the connection between block size and propagation latency which affects the minimum viable block time." [https://www.multichain.com/qa/5556/about-throughput-performance]</i>

Legal considerations

There is a possibility that Trubudget could not replace any of the current processes and/or reports because legal and regulatory rules. In fact, at this point, we are considering Trubudget as an additional source of information.

The General Data Protection Regulation in EU law was a concern because Trubudget stores every single data in its blockchain, including emails. Therefore, we decided to use corporate emails to keep only corporate data and avoid personal data.

Risks

Legal, business and technical risks related to use case

The information provided on Trubudget is already open and public by the Amazon Fund.

Trubudget is an opensource project under the MIT License. The software uses other opensource libraries and modules and these external modules can have vulnerabilities.

Special Requirements

The agreement between KfW and BNDES was formalized by a Memorandum of Understanding and if someone does not follow the rules, it can affect the business.

External References and Miscellaneous

KfW Trubudget site:

<https://openkfw.github.io/trubudget-website/>

Trubudget for the Amazon Fund Video Demo:

<https://www.youtube.com/watch?v=0tysH44dzm8&feature=youtu.be>

BNDES Trubudget site:

www.bnmes.gov.br/trubudget

The Trubudget source code:

<https://github.com/openkfw/TruBudget>

The ETL SAP-Trubudget source code:

<https://github.com/bnmes/trubudget-bnmes>

Other Notes

Trubudget for Amazon Fund is workflow management system that tracks the money flow in a blockchain. Its use case is simple. It is an additional and reliable source of information for different stakeholders to follow the donations of the supported projects for the Amazon Forest.

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)
-

Mudamos - Lawmaking

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-003	Use Case Type:	<i>Vertical</i>
Use Case Title:	Mudamos	Is Use Case supporting SDGs	<i>No</i>
Status of Case	<i>Implementation</i>	Sub-Domain	<i>If necessary</i>
Contact information of person submitting/managing the use-case	<p><i>Marco Konopacki Project Coordinator marco@itsrio.org +55 21 999278090 marco@itsrio.org @marcoamarelo http://itsrio.org http://mudamos.org</i></p>		
Proposing Organization	<i>Institute for Technology and Society</i>		
Short Description	<i>Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures.</i>		
Long description	<i>Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures. Any citizen with a smartphone (Android or iOS) can download the app and register with his or her electoral ID, name and address, information which Mudamos keeps secure and verifies with Brazil's Electoral Court. The app issues what is known as a cryptographic key pair, a small piece of code used for verification. One half of the key is stored on the user's phone and the other with Mudamos, which makes it possible to authenticate a person's signature. In this way, members of the public can draft and sign petitions in a way that is verifiable and secure.</i>		
SDG in Focus (when applicable)	<p><i>Enter one or more number (1-17) and specific corresponding indicator/s as applicable</i></p> <p><i>See https://www.un.org/sustainabledevelopment/sustainable-development-goals/</i></p> <p><i>Goal 16: Promote just, peaceful and inclusive societies</i></p>		

Value Transfer:	<i>If potential solution allows to transfer any value (e.g. assets, tokens, etc.)</i>	Number of Users:	350.000
Types of Users:	<i>Voters regular registered to vote.</i>		
Stakeholders	<i>Citizens (engaged citizens in support for law making), Legislative Houses (representatives and public servants).</i>		
Data:	<i>In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks, where they can be publicly scrutinized. This ensures that signature lists are immutable, and if an interested agent wants to audit the entire signing process, from the first signature collected, they have the capability to do it without relying on Mudamos or any other agent.</i>		
Identification:	<i>Auto geranted Private key / Electoral data</i>		
Predicted Outcomes:	<i>Signature lists in support of citizens' initiative draft bills.</i>		

Overview of the Business Problem or Opportunity
<p>Brazil's Constitution provides several direct democratic mechanisms, including the referendum, plebiscite, and citizens' initiatives. The initiative mechanism allows any citizen to propose a draft bill to the lower house of municipal, state or federal legislatures. If the proposal gets the requisite number of signatures from registered voters in support then the campaign organizers present the bill before the House. Once the signatures are verified, the Speaker assigns a House committee to start bill discussion that could lead (or not) to the bill becoming a law. At the federal level, the minimum amount of signatures is 1.5 million, which is problematical to organize using paper-based petitions. Popular initiatives to collect signatures are often paper-based which, apart from being costly, also present problems of transparency and integrity. In fact, no citizen bill has ever been approved at the national level due to the verification barrier and participation costs.</p> <p>Thus Institute for Technology and Society (ITS Rio) created Mudamos in 2017 to reduce the high costs of creating paper-based petitions by offering a verifiable online mechanism for the creation and signing of citizen petitions and offer a robust means of participation that, in turn, should help to raise citizens' degree of trust in political institutions and contribute to the construction of participatory rules and norms.</p>
Why Distributed Ledger Technology?
<p>The uniqueness of the signatures is guaranteed by the association of unique electoral ID number combined with the signature timestamp and the user's private key. The private key generates a unique hash based on the data reported for signature. Verifiability is guaranteed by publishing the user's public key along with the data given for signature and the signature hash. In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks.</p>

Section 2: Current process

Current Solutions
N/A

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Create a campaign for signature gathering	N/A. Paper-based
2.	Paper-based form download from legislative house	Access legislative house website and download form template.
3.	Signature	N/A. Paper-based signature
4.	Present signatures	N/A. Paper-based process. 1.5 million paper-based signatures have an average of 2ton weight.

Process scheme (as-is)

Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	Electoral Personal Data (Name, Electoral ID, ZIP Code) and signature written down on paper-base forms.
2	<i>Payment transactions</i>	N/A

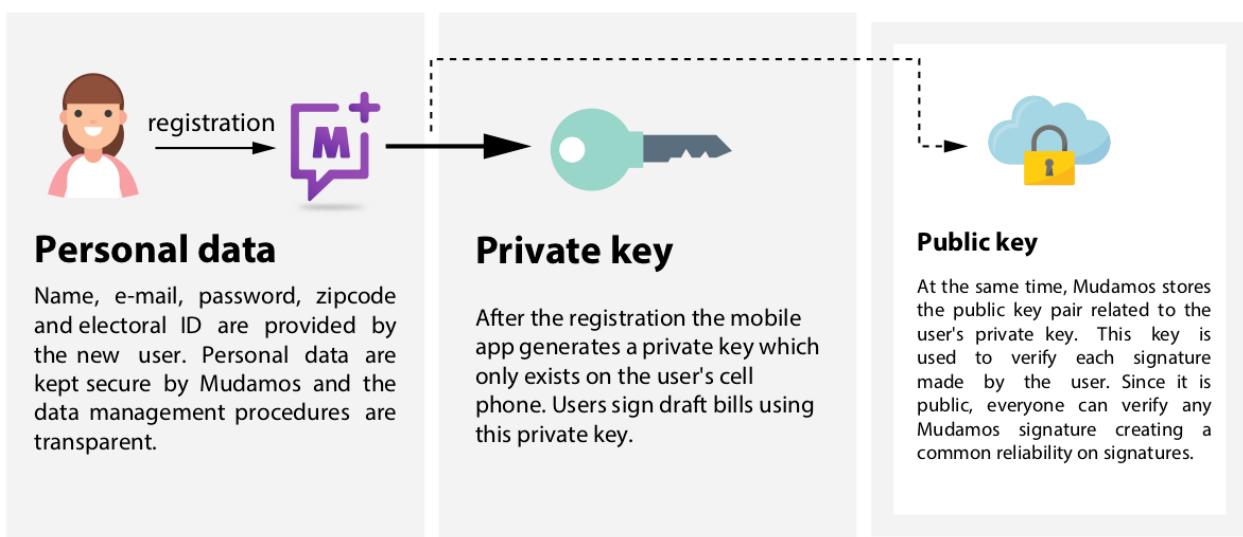
Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Legislative houses</i>	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
2	<i>Signature campaign leaders</i>	People who decide organize campaigns in support for a draft bills and manage all logistics for that.
3	<i>Signers</i>	People how sign in support for a draft bill.

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Register on Mudamos	Generate key pair
2.	User signature	Electoral data hashing based on private key
3.	Signature verification	Checking electoral data against signature hash and user's public key
4.	Check public signature lists	PDF signature list hashes checking on public Blockchains
5.	Reach signatures threshold	Present lists into a flash drive to legislative house speaker to start bill discussion

Process scheme (to-be)





Every user own your unique private key

Sign a draft bill

Personal data is compiled based on the legal Brazilian standard. In addition, Mudamos adds some metadata to strengthen the signature and make it reliable (i.e. timestamp).



L27DH20	HF7D923	2373 FDJ
L27DH20	HF7D923	2373 FDJ
L27DH20	HF7D923	2373 FDJ

Hashing data

The data is hashed by user's private key and the outcome is a cyphered word. This word is the evidence of the user's act in order to support a draft bill.



Signature storage

All the signatures hashes are stored on Mudamos' servers. These signatures can be verified how many times are necessary using the public keys related for each user registration.



Regular publishing

Mudamos regularly compile each draft bill campaign signatures in a single document and make it public to allow every one follow the ongoing process.



Blockchain register

Every signatures document is registered on public Blockchains to ensure its authenticity and integrity, in other words, ensure they were not modified during the signature gathering campaign.



Presenting to a legislative house

The signatures document can be independently verified by the legislative house. In fact, every stakeholder can do your own signature verification without any special resources from Mudamos.

Participants and their roles

Actor	Type/Role	Description
1	<i>System Manager</i>	ITS Rio. Responsible to support Mudamos and make it online.
2	<i>Mudamos users</i>	Brazilian citizens registered to vote who can propose draft bills or sign for existing ones.
3	<i>Legislative houses</i>	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
4	<i>Draft bill proponents</i>	People who propose draft bills to be supported through Mudamos platform.

Data and information

Data	Type	Description
1	<i>Documents</i>	Electoral Personal Data (Name, Electoral ID, ZIP Code) PDF list containing signatures compilation
2	<i>Payment transactions</i>	N/A

Security and privacy

1. Verification process can be automatized
2. On going campaigns lists have personal data anonymized
3. Signature information can be changed by man in the middle attacks due to its verifiability by its signature hash and public key.

Main Success Scenario + expected time line

Description of DLT-based solution, which potentially will be created

Conditions (pre- or post-)

- 1.

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

Legal considerations

Currently, thanks to the Internet and other technologies, it is possible to collect signatures throughout Brazil and verify them automatically. Digital signatures already had their relevance recognized and used in common civic procedures, as instituted by the Presidency Act MPV 2200/2001, and in legal acts, as instituted by Law 11419/06. However, since the cost of obtaining official digital certificates is prohibitive, they did not gain widespread adoption and a mere .005% of Brazilians have them.

Digital signatures based on certificates issued by the Brazilian government have the advantage that they are legally binding, meaning any documents signed using those certificates are recognized by any authority as authentic for any purpose, from the recognition of a debt to real estate transactions. However, when we talk about political rights, we do not need signatures to be that strong because people's support of causes are the expression of their political desire, not legal intent. Signature campaigns need only ensure that signatories have the constitutional right to sign the draft bill and signatures only need to allow for public scrutiny to audit the political support given to the bill.

Taking this into account, Mudamos created a way to allow people to sign draft bills using self-issued certificates using their own smartphones. The technology stack used by Mudamos is the same used by certificate authorities to issue certificates, excluding the fact Mudamos is not a recognized authority to issue legally-binding certificates. That is to say, while Mudamos issued certificates cannot be used to authenticate a contract in court, nonetheless the signatures are technically unbreakable and verifiable and well-suited to the purpose of ascertaining citizen wishes but without the cost of doing through one of a handful of monopoly legal certificate providers. In short, Mudamos created a secure and affordable way for people to express themselves politically through digital means.

Risks

Despite all it has to offer, Mudamos's electronic signature is not a national standard and the major risk to the Mudamos project is the contesting of the validity of its signatures by legislative bodies or in courts. Actually, Mudamos is facing a challenge from the legislative house of the Federal District, where Mudamos signatures were not accepted in support of a citizen's initiative draft bill, which called for reducing the House budget. Since an electronic signature standard is not established by law or even by a House of Representatives rule, the decision whether or not to accept Mudamos signatures is discretionary. To mitigate this scenario, ITS drafted a report about citizen initiatives bills arguing that electronic signatures should be accepted based on the current legislation. In addition, the Mudamos team has been talking to congressmen and other leaders, pushing for legislation to standardize electronic signatures. The Mudamos legal framework is another approach to build dialogue bridges between technicians, activists, and legislative houses to support local and national legislative change.

Another risk faced by Mudamos is the adoption rate of the app (350,000 active users) in relation to the number of signatures required to propose a national level draft bill (1.5 million). Despite the fact that Mudamos had at least 4 viral waves since its launch, new user registrations are not growing at a substantial rate. Continuous engagement on Mudamos requires fostering internal variables, such as better user experience and strategic communication for action, and external variables, such as the participatory will of the people which leads to more interest in collaboration and representation in the political process. Mudamos launched its second major version (2.0) in January 2019, seeking user experience improvements, especially features to make campaigns sharing easier.

Mudamos started using public Blockchain as part of its technical architecture, aiming to create a completely transparent and accountable system for verifying signatures. However, after almost 2 years running, the Mudamos team realizes that the availability of this secure infrastructure where anyone can "look under the hood" does not de facto mean anyone is actually doing so. As with the volunteer lawyers, there is a need to develop an independent, crowdsourced technical governance mechanism to ensure that the system maintains its legitimacy.

Finally, the populist, right-wing president, Jair Bolsonaro elected in 2018, has expressed authoritarian tendencies. It is, thus far unknown, how changes in politics will impact political culture in Brazil in the near and longer-term. One can surmise that the trend in government toward more autocratic behavior could end up depressing political mobilization and participation. Or, to the contrary, Mudamos may become more popular than ever if it escapes legal challenge.

Special Requirements

Business and technical requirements of use case

External References and Miscellaneous

For a complete reference of Case Mudamos see: <http://congress.crowd.law/case-mudamos.html>

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)
-

Real Time Tax Compliance

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-004	Use Case Type:	Vertical
Submission Date:	March 28, 2019	Is Use Case supporting SDGs	Yes
Use Case Title:	Real Time Tax Compliance	Domain:	Government and Public Sector: Taxes
Status of Case	Proof of Concept Demo	Sub-Domain	N/A
Contact information of person submitting/managing the use-case	Priyanka Desai, VP of Business Development & Operations Anne T Griffin, Lead Product Manager Kirsten Albers-Fiedler, Law Associate & Legal Engineer E-mail addresses: priyanka.desai@consensys.net , anne.griffin@consensys.net , kirsten.albersfiedler@consensys.net Telephone number: Social media: https://twitter.com/OpenLawOfficial Web site: https://openlaw.io/		
Proposing Organization	OpenLaw (ConsenSys) - United States of America		
Short Description	<i>The premier open source protocol to rapidly build commercial relationships on blockchain technology.</i>		
Long description	The premier open source protocol to rapidly build commercial relationships on blockchain technology. OpenLaw makes it easy to automate agreements, collect secure e-signatures storing them on the blockchain, turn legal agreements into simple forms, tokenize assets, and execute, trigger, and halt smart contracts. Additionally, OpenLaw has free open source legal agreement library, that gives people around the world easier access to justice and the law for resources that can cost thousands of dollars elsewhere. This technology supports individuals, corporations, and governments in building powerful but simple solutions to complex problems. OpenLaw supports, but is not limited to, use cases such as automatic tax collection and alternative dispute resolution that help communities by making sure public services can be paid for and access to justice.		
SDG in Focus (when applicable)	16 Peace, Justice, and Strong Institutions		
Value Transfer:	Automatic transfer of monetary instruments to the government(s) to which they are owed	Number of Users:	Number of employees + Number of companies + Government Tax Agency

Types of Users:	Individual employees, corporations, government tax collection agencies
Stakeholders	Government tax collection agencies, employers
Data:	<p>Data saved to distributed ledger: Employee First Name, Employee Last Name, Employee Ethereum Address, Salary in Wei per Minute, Amount of Income Tax Withheld in Wei per Minute, Medicare Tax Threshold Amount in Wei, Medicare Tax below Threshold Amount in Wei per Minute, Medicare Tax above Threshold Amount in Wei per Minute, Social Security Tax Base Limit in Wei, Social Security Tax in Wei per Minute, Additional Withholding Amount in Wei per Minute, FUTA Tax Cap Amount in Wei, FUTA Tax in Wei per Minute</p> <p>Our system would interact with any HR systems of the employer, the employee's wallet, the government's wallet, and any government systems that track the payment of taxes.</p>
Identification:	Individual paying taxes is identified in the agreement, however, their signature is hashed to keep their information private from those who are not intended to see the agreement.
Predicted Outcomes:	Will decrease the amount of infrastructure needed to support the payment of taxes, reduce costs of maintaining systems to pay taxes, and reduce tax evasion since these calculations are happening directly in a smart contract.

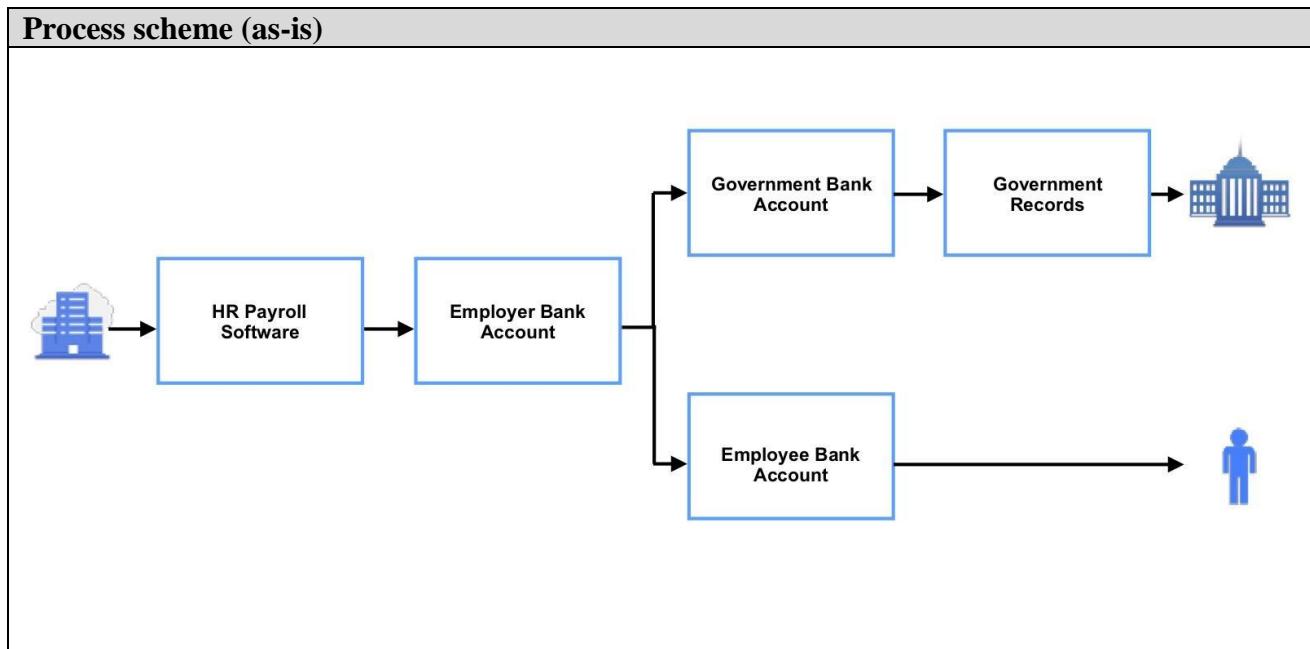
Overview of the Business Problem or Opportunity	
Across the world, there are issues with tax evasion or those who would pay taxes but the lack of infrastructure creates barriers to payment. With OpenLaw's blockchain-based protocol, we're creating a more efficient future, where an employer can pay an employee in ether every minute, eliminating the costs of payroll processors or the need for other centralized intermediaries in the process, while at the same time decreasing the tax gap and the needless waste of resources associated with tax compliance.	
Why Distributed Ledger Technology?	
Using smart contracts on the blockchain allows the process to be more direct and more efficient. It also decreases the number of intermediaries, and the tax gap.	

Section 2: Current process

Current Solutions	
<i>Existing solutions usually involve several systems within HR software within different companies and several systems within a tax collection agency within the government.</i>	

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Employer creates agreements and forms for employee to provide information about self and bank account	Generation of employment agreement.

2.	Employee and employer sign the agreement	Agreement saved to database via agreement software.
3.	Employer enters the information into HR payroll system and sends applicable paperwork to the government	HR payroll system saves employee information.
4.	Company triggers payment process automatically every two weeks	Payroll system looks up employee information.
5.	Automated	Payroll system determines the amount owed to the employee and amount owed in taxes.
6.	Automated	Employer bank account triggers payment to employee bank account.
7.	Automated	Employee bank processes payment.
8.	Automated	Employer bank account triggers payment to government with information.
9.	Automated	Employer bank account processes payment.



Data and information (as-is)		
Data	Type	Description
1.	Employee information	Name, bank account information, income.
2.	Taxes	Types of taxes owed, quantity of taxes owed.

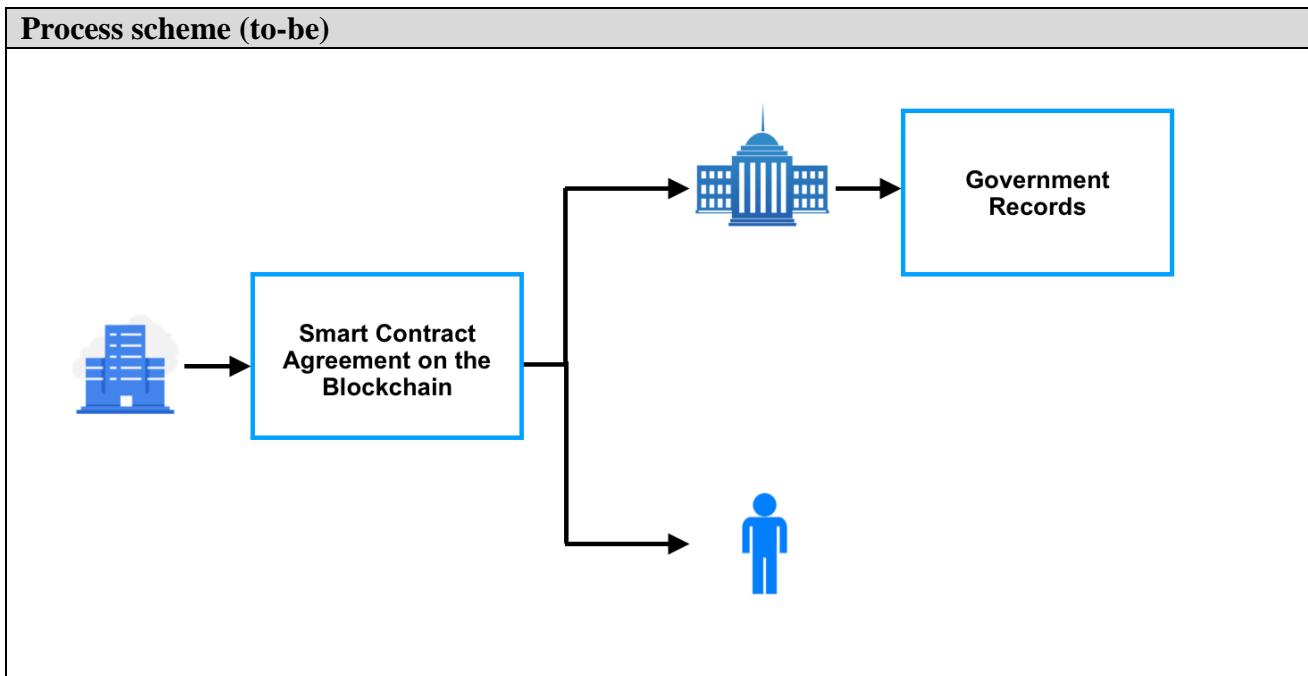
3.	Record of payment to employee, and government tax agency	Records that show the employee was paid and the government tax agency was paid.
4.	Government Tax Agency information	Bank account information for payment.

Participants and their roles (as-is)		
Actor	Type/Role	Description
1.	Employee	Individual employed who needs to have taxes paid to the government.
2.	Employer	Employer who pays the employee and responsible for withholding taxes from the employee's paycheck
3.	Government Tax Collection Agency	Government entity responsible for receiving tax payments and keeping tax records for employees and employers.
4.	Bank	Responsible for sending and receiving payments on behalf of the employee, employer, and government.

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Employer generates employment agreement	Employment agreement is generated as a smart contract
2.	Employee and employer sign agreement	System saves signature and start date to the blockchain
3.	Automated	Payment automatically paid to the employee's wallet for the agreed upon amount and start date via the smart contract
4.	Automated	Payment automatically paid to the government tax collection agency's wallet based on the taxes owed



Participants and their roles		
Actor	Type/Role	Description
1.	Employee	Individual employed who needs to have taxes paid to the government.
2.	Employer	Employer who pays the employee and responsible for withholding taxes from the employee's paycheck
3.	Government Tax Collection Agency	Government entity responsible for receiving tax payments and keeping tax records for employees and employers.

Data and information

Data	Type	Description
1.	Employee information	Name, ethereum address, income.
2.	Taxes	Types of taxes owed, quantity of taxes owed.
3.	Record of payment to employee, and government tax agency	Records that show the employee was paid and the government tax agency was paid.
4.	Government Tax Agency information	Government Ethereum address.

Security and privacy
All information on the Ethereum blockchain is stored as a cryptographic hash on a distributed public ledger.

Main Success Scenario + expected timeline
Ideally, many businesses will begin using this technology with their employees and respective governments. Those businesses and governments will see a cost reduction in the systems needed to maintain the old way of handling payments and taxes, and employees and tax collection agencies can be paid in real time as value is being contributed to the economy, instead of on a schedule that only aligns with intermediary institutions. It should take most businesses less than a year to implement these solutions. For small businesses with less legacy technology, it could take less than six months to implement.

Conditions (pre- or post-)
1. Access to the Internet
2. Access to the Ethereum online wallet.

Performance needs
N/A

Legal considerations
In the United States, there aren't laws explicitly banning cryptocurrency or their use for payment, however not all local governments have explicitly stated they accept them.
Outside of the United States, some countries have banned cryptocurrencies such as Bolivia, or allow cryptocurrency, but do not treat them as a currency. Influence of policy could help governments around the world accept cryptocurrencies so they can use blockchain technology in combination with payments in cryptocurrency or conversion from cryptocurrency to fiat currency. In addition to policy changes, <u>stablecoins</u> can help mitigate concerns around cryptocurrency. They can be tied to fiat currencies, which lowers their volatility, and can tie their value to the fiat currencies of the respective countries that are interested in implementing this solution.
https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

Risks

Current laws do not include withholding amounts for cryptocurrencies, and the conversion rate of ether into USD is subject to volatility, we have converted the salary that an employee receives in ether into USD based off the conversation rate as of May 21, 2018 in order to make the appropriate tax calculations. We then converted the tax and adjusted salary amounts back to ether using the same conversion rate. Depending upon how laws shape themselves around cryptocurrencies in the future, the conversion of ether to USD may require the use of an oracle or, possibly, stable coins.

Also risks regarding security of smart contracts so they aren't hacked and money is sent to the incorrect address.

Special Requirements

Access to the Ethereum

External References and Miscellaneous

State of Ohio Allowing Payment of Taxes in Crypto - <http://ohiocrypto.com/>

Arizona Senate Bill Allowing Crypto Payment - <https://legiscan.com/AZ/bill/SB1091/2018>

Illinois House Bill Allowing Crypto Payment - <https://legiscan.com/IL/bill/HB5335/2017>

Georgia State Senate Bill Allowing Crypto Payment - <https://legiscan.com/GA/bill/SB464/2017>

Other Notes

N/A

Regtech Improving Governance Authenticating Identities, Authorization Signatures and Digital Content

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-005	Use Case Type:	Government and Public Sector
Use Case Title:	OriginalMy Blockchain	Is Use Case supporting SDGs	<i>Yes</i>
		Domain:	<i>List 1 Appendix 1</i>
Status of Case	Running/Production	Sub-Domain	<i>If necessary</i>
Contact information of person submitting/managing the use-case	Full Name: Edilson Osorio Junior Job Title: CEO E-mail address: osoriojr@originalmy.com Telephone number: +372 5709-5771 Social media: https://www.linkedin.com/in/osoriojr/ Web site: https://originalmy.com		
Proposing Organization	OriginalMy Blockchain OÜ Registry Code: 14450907		
Short Description	A LegalTech engine platform that builds Trust in e-Governance seamlessly authenticating: identities, authorisation signatures, and digital content		
Long description	<p>Founded in 2015, OriginalMy envisions a world in which individuals and entities have a balanced alignment of interests and are empowered to take necessary actions that build Trust in the e-Governance for the benefit of the entire organisation.</p> <p>The challenge to achieve that vision is building Trust and increase the overall governance process while providing compliance, risk management and cybersecurity tools that cannot be flawed, corruptible, temperable and non-verifiable - because of centralisation.</p> <p>The solution is presenting a trusted and immutable blockchain framework with:</p> <ul style="list-style-type: none"> - The next generation of Digital Identity & storage of assets; - Seamlessly authentication with proof-of-authorship; - Single Sign-On, with control of delivering of personal data; - Authentic signed documents, contracts and transactions ; - Proof-of-authenticity for digital content; - Blockchain-enabled e-voting systems; <p>This approach is trustful because it improves the overall e-Governance reducing costs and saving time, is flexible to address an array of risk and compliance needs, performs traceability of all digital acts performed and has the security provided by blockchain cryptography protocols.</p>		

SDG in Focus (when applicable)	<p><i>Enter one or more number (1-17) and specific corresponding indicator/s as applicable</i></p> <p><i>See https://www.un.org/sustainabledevelopment/sustainable-development-goals/</i></p> <p>Use your right to elect the leaders in your country and local community</p> <p>Goal 16: Promote just, peaceful and inclusive societies</p> <p>16.3 Promote the rule of law at the national and international levels and ensure equal access to justice for all</p> <p>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</p> <p>16.5 Substantially reduce corruption and bribery in all their forms</p> <p>16.6 Develop effective, accountable and transparent institutions at all levels</p> <p>16.7 Ensure responsive, inclusive, participatory and representative decision-making at all levels</p> <p>16.8 Broaden and strengthen the participation of developing countries in the institutions of global governance</p> <p>16.9 By 2030, provide legal identity for all, including birth registration</p> <p>16.10 Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements</p> <p>16.A Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime</p> <p>16.B Promote and enforce non-discriminatory laws and policies for sustainable development</p> <p>Call out sexist language and behaviour</p> <p>Goal 5: Achieve gender equality and empower all women and girls</p> <p>5.1 End all forms of discrimination against all women and girls everywhere</p> <p>5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation</p> <p>5.B Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women</p> <p>5.C Adopt and strengthen sound policies and enforceable legislation for the promotion of gender equality and the empowerment of all women and girls at all levels</p> <p>Raise your voice against discrimination</p> <p>Goal 10: Reduce inequality within and among countries</p> <p>10.2 By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin,</p>
---------------------------------------	---

	<p>religion or economic or other status</p> <p>10.3 Ensure equal opportunity and reduce inequalities of outcome, including by eliminating discriminatory laws, policies and practices and promoting appropriate legislation, policies and action in this regard</p> <p>10.6 Ensure enhanced representation and voice for developing countries in decision-making in global international economic and financial institutions in order to deliver more effective, credible, accountable and legitimate institutions</p> <p>10.7 Facilitate orderly, safe, regular and responsible migration and mobility of people, including through the implementation of planned and well-managed migration policies</p> <p>Partnership for the goals</p> <p>Goal 17: Revitalize the global partnership for sustainable development</p> <p>17.7 Promote the development, transfer, dissemination and diffusion of environmentally sound technologies to developing countries on favourable terms, including on concessional and preferential terms, as mutually agreed</p> <p>17.8 Fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology</p>		
Value Transfer:	<p>It allows the tokenization of all of your own resources, assets and attributes carrying it on your identity, avoiding the needing of a third party to certify/comprove what belongs the to you. It reduces costs, bureaucracy, time and empower people.</p>	Number of Users:	30.000
Types of Users:	natural person and entities		
Stakeholders	natural person, entities and government		
Data:	<p><i>What data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc.</i></p> <p><i>How DLT solution would interact with external data and other systems.</i></p> <p>Stores the link between the document id and the blockchain id, mantaining history of changes.</p> <p>Stores the hashes of digital documents, the signatures made on documents and authorisations and, in the future, the reputational system.</p> <p>It don't store any personal data on the ledger. Thus, OriginalMy will use tokens to reward users who made tasks, like working on the decentralised network of validation being constructed.</p>		
Identification:	Identity validation automatically or using own bureau. After the validation, the personal data is stored just with the user. There's no possibility of anonymous use.		

Predicted Outcomes:	
----------------------------	--

Overview of the Business Problem or Opportunity

Explanation of the business problem or opportunity.

The problem is the lack of trust on digital content and on who is performing the digital act or transaction, in situations where the authenticity, authorship or ownership is critical.
It opens a window for corruption, bureaucracy and expending of money and time.

Fines and compliancy divergences costs:

- **\$300 billion post 2008 crisis regulatory fines**
FT Research
- **492% volume of regulatory change between 2008 and 2015**
Thomson Reuters
- **45x increase of regulatory fines in 20 large US and EU banks**
McKinsey
- **10-15% of total workforce dedicated to governance, risk and compliance**
McKinsey
- **Proxy voting remains "noisy, imprecise and disturbingly opaque"**
Barons - about \$60m P&G proxy fight costs

The opportunity:

- **\$780 billion** per year regulatory divergence costs Thomson Reuters: Cost of Compliance 2018 Report
- **ROI of 600%** in regulatory software investment
LPT Research: Strategic Analysis of RegTech - A \$100b Opportunity
- **\$118.7 billion** per year revenue stream by 2020
LPT Research: Strategic Analysis of RegTech - A \$100b Opportunity

On the Identity field, a McKinsey report identified that until 2030, countries will spend up to 13% of the GDP on Digital Identity and related services, to avoid identity and payroll fraud and improving the onboarding systems.

Why Distributed Ledger Technology?

How distributed ledger technology would improve the current solutions (if they exist) or enable new solutions which were previously unavailable.

Please also specify which DLT features are required (immutability, security, verifiability, resilience, transparency, etc.)

The full solution is only possible because of blockchain technologies.

- Allows the full decentralisation of the identity and being the future generation of digital identity (where the identity will store itself all of your resources, assets and attributes).
- Allows the transaction of personal data being tracked and rewarded.
- Allows the proof-of-authenticity of digital content and transactions
- Allows proof-of-authorship for authorisation signatures on documents, and contracts
- Single sign-on systems with delivering (transacting) of personal data with proof-of-agreement
- Improves trust on e-voting, where the main problem is the lack of trust just after casting the vote to the blinded ballot box and in the centralised tallying phase (see Hääl - the

worldwide first protocol for Secret E-Voting on Public Blockchains, with running PoC:
<https://github.com/eddieoz/haal>)

- Allows decentralised reputation system and dispute resolution
- Security provided by many layers of strong cryptography
- Immutability and integrity of all data stored, as resilience and redundancy for contingence.
- Transparency and auditability of all data and transactions
- High availability of all network

Section 2: Current process

Current Solutions

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

- OriginalMy: providing end-to-end digital governance

And other systems who addresses part of the solutions:

UPort: digital identity

Civic: digital Identity

Signatura: signing contracts and documents

BlockNotary: notarisation of documents

Existing Flow (as-is): Signing documents and contracts

Step	User Actions	System Actions
1.	Local authentication	User goes to a notary
2.	Sign a contract	User register the contract on a notary

Existing Flow (as-is): Signing public petitions

Step	User Actions	System Actions
1.	Signature collecting	User signs a paper
2.	Validation	Impossible to validate
3.	Acceptability	Representative endorses the petition

Existing Flow (as-is): Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)

Step	User Actions	System Actions
-------------	---------------------	-----------------------

1.	Collecting the legal proof	User goes to a Notary Notary transcribe the page on a report The report can be attached to a case and sent to the justice
----	----------------------------	---

Existing Flow (as-is): Platform: Notarization of documents		
Step	User Actions	System Actions
1.	Authenticating documents	User goes to a Notary Notary makes a copy of the document Notary authenticates the copy of the document

Existing Flow (as-is): E-voting		
Step	User Actions	System Actions
1.	Voter casts the ballot	Send to a centralised platform Needs to Trust on the platform; Too much power on a centralised entity No transparency and verification in real-time Black-boxes of voting

Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	In paper
2	<i>Web content</i>	Must go to a Notary
3	<i>Certificate of Signatures</i>	Must go to a Notary to verify the signatures
4	<i>Certificate of Authenticity</i>	Provided by a notary, in paper
5	<i>Notary Authentication</i>	Digitally stamped document issued by a notary
6	<i>Notary declaration</i>	Report issued by the notary, with the description of the service provided
8	<i>Collecting Signatures on Public petitions</i>	On paper

9	<i>Voting ballot</i>	On-paper or electronic by centralised trusted entity
----------	----------------------	--

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Lawyers</i>	Collect evidence to attach to the process
2	<i>Bank</i>	Pre-authenticate documents to send to the notary
3	<i>Government</i>	Preserves the authenticity of your papers and documents
5	<i>Users</i>	Has the needs of authenticating documents, verifying themselves or their signatures
6	<i>Notary</i>	Provides the service for authenticating documents and signatures

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Existing Flow (to-be): Mobile app: Signing documents and contracts		
Step	User Actions	System Actions
1.	Local authentication	User uses local biometrics to validate him/herself
2.	Sign a contract	User proves the ownership of the document to be signed (using pin-code) System verifies on-chain if the user is allowed to sign and if the document is authentic System stores the digital signature and the blockchain id on the smart-contract, together to the other signatures of that document

Existing Flow (to-be): Mobile app: Authentication system with delivering of personal data		
Step	User Actions	System Actions
1.	Local Authentication	User uses local biometrics to validate him/herself
2.	Scans a QR-code	Opens a popup showing all the data that will be collected by the platform
3.	User agree on delivering of the data	Authenticates user using cryptography challenges Sign the data to be transferred Transfer the data to the desired platform Registers the transaction The desired platform checks the authenticity of the data, as the reputation.

Existing Flow (to-be): Mobile app: Mudamos+ (created by ITS-Rio) internally using our engine for identity, signatures and authentication, for signing public petitions (+600k downloads, 2 laws approved)		
Step	User Actions	System Actions
1.	User selects the public petition	verifies the authenticity of public petition on-chain
2.	User decides signing	System uses the stored and previously validated Blockchain ID for signing the petition App does proof-of-work, generating a block to be accepted by the network (avoiding hacking, spam and brute-force on the network) Sends the block to network.

		If the block is valid, the network stores the block on a sidechain In the selected times, the system scan the sidechain, revalidates all user signatures, and generates and publish a new version of the PDF report with all signatures collected for all open public petitions System authenticates each generated new version of the report on blockchain
3.	User submits the signatures report to verify the authenticity	System verifies the authenticity of the report on-chain System validates each signature in the report: user validity and integrity of the user signature

Existing Flow (to-be): Chrome Plugin: Proof-of-authenticity of web content + notarization (avoiding fake news dissemination, harassment and other on social media)		
Step	User Actions	System Actions
1.	Click on Chrome Plugin	Scans the page Generates a report which contains the permalink, timestamp and the copy of the page Authenticates the report in blockchain Send the report to the notary Notary verifies the authenticity in on-chain Notary extracts the permalink, access the page, copies the page, authenticates the copy of the page and delivers back to the user

Existing Flow (to-be): Platform: Notarization of documents		
Step	User Actions	System Actions
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount

3.	User makes the payment	System authenticates the hash of the document in on or more blockchains
----	------------------------	---

Existing Flow (to-be): Platform: Registration of documents to be signed		
Step	User Actions	System Actions
1.	User submits a document	Extracts the hash Verify on-chain the authenticity of the document If document is already authenticated, returns the full information If the document is not authenticated yet, goes to the checkout
2.	User goes to the payment page	System detects if the user is staking the token ABC - Anti Bureaucracy Coin If yes, system recalculates the discount
3.	User makes the payment	System authenticates the hash of the document in on or more blockchains System opens a session on a smart-contract to start collecting the signatures System notifies all signatories Signatories make the signature System stores the signature together on the smart-contract After collecting all signatures, system generates a report and send to each signer.

Existing Flow (to-be): Platform and app: Public e-voting		
Step	User Actions	System Actions
1.	Voter submits the filled voting ballot for signing	Extracts the hash Register the ballot for signature by the selected BlockchainID on the smart-contract and wait for the signature
2.	Voter sign the ballot with BlockchainID	System stores the user signature on the smart-contract After confirmation, system provides a certificate of signature to the user
3.	User submit the ballot and the certificate to the voting	off-chain process

	administration for tallying purposes	
--	--------------------------------------	--

Expected Flow (to-be): Secret voting on public blockchain PoC and paper: https://github.com/eddieoz/haar		
Step	User Actions	System Actions
1.	User authenticates to voting session	Validate the user identity Open the voting session Unlink user identity Generates the stealth addresses for voting and register it on chain to be discovered
2.	User cast the vote through stealth wallet	System creates the zero-knowledge proof-of-vote Encrypts the ballot with homomorphic encryption Casts the encrypted ballot and store in blockchain Validates the zkProof-of-Vote on chain User verify own vote Closes the voting session
3	Voting administrator closes the election session	Smart-contract automatically the result Smart-contract publishes the result
4	Auditor retrieve all results to check	Decrypts all votes Calculates the final result Generates the proof-of-result Publish the proof-of-result on chain

Expected Flow (to-be): Decentralized network of validation		
Step	User Actions	System Actions
1.	User A collect the web-content proof and send to the platform	Opens a collecting proofs session System authenticates the proof on blockchain System asks for how many people must access and collect proofs System calculates how much ABCs must be deposited to reward the network for collecting proofs
2.	User A deposits the amount	System randomly notifies the network to collect proofs
3.	Users from network receive the notification and agrees on collecting proof from their device	System generates automatically the proof System asks for user to sign the proof with the Blockchain ID to prove it is a real person
4.	User from network agrees on signing	System sign the proof using the Blockchain ID System authenticates the generated proof on blockchain Stores the proof to the proofs repository
5.	User A collects the proofs collection	After aproval, rewards user from network Delivers all signed proofs to the User A Closes the collecting proofs session

Process scheme (to-be)		

Participants and their roles		
Actor	Type/Role	Description
1	<i>Government/Institution</i>	Voting system administrator: Setup the voting infrastructure, open and closes the voting session
2	<i>Natural person</i>	Vote, request webcontent proofs participate on the decentralized network for collecting webcontent proofs.
3	<i>Lawyer</i>	Request webcontent proofs from decentralized network
4	<i>OriginalMy</i>	It is the first validator of user identity
5	<i>Auditor</i>	Audit the voting process in real time, compute the result and the proof-of-result to check if it matches with the automatically calculated by the smart-contract, count users, count open voting sessions, verify if user validation is correct
6	<i>Notary</i>	Executes a digital process of authenticating documents and signatures

Data and information		
Data	Type	Description
1	<i>Web Content</i>	Content collected on Web Browser
2	<i>Proof-of-Authenticity of Web Content</i>	PDF report that contains the permalink, timestamp and the copy of the web content.
3	<i>Ballot</i>	Ballot that contains all the races and candidates
4	<i>Encrypted Vote</i>	The ballot with each vote encrypted
5	<i>Proof-of-Vote</i>	Zero Knowledge proof-of-vote issued optionally after voting, used as vote receipt
6	<i>Proof-of-Result</i>	Zero-knowledge proof-of-result, proves the voting administrator decrypted all votes and calculated the result for auditing purposes
7	<i>Digital Document</i>	Any kind of digital media, to be authenticated
8	<i>Digital Signature</i>	Signature made using the private-keys owned by the user

9	<i>Digital Identity</i>	Digital certificate where the private-keys are located. It must be stored just with the user
----------	-------------------------	--

Security and privacy

1. User validates the identity for using the BlockchainID
2. User casts the vote, unlinked to identity
3. No participant can see the content of the vote of another user
4. No possibility of double-voting
5. User can keep the (zk)proof-of-vote, to prove the vote without exposing the vote
6. Vote buying and vote coercion avoided if the voting session is open for many days and user have the possibility of changing vote anytime (Estonia example)
7. OriginalMy dont store user personal data, content or documents, for privacy purposes
8. User delivers own personal data, signing the data delivered. Destination platform has proof-of-agreement for all received data.
9. Decentralized identity and decentralized storage of personal data. No single point of failure

Main Success Scenario + expected time line

Actual Key Achievements

The main key achievements are:

- having blockchain proofs accepted in the Court of Appeals (Superior Court),
- new laws created that started on our engines (through Mudamos+),
- marriages and child born registrations,
- used by presidential candidates to fight against fake-news dissemination,
- shareholders e-voting on Brazilian Fintechs Association,
- mentioned in books and academic papers,
- Brazilians no longer need to go to the notary to authenticate documents, because of the first notary integration,
- featured on a US documentary of Reason.tv: "3 Ways Bitcoin is Promoting Freedom in Latin America"
- featured on a documentary of Globo, the second largest commercial TV: "Estonia has a pioneering project to end bureaucracy and facilitate citizens' lives"

Awarded:

- Google.org Social Impact Challenge in 2016 (through Mudamos+ by ITS-Rio - app for signing public petitions powered by our engine for identity, signatures and authentication),
- Financial Personality of the Year in 2017
- Most Innovative Startup in 2018

Future Success Scenario

An anonymous electronic voting system on public blockchains with the transparency and auditability provided by a public blockchain like Ethereum to bring another level of trust and security because everything can be auditable during the voting process. The smart-contract starts the tally phase and verify it using distributed computing if needed. The voting privacy is granted by stealth wallets, homomorphic encryption, at the same time that zero-knowledge proofs grant the proof-of-vote and the proof-of-result.

We expected until the end of 2019 having a open capital company doing the shareholders proxy-voting through our platform

Conditions (pre- or post-)

For using Blockchain ID:

1. Download OriginalMy app
2. Validation of the identity of the user through automated or manual process

For authenticating documents

1. Create an account on the website

For authenticating web-proofs

1. Installing the Chrome Browser extension

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

- Improving the confirmation time for contract and signatures
- Improving the fee & gas of blockchain/smart-contracts
- Scale the identity validation
- Implement another public blockchains (Waves, Litecoin and others)
- Interoperability with x509 certificates
- reducing fee for using ABC token

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. Compliance with MP 2200-2/2001
2. Compliance with Civil Law Arts. 104-107, 219 and 220
3. Legal opinion for digital authentication with notaries

No law barriers with negative impact, but laws expressly approving the format of authentication could be helpful, like the case of Wyoming

<https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#2943280e5fde>

Risks

Legal, business and technical risks related to use case

Risks of lobby by notaries, banks and congressmen

Lack of regulations in Brazil creating an insecure environment for crypto-startups

Tech risks:

- 0-day in Bitcoin, Ethereum or EDSA curves,
- 51% attack,
- expensive fee costs because of cryptocurrency prices

Special Requirements

No special requirements

External References and Miscellaneous

List of references for standards or well-defined mechanisms if any of requirements calls for the implementation of a standard or protocol or other well-defined mechanism. If the use case needs non-standard consensus mechanisms or cryptographic tools, such information should be included here. Also such section may be used to provide more information regarding the use case including links to any kind of related materials, terms and descriptions or any other related information.

Albrecht, Martin, et al. *Homomorphic Encryption Standard*. 21 Nov. 2018, <http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf>.

A Next-Generation Smart Contract and Decentralized Application Platform. <https://github.com/ethereum/wiki/wiki/White-Paper>. Accessed 13 Jan. 2019.

Aztec Protocol Specification. <https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf>. Accessed 13 Jan. 2019.

Baudron, Olivier, et al. "Practical Multi-Candidate Election System." *Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing - PODC '01*, 2001, doi: 10.1145/383962.384044.

Bitcoin-Development / Stealth Addresses. <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html>. Accessed 14 Jan. 2019.

Blum, Manuel, et al. "Noninteractive Zero-Knowledge." *SIAM Journal on Computing*, vol. 20, no. 6, 1991, pp. 1084–118.

Camenisch, Jan, et al. "Efficient Protocols for Set Membership and Range Proofs." *Lecture Notes in Computer Science*, 2008, pp. 234–52.

Dahlin, Taylor Fox, and daylighting society. "Paillier Zero-Knowledge Proof."

<Https://paillier.daylightingsociety.org>, 17 Dec. 2016,

https://paillier.daylightingsociety.org/Paillier_Zero_Knowledge_Proof.pdf. Damgård, Ivan. *On Σ-Protocols*.

<http://www-cs.ccny.cuny.edu/~fazio/F15-csc85030/readings/Dam10.pdf>. Accessed 13 Jan. 2019. *Decentralised Applications*.

[https://github.com/ethereum/wiki/wiki/Decentralized-apps-\(dapps\).Developer%20Guide%20-%20Bitcoin%20%2F%20Blockchain](https://github.com/ethereum/wiki/wiki/Decentralized-apps-(dapps).Developer%20Guide%20-%20Bitcoin%20%2F%20Blockchain).

<https://bitcoin.org/en/developer-guide#block-chain>. Accessed 14 Jan. 2019.

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman. *Security Analysis of the Estonian Internet Voting System*. <https://jhalderm.com/pub/papers/ivoting-ccs14.pdf>. Accessed 13 Jan. 2019. Goldwasser, S., et al. "The Knowledge Complexity of Interactive Proof-Systems." *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85*, 1985, doi:10.1145/22145.22178.

Goldwasser, Shafi, et al. *The Knowledge Complexity of Interactive Proof Systems*. Feb. 1989, http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.

Heiberg, Sven, et al. "Improving the Verifiability of the Estonian Internet Voting Scheme."

Lecture Notes in Computer Science, 2017, pp. 92–107. *Introduction – Homomorphic Encryption Standardization*.

<http://homomorphicencryption.org/introduction/>. Accessed 14 Jan. 2019.

Lai, Wei-Jr, et al. "DATE: A Decentralized, Anonymous, and Transparent E-Voting System." *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018, doi:10.1109/hoticn.2018.8605994.

Racanelli, Vito J. "Proxy Voting Is Broken and Needs to Change." *Barrons Online*, Barrons, 7 July 2018, <https://www.barrons.com/articles/proxy-voting-is-broken-and-needs-to-change-1530924318>.

Rivest, Ronald L. *The ThreeBallot Voting System*. 1 Oct. 2006, <https://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf>.

Tsang, Patrick P., and Victor K. Wei. "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation." *Lecture Notes in Computer Science*, 2005, pp. 48–60.

What Are Zk-SNARKs? <https://z.cash/technology/zksnarks/>. Accessed 14 Jan. 2019. Wu, Wei-Jr Lai Ja-Ling. *An Efficient and Effective Decentralized Anonymous Voting System*. 18 Apr. 2018, <http://arxiv.org/abs/1804.06674>.

Yu, Bin, et al. "Platform-Independent Secure Blockchain-Based Voting System." *Lecture Notes in Computer Science*, 2018, pp. 369–86. *Zcash Protocol Specification*.

<https://github.com/zcash/zips/blob/master/protocol/protocol.pdf>. Accessed 13 Jan. 2019.

Other Notes

Any assumptions, issues

Diploma Verification

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-006	Use Case Type	<i>Vertical</i>
Use Case Title:	Diploma Verification	Is this Use Case supporting SDGs	<i>Yes</i>
		Domain:	<i>Government and public sector</i>
Status of Case	<i>Pilot</i>	Sub-Domain	<i>Education</i>
Contact information of person submitting/managing the use case	<p><i>Full Name</i> Pierre-Yves Burgi <i>Job Title</i> Directeur SI adjoint <i>E-mail address:</i> Pierre-Yves.Burgi@unige.ch <i>Telephone number:</i> +41 22 379 75 09 <i>Website:</i> https://www.unige.ch/stic/acteurs/organigramme/direction/burgi/</p>		
Proposing Organization	<i>University of Geneva, Switzerland</i>		
Short Description	<i>Pilot for verification of diplomas by Ethereum smart contract and legally recognized electronic seal. Possibility of revocation of diplomas.</i>		
Long description	<p>The falsification of university certificates is a major problem. Since diplomas are often only presented as scans, forging them has become very easy. As a result, the University of Geneva is being confronted with an increasing number of verification requests.</p> <p>A pilot application has been developed that uses a legally regulated seal and a timestamp on a public blockchain (Ethereum) to prove the authenticity of a diploma. The document is verified by using the original PDF/A-file or a short summary of the diploma. The use of a public blockchain ensures that the diploma can be proven even in the case of the university not being able to confirm its validity anymore</p>		
SDG in Focus (when applicable)	<i>SDGs in Focus are SDG 4 – education and SDG 8 – decent work.</i>		
Value Transfer	<i>No transfer of value</i>	Number of Users:	<i>40 (currently in the pilot), several thousand planned in the future</i>
Types of users	<i>Students and everybody to whom they present their diplomas</i>		
Stakeholders	<i>Students, universities, employers</i>		
Data:	<p>For diplomas, only hashes are stored with no metadata added. This will only allow the verification of the originality of a document that is presented to the users.</p> <p>Only in the case of revocation is the information about the revocation added. However, even then, this information can only be linked to a student when somebody is in the possession of a copy of the diploma and therefore has a legitimate reason to verify its validity.</p>		

	External recruitment systems may access the smart contract directly to verify that the documents they receive are original and have not been revoked.
Identification	Education certificates are bound to an identity and cannot be transferred. There are no anonymous certificates. The system however, needs proof that the user is already in the possession of a copy of the certificate in order to allow the verification of the certificate. Without a copy of a diploma, no personal information can be derived from the blockchain. With a copy of a diploma, only the information about the originality and the revocation status can be derived from the blockchain.
Predicted Outcomes	Less forged diplomas, less unqualified people in jobs, more trust in education, less work in verifying university certificates.

Overview of the Business Problem or Opportunity	
When the recruitment process becomes digital, the proof of the authenticity of university degrees is lost. Scanned PDFs are easy to forge. The number of verification requests is rising.	
Why Distributed Ledger Technology?	
The solution combines a server at the University of Geneva, a regulated digital seal according to the Swiss law ZertES and a smart contract on the Ethereum blockchain. This combination was chosen for the pilot project to reach a maximum durability and to evaluate the advantages and disadvantages of the different solutions. The ultimate goal is to replace paper certificates.	

The advantages of DLT in this context are:

- Certificates can be revoked
- Certificates can be verified even when the university server is down
- The blockchain-based proof does not need any maintenance by the university

Section 2: Current process

Current Solution	
Until now, diplomas have only been issued on paper	

Existing Flow		
Step	User Actions	System Actions
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Distribute paper diploma to students	No automation

Participants and their roles		
Actor	Type/Role	Description
1	<i>Students</i>	Students currently scan their diplomas and use the scan in the recruitment process

Participants and their roles		
Actor	Type/Role	Description
2	<i>Employers</i>	Employers either trust the scans or manually send a verification request to the University of Geneva

Section 2: Pilot process

Pilot Solution
The pilot does not disrupt the diploma generation but is an add-on to the current process

Flow (pilot)		
Step	User Actions	System Actions
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Scan diploma	Add third page with description and generate PDF/A
4.	Confirm electronic seal	Add electronic seal
5.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
6.	Send PDF/A by email and distribute physical diploma to students	Partly automated
7.	Employers receive a digital or printed copy of the diploma	
8a.	Verification of the PDF/A by employer	An employer can <ul style="list-style-type: none">• verify the digital seal on the PDF/A• verify the PDF/A through the university website• calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
8b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
8c.	Verification of the information on the diploma	An employer can verify the information on the diploma <ul style="list-style-type: none">• through the university website• by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Section 3: Final process

Expected Flow (Production)		
Step	User Actions	System Actions
1.	Confirm diploma to be generated	Generate PDF/A
2.	Confirm application of digital seal	Apply digital seal
3.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
4.		Send signed PDF/A to students
5.	Optionally print diploma, apply physical seal and distribute it to students	Manual process
6.	Employers receive a digital or printed copy of the diploma	
7a.	Verification of the PDF/A by employer	An employer can <ul style="list-style-type: none">• verify the digital seal on the PDF/A• verify the PDF/A through the university website• calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
7b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
7c.	Verification with the information on the diploma	An employer can verify the information on the diploma <ul style="list-style-type: none">• through the website of the university• by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Participants and their roles		
Actor	Type/Role	Description
1	<i>University</i>	Creates the certification if student has complied with all prerequisites and sends it to the student
2	<i>Student</i>	Determines who shall be able to see and verify the diploma

Participants and their roles		
Actor	Type/Role	Description
3	<i>Employer, etc.</i>	Employer is able to verify the diploma even in the unlikely event that the university is not reachable anymore

Data and information		
Data	Type	Description
1	<i>Documents</i>	Diploma with digital seal
2	<i>Hashes</i>	Hashes of the PDF/A and of a short form of the relevant information will be written to a blockchain through a smart contract
3	<i>Revocation</i>	A revocation entry can be added through the smart contract

Security and privacy
<i>1. Great care has been taken to provide a very high level of security and privacy.</i>
<i>There is a key management system for the keys that allows diploma hashes to be put or revoked to the Ethereum blockchain.</i>
<i>Without already having access to a diploma, no information can be derived from the blockchain. With the diploma, no additional information is available except in case of revocation of the diploma</i>

Main Success Scenario + expected timeline
<i>The pilot system works even for only one university using the system. However, universities should join forces, develop a common system or even interface with a system for self-sovereign IDs</i>
Conditions (pre- or post-)

Performance needs
<i>With only a couple of thousands of diplomas being issued per year, the performance of Ethereum is sufficient</i>

Legal considerations
<i>An in-depth evaluation of GDPR was part of the project</i>

Risks
<i>Application of GDPR on DLT still involves some legal uncertainty.</i>

There might be an evolving standard for university diplomas. Current diplomas might have to be migrated in the future

Special Requirements

Transaction fees need to stay manageable

External References and Miscellaneous

An in-depth description of the project can be found here:

<https://erbguth.ch/slides/DiplomaPaper.pdf>

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

錯誤! 所指定的樣式的文字不存在文件中。

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

Supply Chain Finance in Pharmaceutical Industry with DLT

Section 1 Summary

Use Case Summary			
Use Case ID:	HLC-001	Use Case Type:	Vertical
Submission Date:	October 30, 2018	Is Use Case supporting SDGs	Yes
Use Case Title:	Supply Chain Finance in Pharmaceutical Industry with DLT	Domain:	Industries
Status of Case	Pilot	Sub-Domain	Pharmacy
Contact information of person submitting/managing the use-case	Full Name: Michael Dong E-mail address: dongning@chainnova.com Telephone number:+86 13511068330 Social media: WeChat Account: immdong Web site: www.chainnova.com	Job Title: CEO	
Proposing Organization	ChainNova Data Technology (Nantong) Co. LTD, PRC.		
Short Description	This use case is a proposal to trace the logistics of medicines and provide lower-cost financial support for the trader on pharmaceutical industry chain.		
Long description	This use case is a proposal to trace the logistics of medicines and provide lower-cost financial support for the trader on pharmaceutical industry chain. In traditional pharmaceutical supply chain, we see the issues like fake medicines, fragmented medical logistics, untransparency of trading processes and restriction of credit grantees for SMEs. In this use case, ChainNova built a pharmaceutical supply chain financial platform based on DLT technology which can make the whole trading process traceable and increase trust among the participants on the supply chain.		
SDG in Focus (when applicable)	3: Good Health and Well-Being		
Value Transfer:	No	Number of Users:	
Types of Users:	Pharmaceutical companies, medicine distribution companies, banks, hospitals		
Stakeholders	Government, Pharmaceutical companies, medicine distribution companies, banks, hospitals doctors, patients		
Data:	The medicine data, logistics data, sales date		

Identification:	Full identification of all the participants
Predicted Outcomes:	<p>The predicted outcomes are:</p> <ul style="list-style-type: none">- Increase the transparency of the trading processes- Integrate the pharmaceutical industry deeper with finance- Increase the transaction efficiency on the supply chain- Strengthen the credit of medicine distribution companies and lower the cost of financial due diligence for banks- Facilitate the development of medicine distribution companies with greater support from financial institutions- Prevent fake medicine circulation

Overview of the Business Problem or Opportunity
<ul style="list-style-type: none">➤ In traditional supply chain finance area, there are restrictions of credit grantees for medicine distribution companies- Since the national credit information systems is not complete, there is information asymmetry for medicine distribution companies in the supply chain and banks can't directly grant credits to them. The bank credit is based on the credit of core companies.➤ Limitations of information integration on the supply chain- The core enterprises own IT system is difficult to integrate the upstream and downstream companies' transaction information on the supply chain, the authenticity of the transaction information is hard to verify and tell if the transaction information has been tampered.➤ The transaction information is untransparent in the trading process- Supply chain finance integrates business flow, logistics and cash flow. If the online business flow and offline logistics cannot achieve information transparency and full visibility, the bank's right to control the collateral may create risk and directly affect the business development.

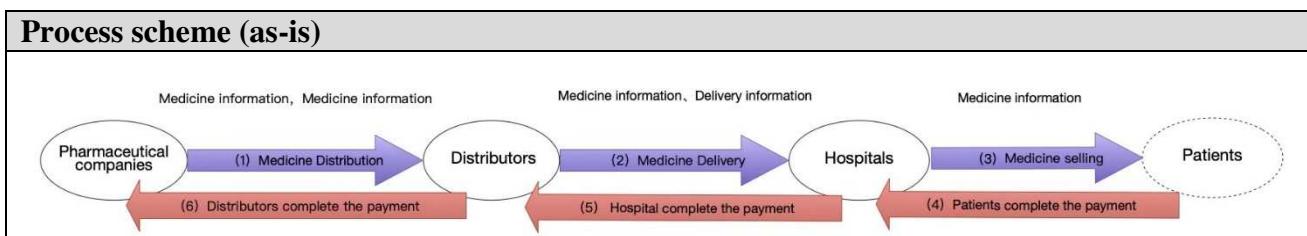
Why Distributed Ledger Technology?
The DLT technology can ensure all the information on the supply chain transparent and reliable as they can't be tampered. This will help the financial institutions to access and grant credit to the medicine distribution companies which can lower the cost for their credit investigation and stimulate the development of medicine distribution companies in return. In addition, the smart contract of DLT can automate the trading process with efficiency greatly improved.

Section 2 Current process

Current Solutions
On ChainNova's supply chain finance platform, the credit based on the digital certificates become authentic and transferrable to help medicine distribution companies get more financing support from

banks. The digital certificates will be supervised and granted by the core enterprises on the supply chain and all the information of the certificates is transparent to every participant.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Pharmaceutical companies provide medicines for distributors on credit	Pharmaceutical companies will supervise the delivery and account receivable of the medicines
2.	Distributors re-sell the medicine to hospitals with large amounts of accounts receivable	Distributors manage the medicines from different factories by batch with details recorded for further analysis.
3.	Hospitals sell the medicine to patients	Hospitals record the source, logistics and inventory of the medicine as the reference for future procurement plan
4.	Patients trace the source of medicines	Patients trace the logistics of the medicines
5.	Hospitals pay the due account , distributors collect the payment and pay the pharmaceutical companies	Hospital update the inventory and account information Distributors update the inventory and account information Pharmaceutical companies update the inventory and account information



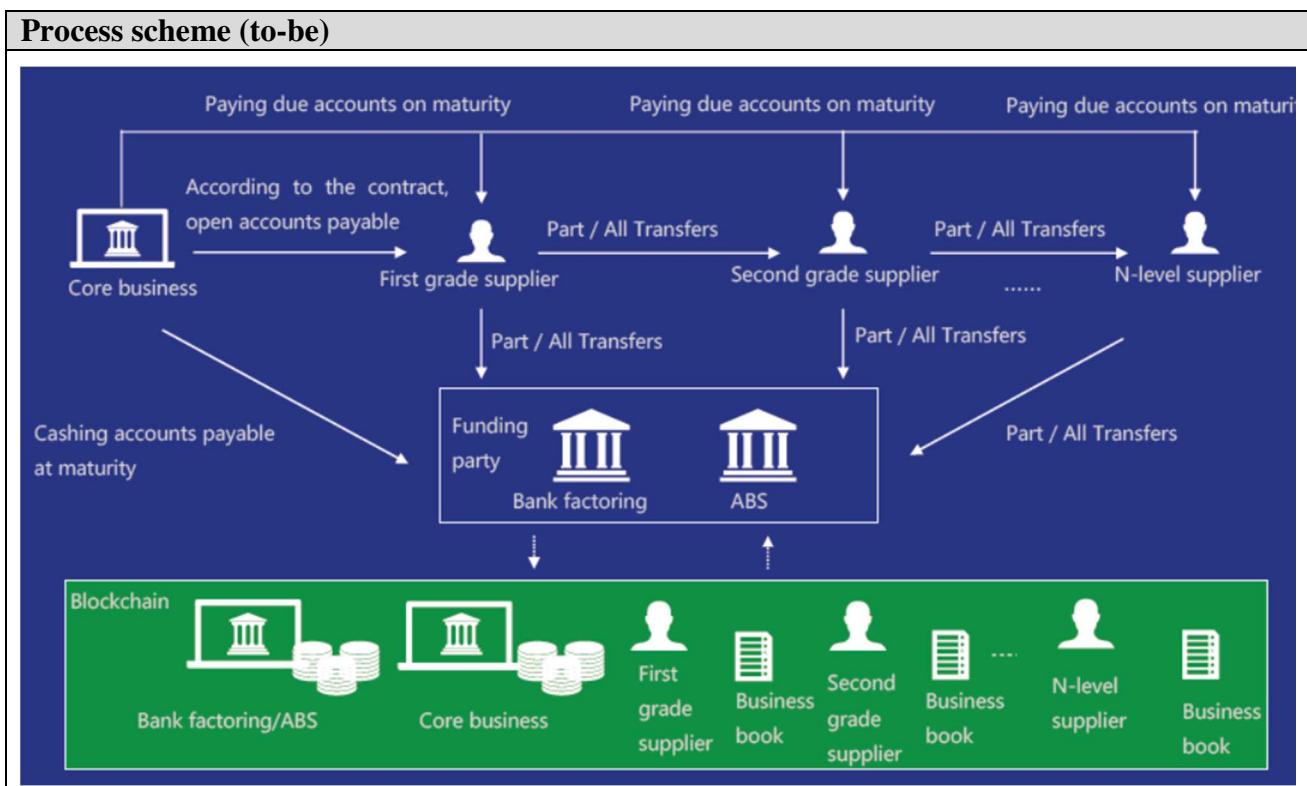
Data and information (as-is)		
Data	Type	Description
1	Medicine Logistics	All the information during the trading process
2	Sales data	The sales data includes the amount, inventory, sales volume etc.

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Pharmaceutical companies	The medicine production factories
2	Medicine distribution companies	The medicine distributors, this may include the first-layer distributor, second-layer distributor etc.
	Banks	Provide loan to the traders especially the distributors
	Hospitals	Provide the medicine for the patients

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	The pharmaceutical companies sell the medicine to distributors with account receivable generated	The distributors' system generates the electronic certificate for account payable for pharmaceutical companies
2.	Pharmaceutical companies digitalize the accounts receivable and make it transferrable	The electronic certificates will be transferred,split,held and financed.
3.	The pharmaceutical companies pledge accounts receivable to banks to obtain credit lines and financing	The electronic certificates for accounts receivable will be circulated online as an asset



Participants and their roles		
Actor	Type/Role	Description
1	Pharmaceutical companies	The medicine production factories
2	Medicine distribution companies	The medicine distributors, this may include the first-layer distributor, second-layer distributor etc.

Participants and their roles		
Actor	Type/Role	Description
	Banks	Provide loan to the traders especially the distributors
	Hospitals	Provide the medicine for the patients

Data and information		
Data	Type	Description
1	Medicine logistics	The medicine logistics information from end to end will be accurately recorded and can not be tampered
3	Sales data	The sales data includes accounts receivable and payable, inventory, electronic certificates etc will be recorded onto blockchain with full transparency

Security and privacy
1. Since transparency is the main requirement, the ideal information visibility is public; 2. If business privacy prevent public visibility, this critical subset of data can be encrypted or protected; 3. DLT system should be able to provide mechanisms of DLT data integrity control;

Main Success Scenario + expected time line
1. The distributors and pharmaceutical companies can get loan from banks in easier way 2. Banks will lower the cost for investigation before providing loan 3. The hospitals and patients will have more trust on the medicine

Conditions (pre- or post-)
1. All parties are connected to DLT network

Performance needs
N/A

Legal considerations
N/A

Risks
1. Risks related to DLT immaturity.

Special Requirements

N/A

External References and Miscellaneous

N/A

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)
 - b.

Blockchain Web/Mobile Application for Vaccine Supply Chain

Section 1: Summary

Use Case Summary					
Use Case ID:	HLC-002	Use Case Type:	<i>Vertical</i>		
Submission Date:	January 9, 2019	Is Use Case supporting SDGs	<i>yes</i>		
Use Case Title:	Blockchain Web/Mobile application for vaccine supply chain	Domain:	<i>Healthcare</i>		
Status of Case	<i>Pilot Implementation</i>	Sub-Domain	<i>Pharma</i>		
Contact information of person submitting/managing the use-case	Dr. Agnes Naliaka Mindila amindila@icsit.jkuat.ac.ke				
Proposing Organization	<i>Jomo Kenyatta University of Agriculture and Technology (JKUAT), KENYA</i>				
Short Description	The application seeks to achieve visibility, transparency and traceability of the vaccines along the supply chain and ensures that each vaccine can be isolated, analyzed and all activities associated with it identified.				
Long description	<p>Developing countries face challenges in the vaccine supply chain. The Challenges threaten vaccine access, availability, and quality. As countries adopt newer and more expensive vaccines and attempt to reach people at different ages and in new settings, the supply chain must be optimized. Information about demand, stock-levels and timely use of vaccines is poorly kept affecting timely supply leading to expirees and/or lack of needed vaccines. There is also the risk of poor product quality and counterfeiting that countries face and avoidable wastage. Accurate data collection, secure data storage and a flow of trusted information between parties is required.</p> <p>Development of Permissioned Blockchain-based web/mobile application will enable incorporation of Identity Management technologies, achieve end to end visibility with the incorporation of BLE iBeacon technologies, GS 1 data matrix codes and map the physical to the digital. The application will achieve transparency and traceability within the vaccine supply chain through the use of immutable record of data and transactions, distributed storage, rules enforcement, and controlled user accesses. This will ensure every vaccine in the supply chain can be isolated, analysed and all activities associated with it identified. Data analytics and creation of dashboards for decision makers will be possible.</p>				
SDG in Focus (when applicable)	<p>SDG 3. Indicator 3.2 and 3.8</p> <p>The application aligns to SDG 3 indicator 3.2 and 3.8 by ending preventable deaths to children under five and access to quality essential health-care services such as vaccines.</p>				

	<p>SDG 9. Indicator 9.1</p> <p>The blockchain application aligns with SDG 9. Indicator 9.1 in that it will provide a reliable and resilient infrastructure that will support human well-being by enabling access to vaccines.</p> <p>SDG 17. Indicator 17.18</p> <p>The blockchain application aligns with SDG 17. Indicator 17.18 by increasing significantly the availability of high-quality, timely and reliable data disaggregated by gender, age, geographic location and other characteristics relevant in national contexts concerning immunization.</p>		
Value Transfer:	The Application will generate assets for transactions on the blockchain. The proof of concept involves three counties in Kenya	Number of Users:	1000
Types of Users:	Manufacturers of vaccines, Manufacturers of cold chain equipment, UNICEF Supply Division, National Vaccine and immunization Programme (NVIP), MoH Head, National Logistitian, Logisticians, National Primary Store Managers, Regional Store Managers, Sub-County store managers, hospitals, health centres, Cold chain equipment technical officers, community health workers and Mothers/care givers, Kenya Regulatory Board		
Stakeholders	Donors, Government of Kenya specifically Ministry of Health (MoH), the citizens who need the vaccines, NVIP, UNICEF, Manufacturers of Vaccines, Manufacturers of cold chain equipment, Kenya Regulatory Board		
Data:	<p><i>What data are expected to be stored in distributed ledger in terms of types, record structure, privacy</i></p> <p>The application has both human actors and what we call IoT actors. Both actors have different data sets.</p> <ol style="list-style-type: none"> 1. IoT actors include data from the (a) i beacons that have temperature sensors that send temperature readings for vaccines in storage and those on transit (b) i beacons that send location data for vaccines on transit and storage (c) identification data that uniquely identifies the different devices involved (ibeacons, smart phones, coldchain equipment, gateways) 2. GS 1 data matrix codes data scanned from the vaccines and hold each vaccine details 3. Human actor's data that includes (a) identification data of participants in the blockchain network since it's a permissioned blockchain (b) assets in the form of messages that are exchanged between the participants (c) Transactions performed along the supply chain (d) Mother-child data for last mile monitoring <p>Privacy is ensured by the blockchain structure of creation of different channels, where one needs authorisation to access any specific channel in the blockchain network achieved through the Certification Authority(CA) of the blockchain architecture.</p> <p>The NVIP plans to set up its own data centre but meanwhile the data will be stored in the DHIS2.</p>		

	<p>Interaction with external data and other systems will be through authorization through the CA of the blockchain architecture in what can be termed as Personal health trains (PHT) that ‘knock’ and are given access after necessary vetting by the CA according to the rules.</p>
Identification:	<p><i>Identification mechanism and rules; ability of participants to be anonymous, etc.</i></p> <p>Identification Mechanism is achieved by the Certification Authority that is implemented as a chain from the root CA to Intermediary CA to the normal users according to allowable rules for authorization. Participants in a specific channel are known because it's a permissioned blockchain.</p>
Predicted Outcomes:	<ol style="list-style-type: none">1. Every vaccine is visible from the time it comes to the country to the last step when it is used on a child.2. Every vaccine's potency is known from the time it comes to the country to the time it is used on a child3. Every transaction done receives consensus from the participants in the permissioned blockchain hence ensuring transparency and accountability4. Every transaction is immutable and so traceability is achieved.5. Provision of high-quality reliable data6. Every vaccine can be accounted for.7. Data on who was vaccinated, how many, by region, by gender is made available.8. Creation of dashboards and maps to decision makers made possible.

Overview of the Business Problem or Opportunity

Existing systems are unable to cope with the changing landscapes of national immunization programme and as a result they experience:

- Stock-outs
- Potential administration of ineffective vaccines
- Avoidable wastage
- Expirees
- Inadequate cold-chain capacity
- Risk of poor product quality and counterfeiting

Why Distributed Ledger Technology?

The DLT solution will improve data capture by introducing automatic data capture through GS 1 data matrix codes and ibeacons. It will provide dashboards allowing stakeholders to see a country wide view of the stock levels. It will enable stakeholders to transact in a secure manner and offer consensus seamlessly to transactions they are required to with all stakeholders in the picture hence offering transparency. It will enable stakeholders in every process have the same data at the same time. It will enable immutability of records that concern vaccines from the time it comes to the

country to the time its administered and hence every step is verifiable. It will enable stakeholders to accurately ensure potency of vaccines administered. It will offer guidance on redistribution of vaccines in cases of shortages.

Section 2: Current process without DLT

Current Solutions

Chango system that is used for stock management. Manual registers for recording vaccine arrival and dispatch/distribution and administration. Fridge tags for temperature monitoring which have no real time streaming of data capabilities.

Existence of data in silos and untimely and/or unavailability of data along the supply chain.

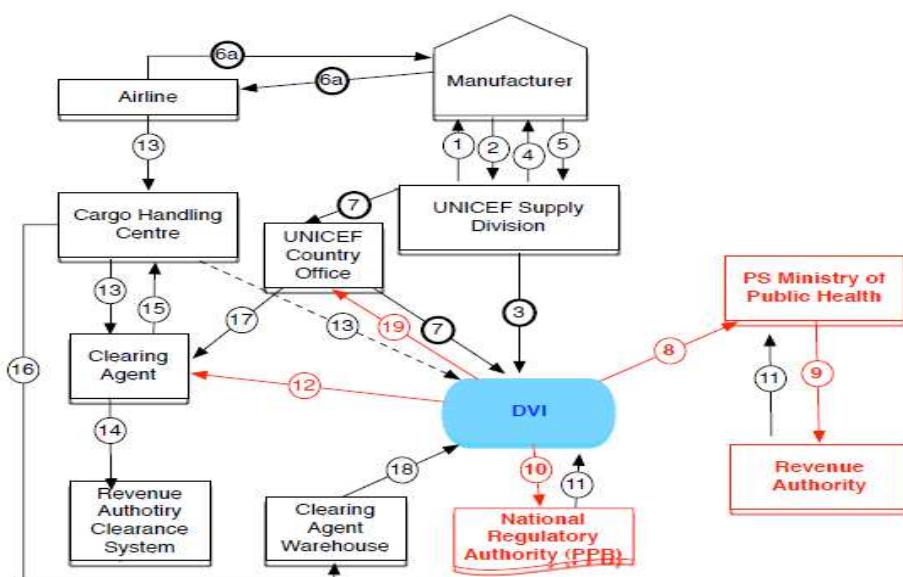
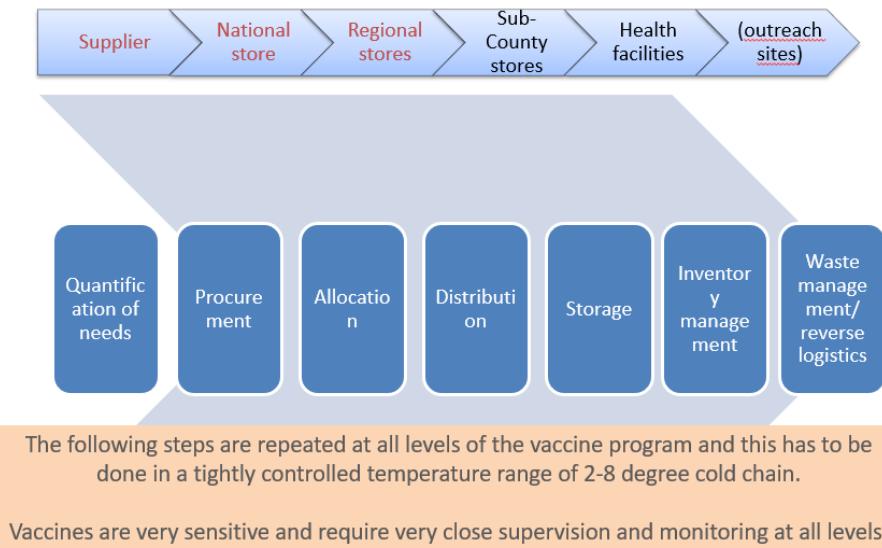
Existing Flow (as-is) Without DLT

Step	User Actions	System Actions
1.	Quantification of needs; concerned personnel fill the information on paper order sheets	In A few places they key in the chanjo system.
2.	Procurement: The NVIP head send the procurement order to UNICEF Supply division which sets in motion the arrival and clearance process once approved. This process is shown in process scheme	
3.	Allocation: The National store allocates to Regional stores, Regional stores allocate to subcounty stores, which allocate to health facilities according to their needs, they fill in paper based vaccine order sheets	In few places this data is again filled in the chanjo system
4.	Distribution; Transporters are engaged to distribute to the regional stores and subcounty stores and health facilities pick their supplies from the subcounty stores.	

Existing Flow (as-is) Without DLT		
Step	User Actions	System Actions
5.	Storage; Stringent SOPs have to be followed during storage and transportation at all levels. The temperatures has to be at acceptable ranges. Every store must record the vaccine details including conditions e.g temperature, wastages and FIFO rules must be followed. The recordings are done on paper-based forms	
6.	Inventory management	A mix of electronic and manual registers is used for inventory management
7.	Waste Management and Reverse Logistics: use paper-based forms to fill in the forms	

Process scheme (as-is)

Vaccine logistics and management



Source: NVIP, MoH Kenya

Data and information (as-is)

Data	Type	Description
1	Vaccine order sheet	Paper- forms that contain number of doses requested for each vaccine type, quantities in stock, date, last order date, current date. In few centres Chanjo stock management system used

Data and information (as-is)		
Data	Type	Description
2	Purchase order	Paper-based form that captures vaccine type, quantity of doses, price per unit
3	UNICEF shipment documents	Five Documents that accompany the shipment of vaccines that enable clearance of vaccines
4	Tax exemption Document	Paper. Based permit
5	Permit from the regulatory body	Paper-based permit
6	Vaccine Details	Antigen type, manufacturer, Batch Id, lot number, expiry date, Temperature
7	Vaccine arrival report	Filled form

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	NVIP head	Head of the entire immunization supply chain and administration of vaccines
2	National Logistician	Oversees the processes
3	UNICEF Country office	Receives the Vaccine arrival report
4	UNICEF Supply Division	Supplies the vaccines
5	Clearing agent	Handles clearance of vaccines from customs on behalf of NVIP
6	Airline	Transports the vaccines into the country
7	Customs	From where the vaccines are cleared
8	Store managers	Receive vaccines, store them, separate wastes from good and dispatch the vaccines and confirm potency
9	Health Workers	Administer the vaccines
10	Mothers and Children	Child is vaccinated
11	Distributors	Contracted to transport vaccines on behalf of NVIP
12	Cold chain equipment Technicians and engineers	Make sure the freezers, fridges, cold rooms and all cold chain equipment works well

Participants and their roles (as-is)		
Actor	Type/Role	Description
13	National Regulatory Authority	Clears vaccines as safe to be administered in Kenya
14	Ministry of Health	Seeks tax exemption for vaccines from KRA

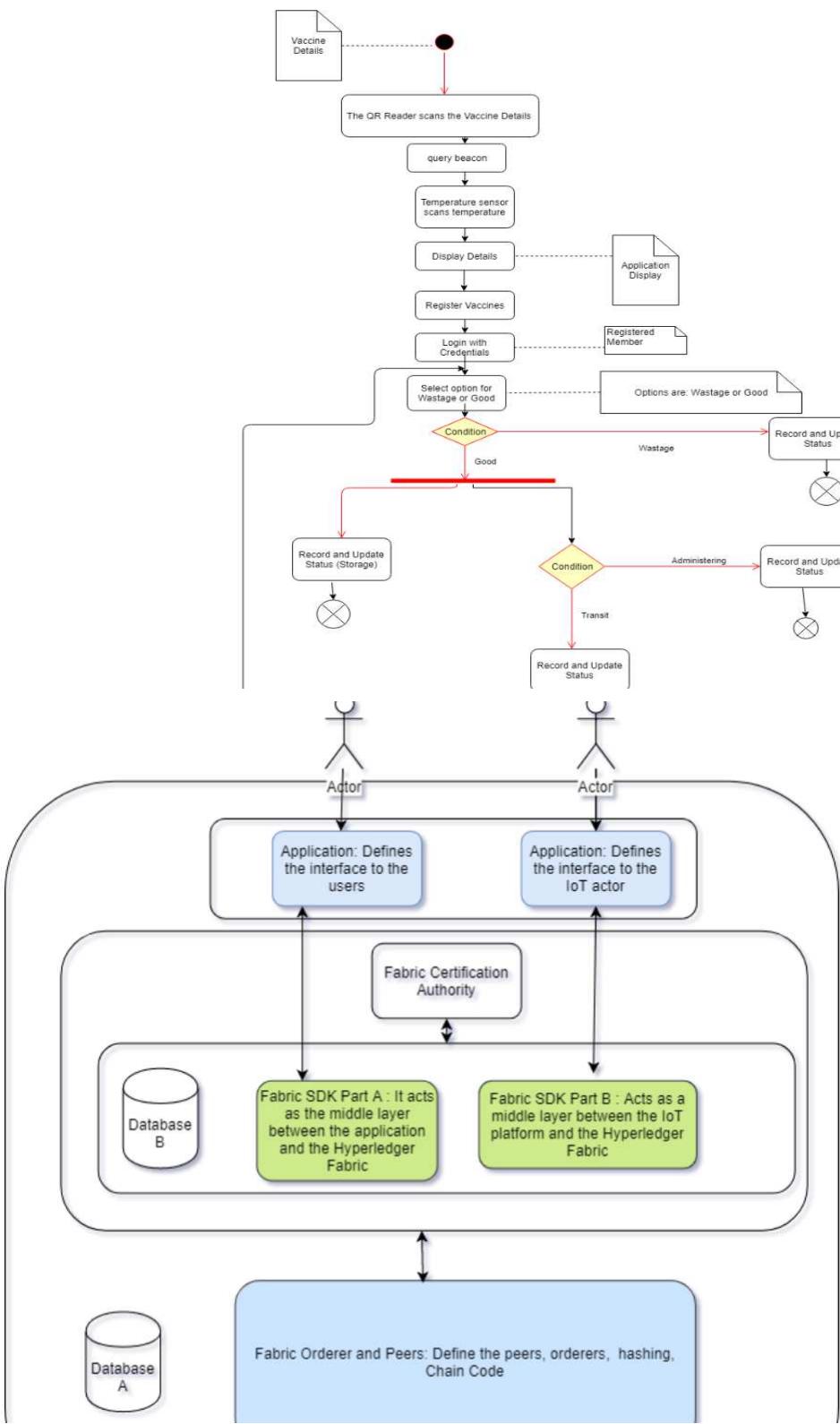
Other Notes
<i>N/A</i>

Section 3: Expected process : VacTrace Blockchain Application (With DLT)

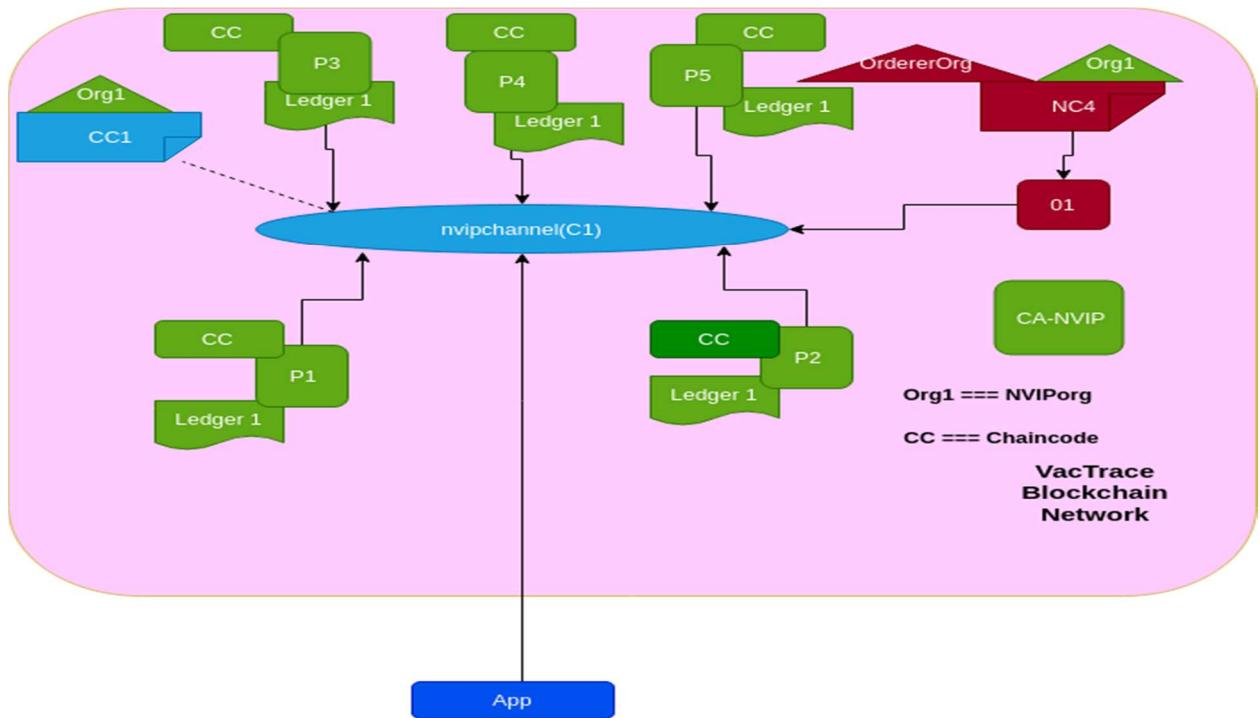
Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Quantification of needs: concerned persons key in the required data into the system	Calculates target population, calculate minimum and maximum doses, get stock available, estimate vaccines needed and generate vaccine order sheet, Submits data into a database, the system submits the data on the blockchain channel for quantification of needs, the concerned participants are prompted by the system for confirmation to reach consensus and the block of data is added on the chain.
2.	Procurement: Fill requestor details, input delivery instructions, fill donor details	Generates procurement order, submits to UNICEF, all participants on the procurement channel give consensus to the data and transactions involved and the block is appended to the chain.
3.	Primary store officer receive arrival dates notification, upload pre-shipment documents, receive pre-shipment documents, sent permit request to National Regulatory board, Tax exemption request sent to MoH,	System sends assets in terms of messages and acknowledgements of receipt. It gets and sends pre-shipment documents, permit and tax exemption signed for authentication by the senders and acknowledge messages send for receipt. The transaction after consensus is appended to the blockchain.

Expected Flow (to-be)		
Step	User Actions	System Actions
4.	Primary store officers receive, record vaccines. Separate the good and bad vaccines and update in database Fill the Vaccine arrival report	Scanner used to update the database of vaccines that arrive. The data matrix form in the system provides a new holder for arrival temperature. ibeacons with temperature sensors in place to read the temperature of vaccines in storage into the system database updated generate the vaccine Arrival Report and submit to UNICEF Country office. The participants in the clearance channel of the blockchain provide consensus to the data and block is appended
5.	Store officers at all levels Arrange vaccines on shelves following FIFO principles	Location ibeacons deployed on each shelf and continuously broadcasting the temperature of vaccines and their details on each shelf. Gateway in place and sends that to the cloud and application. The real time temperature monitoring participants have access to same data and consent and block is appended after agreed time frame
6.	Distribution; Dispatch done according to set SOPs. Use scanners to confirm those dispatched. Ibeacons and gateway are placed in the vehicles	The database updates . the vehicles transmit location, vaccine details and temperature conditions to the transit channel, participants in the channel consent and block added to the block.
7	Administering vaccine to the children. Use scanners to update database. Update data matrix on the mother child card/book	Append the transaction on the administer channel

Process scheme (to-be)



VacTrace Network Structure



Peer Organization

- i) Name: NVIPorg (Org1)
- ii) Ledger 1
- iii) Nvipchannel
- iv) 5 Peers nodes (P1,P2,P3, P4,P5)

Orderer Organization

The Ordering service serves as the network administration point for the VacTrace network and uses the system channel

- i) Name: OrdererOrg
- ii) Solo Orderer for the testing
- iii) System channel(genesis.block)

- iv) The ordering service also supports dashboard nvipchannel linked to a Vactrace client application, for transaction ordering into blocks for distribution

Fabric Certificate Authority

For NVIPorg, there is one **Certificate Authority (CA-NVIP)**. Certificates issued by CAs are at the core of the transaction generation or validation process. For instance, X.509 certificates are used in client application transaction proposal and smart contract transaction responses to sign the transactions digitally. Certificates issued are used to *sign transactions* to show that NVIPorg organization endorses the transaction result – a pre-condition of it being accepted onto the ledger (Ledger1). Different components of the VacTrace Blockchain network use certificates to classify themselves to each other as being from a specific organization. The mapping of certificates to the member organizations is realized by via a structure called a **Membership Service provider (MSP)**.

CA-NVIP

The vacTrace network is a resource, accessed by a **set of users** defined by a Certificate Authority **CA-NVIP**, who have a set of rights over the resources in the vaccine safety network as defined by policies contained inside a network configuration **CA-NVIP**. This is made real when the ordering service node is constituted and started. **CA-NVIP** plays a crucial role in the VacTrace network because it dispenses **X.509 certificates** that can be used to identify participants or nodes as belonging to organization OrdererOrg. Network configuration **CA-NVIP** uses a named MSP to identify the properties of certificates dispensed by **CA-NVIP** which associate certificate holders with organization NVIPorg. The **Network Configuration (NC)** can then use this **MSP** name in policies

to grant actors from NVIPorg special rights over network components. An instance of such a policy is to find the administrators in NVIPorg who can add new member organizations to the network.

Network Configurations and Channel Configurations

- 1) Network Configuration **NC** - The VacTrace network is governed according to policy rules specified in network configuration, the network is under the control of organizations **NVIPorg** and **OrdererOrg**.
- 2) Channel Configuration (C1) with the name; **nvipchannel**, is governed according to the policy rules specified in channel configuration; the channel is under the control of peer organization NVIPorg only.

In VacTrace Network, the ordering service comprises of a single node, **O1**, which is configured according to a network configuration (**NC**), which gives administrative rights to the orderer organization (OrdererOrg). At the network level, Certificate Authority CA-NVIP is used to **dispense identities** to the administrators and network nodes of the OrdererOrg organization.

The Orderer node is initially configured and started by an administrator in organization NVIPorg and hosted in ordererOrg. The configuration **NC** contains the policies that describe the starting set of administrative capabilities for the network. Initially, this is set to only give ordererOrg rights over the network. In the configuration file, the ordererOrg is the first member of the network. The Orderer node is initially configured and started by an administrator in organization NVIPorg and hosted in ordererOrg. The configuration **NC** contains the policies that describe the starting set of administrative capabilities for the network. Initially, this is set to only give ordererOrg rights over the network. In the configuration file , the ordererOrg is the first member of the network.

Adding a Network Admin from NVIPorg

NC is initially configured only to allow ordererOrg users administrative rights over the VacTrace network. An admin from NVIPorg should have similar privileges over the VacTrace network. This

means that the ordererOrg through its root admin should update the network configuration to make the peer organization (NVIPOrg) an administrator too. In this way, even though ordererOrg is running the ordering service, and NVIPOrg has full administrative rights over it. Ordering services are usually **multi-node**, and can be configured to have different nodes in different organizations. For example, we might run O1 in ordererOrg and connect it to another O2. This way, the VacTrace Network would have a **multi-site structure**.

Defining a Consortium

A consortium defines the set of participants in the network who share a necessity to transact with one another – in this case, peer members of NVIPOrg. A network administrator from either NVIPOrg or ordererOrg defines a consortium NVIPConsortium only contains the organization NVIPOrg for now. This consortium definition is stored in the VacTrace network configuration NC. We use consortium NVIPConsortium to create an essential part of a Hyperledger Fabric blockchain a channel.

VacTrace Blockchain APP

Peers and Ledgers

Peer nodes are the network components where copies of the blockchain ledger are hosted. A peer node P1, P2, P3, P4 and P5 can join the channel C1. Peers physically hosts a copy of the ledger L1. Peer nodes and Orderer nodes can communicate with each other using nvipchannel. P1's purpose in the network is purely to host a copy of the ledger L1 for other participants to access. We can think of L1 as being physically hosted on peers but Logically hosted on the nvipchannel. A key part of a peers configuration is an X.509 identity issued by Certificate Authority which associates peers with NVIPOrg organization.

Once peer nodes are started, it can **join channel** the **nvipchannel** using the Orderer O1. When O1 receives this join request, it uses the channel configuration **nvipchannel** to determine P1's permissions on this channel. For instance, **nvipchannel** determines whether peers can read and write information to the ledger L1. Once channel **nvipchannel has a ledger on it**, we can start connecting

client applications (back-end or Front end) to consume some of the services provided by workhorse of the ledger, **the peers**.

Chaincode

ChainCode (CC) can be installed onto **the peers**. VacTrace client application in organization NVIPorg can use **CC** the to access the ledger via peer nodes P1, P2,P3, P4, and P5. The VacTrace client application, peer nodes and the orderer node are all joined to the *nvipchannel*, i.e., they can all make use of the communication facilities provided by that channel.In this case, VacTrace client application can connect to the peer nodes and the orderer node.

NB: In thiscase, VacTrace client application is associated with organization NVIPorg; and although it is outside the Fabric blockchain network, it is connected to it via the *nvipchannel*. All VacTrace client application access is managed via the Chaincode. For now, the critical thing to understand is that to get to this point two operations must have been performed on the Chaincode; it must have been **installed in Peers** and then **instantiated in *nvipchannel*** using **Peers by an** administrator in organization NVIPorg.

Specifically, Peers can see the **implementation logic** of a Chaincode – the program code that it uses to access the ledger L1. After instantiation, **every component** on *nvipchannel* is aware of the existence of the Chaincode but it is not able to see its program logic. Chaincode can now be invoked by vacTrace client application **application**. The most important piece of additional information supplied at instantiation is an **endorsement policy** that describes which organizations must approve transactions before they are accepted by other organizations onto their copy of the ledger. In our *VacTrace Network*, transactions can be only be accepted onto ledger L1 if NVIPorg endorses them. The act of instantiation places the endorsement policy in **channel configuration *nvipchannel***; it enables it to be accessed by any member of the channel.

NB: We contrast this to the Chaincode **interface**, which only describes the inputs and outputs of **CC** Chaincode, without regard to its implementation. Also, when an organization has **multiple**

peers in a channel, it can choose the peers upon which it installs ChainCodes; it **does not** need to install a ChainCode on every peer.

Once a chaincode has been installed on a peer node and instantiated on a channel, it can be **invoked** by a VacTrace client application.

Summary.

Conclusively, NVIPorg and the VacTrace client application can access the ledger L1 through **CC** Chaincode, to generate transactions that will be permitted by NVIPorg, and therefore **accepted onto the ledger** because they conform to the endorsement policy. **The VacTrace Network** grows through the addition of infrastructure from organization NVIPorg. Specifically, NVIPorg has peer node P1, P2, P3, P4 and P5, where each peer host a copy of ledger L1 and Chaincodes. The five peers Join the ***nvipchannel***, which has the VacTrace client application. VacTrace client application are identified using certificates from CA-NVIP. All of this means that the VacTrace client application invoke the **CC** Chaincode on ***nvipchannel*** either using peer node P1, P2, P3, P4 and P5.

Participants and their roles		
Actor	Type/Role	Description
1	IoT actor	GS 1 Data matrix, location ibeacon, temperature ibeacon, gateway, smart phones
2	Human actor	As-is in above table

Data and information		
Data	Type	Description
1	Vaccine details scanned	Digital identifier,Digital twin of the antigen
2	Assets transferred	Information, messages and approvals
3	Real time Temperature readings	ibeacons write to the blocks directly
4	Location readings	Ibeacons in stores transmit location data/ibeacons on transit transmit location data to the block

Security and privacy

Achieved by the CA as shown in the process scheme

Main Success Scenario + expected time line

Prototype scheduled to be complete in April 2019

Conditions (pre- or post-)

Post; to be scaled up for the entire country Pre; adopted in the NVIP strategic plan

Performance needs

At any instance of time a child is being vaccinated in the country. Interoperability achieved via permissioning

Legal considerations

1. Need for standardization of the blockchain and Distributed Ledger Technology
2. Learning Institutions to be deliberate in incorporating DLT education into curriculum

Risks

It would be privacy issues, but the very nature of the architecture that is permissioned, the risk is mitigated

Special Requirements

Training of staff and establishment of data centers and definite platform that integrates smoothly the IoT module, Blockchain and data analytics

External References and Miscellaneous

Use GS 1, Provenance Data Model, Hyperledger Fabric, Cloud services

Other Notes

N/A

Drugs Distribution Ledger

Section 1 Summary

Use Case Summary			
Use Case ID:	HLC-003	Use Case Type:	Vertical
Submission Date:	May 28, 2018	Is Use Case supporting SDGs	No
Use Case Title:	Drugs Distribution Ledger	Domain:	Healthcare
Status of Case	PoC	Sub-Domain	Medicine
Contact information of person submitting/managing the use-case	<i>Full Name</i> Vadim Likholetov <i>E-mail address:</i> vadikas@setere.com <i>Telephone number:</i> +7-921-417-99-55 <i>Social media:</i> none	<i>Job Title</i> CTO <i>Web site:</i> http://www.setere.com	
Proposing Organization	<i>Limited Liability Company “Tech Medical Group”, INN 7841019901</i>		
Short Description	Drug distribution ledger based on DLT can make the distribution process trustworthy and transparent.		
Long description	<p>Main conditions of success scenario:</p> <ul style="list-style-type: none"> • All the medical centers and pharmacies are connected to DDL • Patients can get treatment reports via the internet • All the necessary drugs distribution reports are being provided by DDL <p>The implementation of DLT solution, which allows tracking medical treatments and provides the necessary reports can reduce paperwork and increase common efficiency.</p>		
SDG in Focus (when applicable)	NA		
Value Transfer:	No value transfer	Number of Users:	1000+
Types of Users:	Medical centers, Patients, Federal and Local Government (as auditors)		
Stakeholders	Medical centers, Patients, Federal and Local Government		
Data:	Information about treatment sheets, prescriptions and associated with them drugs distribution should be stored in DLT.		
Identification:	Identification for inserting data to DLT is required. Reports can be provided to anonymous users depending on report type.		
Predicted Outcomes:	Implementation of open DLT for collecting transactions connected with drugs distribution processes will provide transparency of the process. Also every patient can get possibility of tracking their treatment.		

Overview of the Business Problem or Opportunity

There is no information system for collecting all the treatment sheets, prescriptions and connected with them drugs distribution. Every medical centre makes own reports and then send it to government institutions. Patients cannot track their treatment.

Why Distributed Ledger Technology?

The Blockchain and smart-contracts make this process trustworthy and transparent. The implementation of DLT solution, which allows tracking medical treatments and provides the necessary reports can reduce paperwork and increase common efficiency.

Section 2 Current process

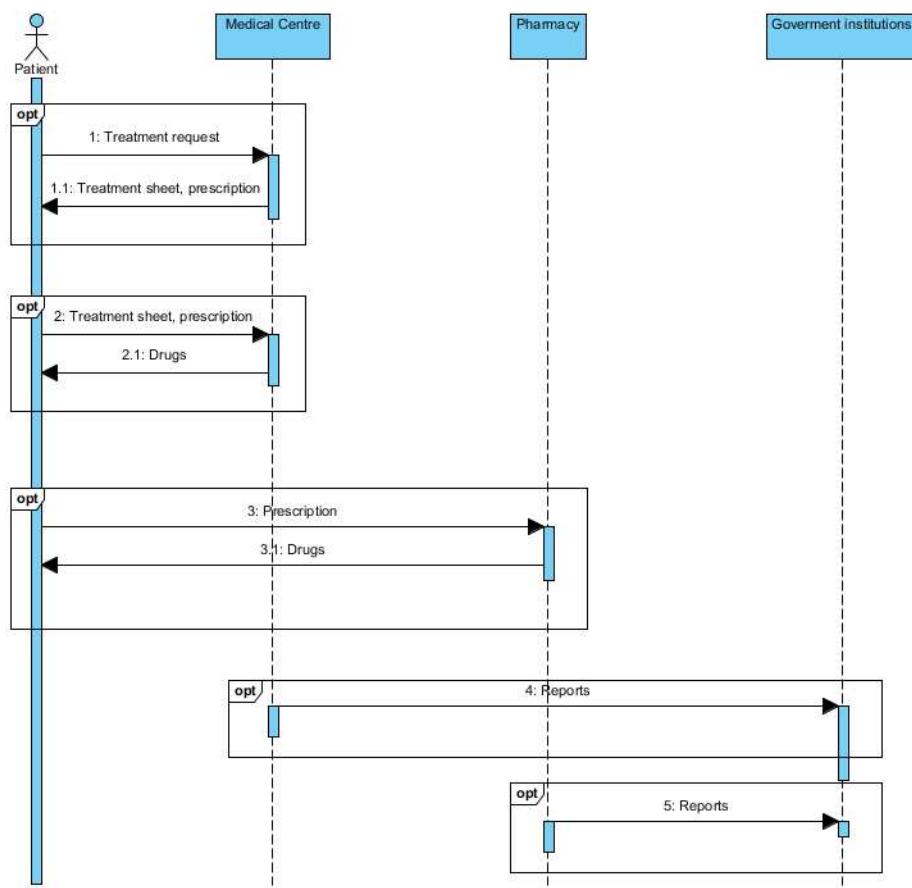
Current Solutions

Medical centres have local Medical Information systems (issuing treatment sheets and prescriptions). Pharmacies have local Drugs distribution systems. Patients cannot track medical treatment. The necessary reports are being provided separately by every organization.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	Medical Centre issues treatment sheet or prescription	n/a
2.	Patient get treatment or drugs according the treatment sheet or prescription	n/a
3.	Medical Centre or Pharmacy creates report	n/a

Process scheme (as-is)



Data and information (as-is)

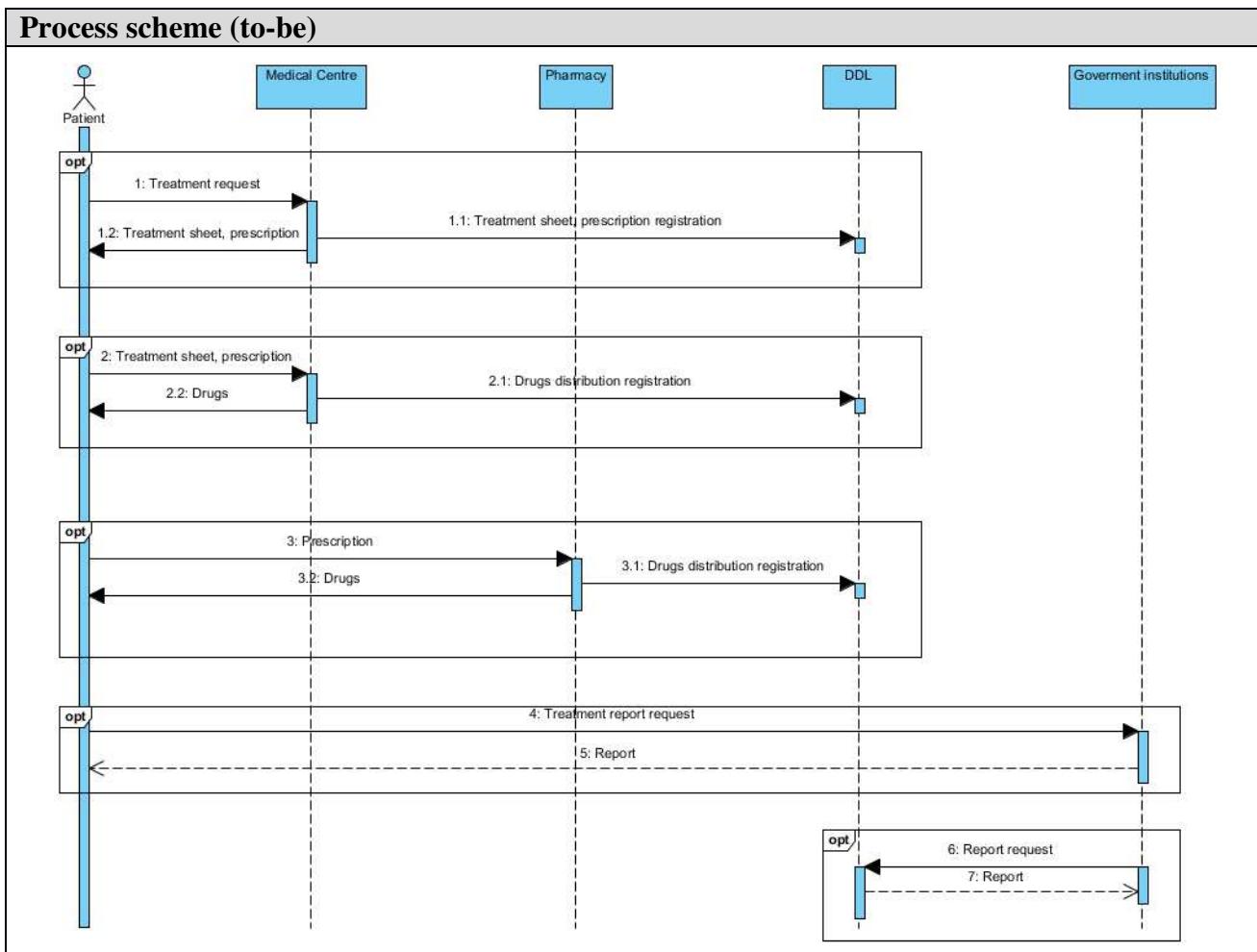
Data	Type	Description
1	Treatment sheet	List of medication and medical procedures
2	Prescription	List of medication
3	Report	Reports of Medical Centers and Pharmacies

Participants and their roles (as-is)

Actor	Type/Role	Description
1	Medical Centre	State or private medical centre
2	Pharmacy	State or private pharmacy
3	Patient	Client of medical center or pharmacy
4	Government Institution	Regulatory or audit functions

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Medical Centre issues treatment sheet or prescription	Registration the treatment sheet or the prescription in DDL(DLT)
2.	Patient get treatment or drugs according the treatment sheet or prescription	Registration the drugs distribution event in DDL(DLT)
3.	Patient get a treatment report	DDL(DLT) provides the treatment report
4.	Governmental Institution get drugs distribution report	DDL(DLT) provides the drugs distribution report



Participants and their roles		
Actor	Type/Role	Description
1	Medical Centre	State or private medical centre

Participants and their roles		
Actor	Type/Role	Description
2	Pharmacy	State or private pharmacy
3	Patient	Client of medical center or pharmacy
4	Government Institution	Regulatory or audit functions

Data and information		
Data	Type	Description
1	Treatment sheet	List of medication and medical procedures
2	Prescription	List of medication
	Treatment Report	Report for Patient
	Drugs Distribution Report	Report for Government Institution

Security and privacy
Identification for inserting data to DLT is required. Reports can be provided to anonymous users depending on report type.

Main Success Scenario
<ol style="list-style-type: none">1. All the medical centers and pharmacies are connected to DDL2. Patients can get treatment reports via the internet3. All the necessary drugs distribution reports are being provided by DDL

Conditions (pre- or post-)
<ol style="list-style-type: none">1. All the local information systems can interact with DDL2. All the transactions needed for DDL correct working are being posted by connected information system

Performance needs
Communication channel capacity

Legal considerations
1.

Risks

Legal risks (possibility to avoid connection of information systems to DDL)

Special Requirements

External References and Miscellaneous

Other Notes

Appendix 1

Domains 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 and logistic
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

Horizontal:

1. Identity Management
2. Security Management
 - a. Public Key Infrastructure
3. Internet of Things
4. Data storage (Inter-organizational data management)

LifeBlocs - Bone Marrow, Blood, and Organ Donation

Section 1: Summary

Use Case Summary			
Use Case ID:	HLC-005	Use Case Type:	Vertical
Submission Date:	January 3, 2019	Is Use Case supporting SDGs	Yes
Use Case Title:	LifeBlocs	Domain:	Healthcare
Status of Case	PoC	Sub-Domain	Bone marrow, blood, and organ donation
Contact information of person submitting/managing the use-case	<p><i>Full Name:</i> Cathy Chen</p> <p><i>E-mail address:</i> cathy.chen@lifeblocs.com</p> <p><i>Social media:</i> N/A</p>	<p><i>Job Title:</i> Co-Founder & CMO & Head of Government Relations</p> <p><i>Telephone number:</i> +1 805 304 5849</p> <p><i>Web site:</i> www.lifeblocs.com</p>	
Proposing Organization	LifeBlocs		
Short Description	<p>LifeBlocs endeavors to reinvent the donation value chain for bone marrow, blood, and organs globally by utilizing the blockchain technology. In doing so, it aims to reduce the number of lives lost as a result of inefficiencies in the donation and matching processes. Moreover, LifeBlocs strives to increase the number of donations amongst the population.</p> <p>Our first use case and current primary focus is bone marrow data storage and matching.</p>		
Long description	<p>LifeBlocs is a start-up that aims to increase blood, bone marrow, and organ donations, and optimize the matching process between donors and receivers. Powered by the Ethereum blockchain, LifeBlocs hopes to optimize supply chain efficiency by equipping each actor in the donation supply chain with a data storage and matching process, from donors and donor organizations to hospitals and patients. It hopes to give patients their much-needed access to healthcare essentials by offering a secure data storage and higher rate of match compatibility, thereby enabling timely availability of life-saving material.</p> <p>In executing its mission, LifeBlocs aims to save human lives by providing the following solutions:</p> <ol style="list-style-type: none"> 1. An easy-to-integrate, decentralized data storage and matching platform that enables greater access for patients, and fosters collaboration between organizations and nations; 2. An incentive system that rewards blood and bone marrow donors through a non-monetary incentive, and through which donors can visualize the impact of their donation; 		

	<p>3. Spreading awareness and increasing the participation of donors worldwide.</p> <p>Finally, through the implementation of LifeBloks' system in multiple smart cities and the learnings gathered in this process, it also plans to provide its system in countries where existing donor systems do not exist.</p>		
SDG in Focus (when applicable)	<p>SDG 3, indicator 3.8.</p> <p>LifeBloks aligns with SDG 3, indicator 3.8, in that it seeks to achieve universal access to a quality essential healthcare services and access to safe, effective, quality and affordable essential bone marrow, blood, and organs for all.</p>		
Value Transfer:	<p>LifeBloks will not generate a token or an asset for transactions on the blockchain.</p>	Number of Users:	N/A
Types of Users:	Donors, Donor organizations, Hospitals		
Stakeholders	Individual donors, donor organizations, hospitals, patients.		
Data:	<p><i>What data are expected to be stored in distributed ledger in terms of types, record structure, privacy, etc.</i></p> <ul style="list-style-type: none"> - The method of storage can be adjusted to comply with specific countries' privacy and health data storage laws. Outlined below is a general description of the default structure. <p>PII (Personally Identifiable Information)</p> <ul style="list-style-type: none"> - PII will be stored separately on a conventional, secure database. <p>Medical Data</p> <ul style="list-style-type: none"> - Medical Data, specifically HLA (Human-Leukocyte Antigen) types, will be stored on IPFS (Inter-Planetary File System). <p>Links to PII and Medical Data</p> <ul style="list-style-type: none"> - The links that provide access to the two sub-sets of data will be stored on the blockchain. Given increased computing power and storage capacity prove to be quite expensive on the blockchain, we aim to utilize blockchain as the technology for the facilitation of storage and matching of health data. <p><i>How DLT solution would interact with external data and other systems.</i></p> <ul style="list-style-type: none"> - The DLT solution interacts with bone marrow registries, IPFS (Inter-Planetary File System), and a conventional, secure database. The DLT stores the separate links to the PII and the Medical data and facilitates cross-border matching. 		
Identification:	When bone marrow registries register new donors, PII and HLA lab results are stored. Bone marrow registries only have access to the PII of individuals that they have registered themselves.		
Predicted Outcomes:	<p>Donors:</p> <p>Individual donors will be able to visualize their individual impact as the LifeBloks system provides a transparent and up-to-date overview of where</p>		

	<p>their donation has been located along the supply chain. Moreover, those who are not donors yet will be encouraged to donate through the non-monetary incentive system.</p> <p>Donor organizations: Organizations that manage donations along the supply chain will become visible and traceable. Furthermore, the data storage and matching process will become more secure.</p> <p>Hospitals: Hospitals will benefit from increased success rates of match compatibility, and face lower administrative costs as a result of the system.</p> <p>Patients: Personal and health data will be stored securely on the system, and patients will have timely availability of life-saving material.</p>
--	--

Overview of the Business Problem or Opportunity

- Technological advancements are lacking in the current tissue and organ donation systems, and lives are lost as a result of inefficiencies in the value chain. As of today, major issues prevent universal access to essential blood, bone marrow, and organs for patients. For example, issues include individuals that are not incentivized to donate, donation registries that are not integrated seamlessly, and large, centralized players in the donor value chain that prevent transparency and traceability.

Why Distributed Ledger Technology?

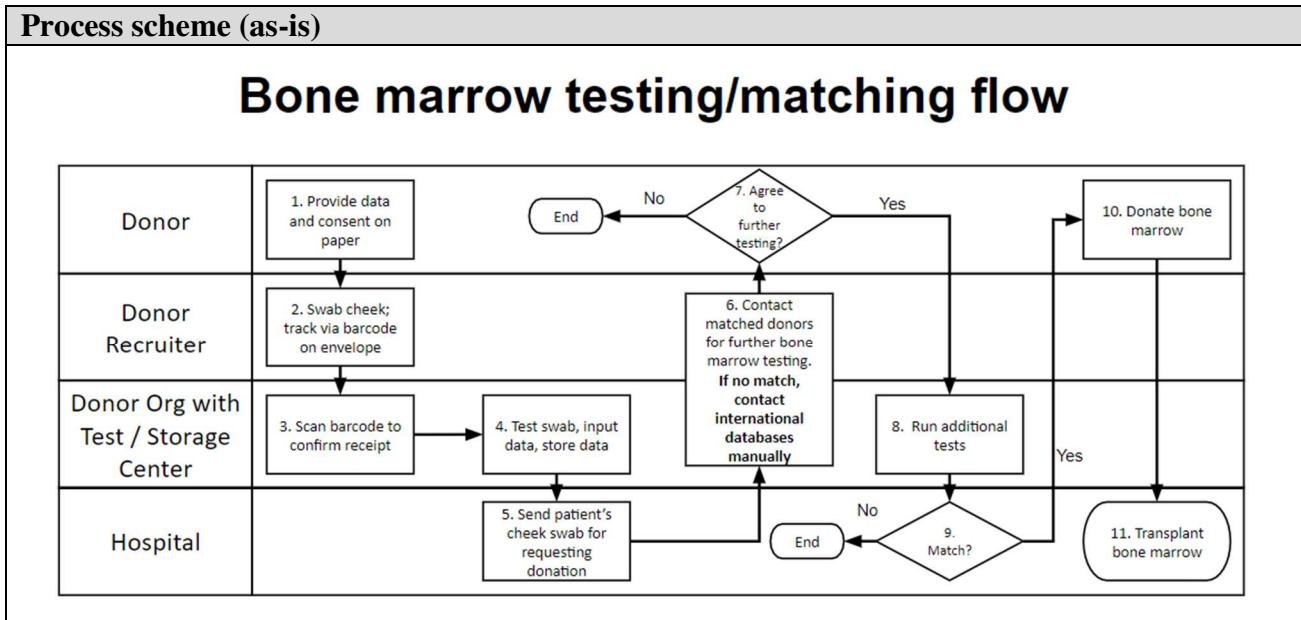
- DLT will seamlessly integrate data siloes across countries without centralizing and harbouring all data in one centralized location. This is essential as many bone marrow registries would be hesitant to share and centralize all of their data into one location. Each of the features listed above (immutability, security, verifiability, transparency) are valuable for our use case of blockchain. For example, having a verifiable source of truth for tracking blood transfusions can be invaluable in countries such as India where, in the past 10 years, 20,000 cases of HIV transmission from blood transfusions have occurred.

Section 2: Current process

Current Solutions

- World Marrow Donor Association currently utilizes a centralized server for matching internationally. DKMS has set up offices in multiple different countries. Neither of these organizations/systems have decentralized/distributed databases. Although, both strive to develop as large of a database as possible.
- Aside from the issue of having siloed data, the administrative processes for registering donors is quite inefficient. Many organizations still use manual paper registration without immediate electronic data or consent storage.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Donor elects to sign up as donor (fills out paperwork manually) and provides DNA sample	
2.	Donor recruiter swabs cheek and sends sample via envelope mail with barcode	
3.	Donor organization lab scans barcode to confirm receipt	System logs receipt
4.	Lab conducts tests and inputs data	System stores lab results
5.	Hospital send DNA sample of patient	
5.1	Repeat Step #4 for patient	System stores lab results
6.	Match patient data against donor database, if no match, manually contact international databases	System matches patient data against database
7.	If there is a match, does the potential donor agree to further testing?	
8.	If so, donor provides blood and doctor runs additional tests	
9.	If additional tests prove positive, donor is eligible to donate	



Data and information (as-is)		
Data	Type	Description
1	PII Data	Personally Identifiable Information such as name, email, phone number, address, ethnicity, country, etc.

Data and information (as-is)		
Data	Type	Description
2	<i>Medical Data</i>	Human Leukocyte Antigen genotypes
3	<i>Other Medical Data</i>	Not currently designed into the bone marrow use case, but for the blood and organs use cases, additional medical data will be necessary such as height, weight, age, sex, sexual orientation/history, recently traveled countries, etc

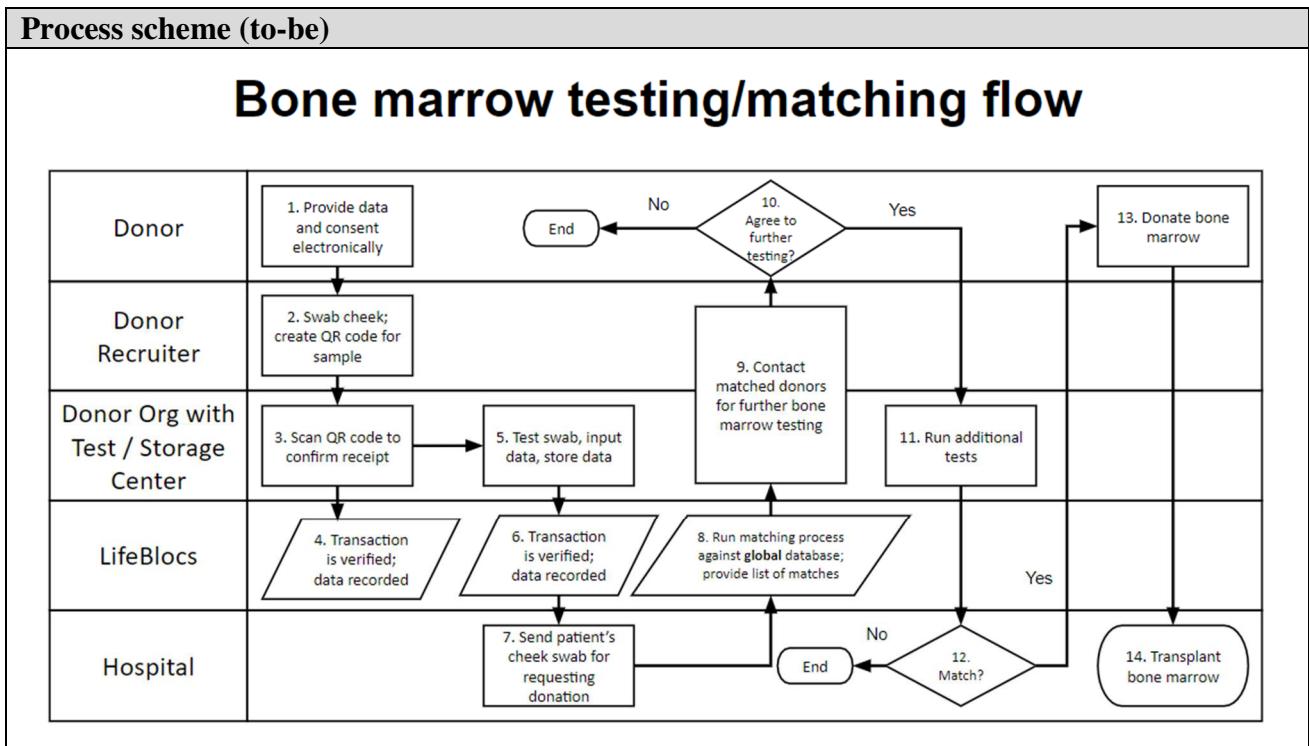
Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Donor</i>	Individual that is willing to donate bone marrow or peripheral blood stem cells (PBSC) to save a patient's life
2	<i>Donor recruiter</i>	Organizations that focus on increasing the number of donors by running bone marrow drives and facilitates the spread of education and knowledge
3	<i>Donor organization / test center / storage center</i>	Organizations that consolidate donors' information to build a database of potential donors
4	<i>Hospital</i>	Provides cheek swab of patient in need of bone marrow transplant

Other Notes
- N/A

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Donor elects to sign up as donor (provides necessary information electronically) and provides DNA sample	
2.	Donor recruiter swabs cheek and sends sample via envelope mail with QR code	System logs sending of cheek swab with a PII link generated stored on secure database
3.	Donor organization lab scans QR code to confirm receipt	System logs receipt
4.	Lab conducts tests and inputs data	System stores lab results to Inter-Planetary File System (IPFS)

Expected Flow (to-be)		
Step	User Actions	System Actions
5.	Hospital scans QR code and sends DNA sample of patient	System logs sending of cheek swab with a PII link generated stored on secure database
5.1	Repeat Step #4 for patient	System stores lab results to Inter-Planetary File System (IPFS)
6.	Match patient data against global donor database	System matches patient data globally
7.	If there is a match, does the potential donor agree to further testing?	
8.	If so, donor provides blood and doctor runs additional tests	
9.	If additional tests prove positive, donor is eligible to donate	



Participants and their roles		
Actor	Type/Role	Description
1	Donor	Individual that is willing to donate bone marrow or peripheral blood stem cells (PBSC) to save a patient's life

Participants and their roles		
Actor	Type/Role	Description
2	<i>Donor recruiter</i>	Organizations that focus on increasing the number of donors by running bone marrow drives and facilitates the spread of education and knowledge
3	<i>Donor organization / test center / storage center</i>	Organizations that consolidate donors' information to build a database of potential donors
4	<i>Hospital</i>	Provides cheek swab of patient in need of bone marrow transplant
5	<i>LifeBloc</i> s	Provides participant #3 with a system that allows a more seamless solution for searching for bone marrow matches globally

Data and information		
Data	Type	Description
1	<i>PII Data</i>	Personally Identifiable Information such as name, email, phone number, address, ethnicity, country, etc.
2	<i>Medical Data</i>	Human Leukocyte Antigen genotypes
3	<i>Other Medical Data</i>	Not currently designed into the bone marrow use case, but for the blood and organs use cases, additional medical data will be necessary such as height, weight, age, sex, sexual orientation/history, recently traveled countries, etc
4	<i>Links to Data</i>	The current infrastructure is built in a way that the blockchain stores the 2 separate links 1. To the PII data and 2. To the medical data.

Security and privacy
- N/A

Main Success Scenario + expected time line
<ul style="list-style-type: none"> - Global adoption with every major bone marrow registry as a member. Best practices and learnings will be applied to create bone marrow registries in countries where registries do not yet exist. We plan to have our pilot implementation completed by end of 2019. Each year, we'd like to have additional implementations in different countries with all countries onboarded by 2030. During this time, we also plan to expand our solution to the blood and organ use cases.

Conditions (pre- or post-)
<ul style="list-style-type: none"> - N/A

Performance needs

- For the bone marrow use case, frequency or load is not of primary concern as bone marrow matching is with a relatively much smaller volume than many other DLT use cases. The current standards should suffice.

Legal considerations

1. USA: HIPAA
 - a. PII and Health data will be stored separately on authorized/certified databases.
2. EU: GDPR
 - a. We will build in a mechanism for breaking the links that provide access to the PII and health data. By destroying the hash, the data becomes inaccessible and unreadable.
3. Korea: Health Data Privacy Consent
 - a. Korean law requires disclosure of what legal entities will have access to / ownership of the data collected. Our current approach to address this is to either 1. Build onto a permissioned/private blockchain or 2. Conduct private transactions on public blockchains.

Risks

Legal risks

- Cross border PII and health data privacy

Business risks

- Limited number of potential revenue channels to sustain the business. Potential to sustain the business through charitable donations

Technical risks

- As with any other DLT use case, advancements in quantum computing poses a risk in the security of the technology

Special Requirements

- N/A

External References and Miscellaneous

- A detailed document with descriptions can be provided upon request.

Other Notes

- We assume all stakeholders in the value chain prioritize increasing the number of lives saved through a more efficient, globally integrated process

My Health Data

Section 1: Summary

Use Case Summary			
Use Case ID:	HLC-006	Use Case Type:	<i>Vertical</i>
Use Case Title:	My Health Data	Is Use Case supporting SDGs	<i>Yes</i>
		Domain:	<i>2 Healthcare</i>
Status of Case	<i>Proof Concept</i>	Sub-Domain	<i>a – Pharma</i> <i>b – Biotechnology</i> <i>c – Medicine</i>
Contact information of person submitting/managing the use-case	<i>Valeria Queiroz</i> <i>Idealizer</i> <i>E-mail address:</i> valfqueiroz@gmail.com <i>Telephone number:</i> 55 21 99327-5080 <i>Social media:</i> https://myhealthdata.github.io/ <i>Web site:</i> www.myhealthdata.com.br		
Proposing Organization	<i>My Health Data, Brazil</i>		
Short Description	<i>My Health Data is born, with the purpose of constructing a system where patient is the sole detector of his/ her data, a system which enables not only unified repository, but, above all, ease of access and portability, once the information holder is the user and not the third party.</i>		
Long description	<p><i>My Health Data using the Blockchain technology, we invite everyone, through our interactions, to create a health data network, in which we will be the agents capable of generating solutions, which bases should be:</i></p> <ol style="list-style-type: none"> 1. <i>Empowerment of people, where the individual is not the patient, but the agent, the generator and the owner of their information;</i> 2. <i>User centralized data generation capable of providing the network with reliable and faithful information;</i> 3. <i>Generation and transmission of consistent information, capable of assisting in medical, pharmaceutical and wellness research and remunerating the parties involved;</i> 4. <i>Creation of an "anti-fragile" system, supported by multiple nodes of the network, encryption, anonymity and database not corruptible and, at the same time, generic capable of adapting to multiple situations, people and cultures easily;</i> 5. <i>User-focused solution, in which the Individuals will always be at the forefront of institutions, whether they are governments or for-profit entities.</i> 		

SDG in Focus (when applicable)	<i>1 – No Poverty 3 – Good Health and Well-being 5 – Gender Equality 8 – Decent work and Economic Growth 9 – Industry, innovation and infrastructure 17 – Partnership for the goals</i>		
Value Transfer:	<i>Data, tokens</i>	Number of Users:	<i>0</i>
Types of Users:	<i>Patients, Partners (hospitals, clinics, doctor office, laboratories)</i>		
Stakeholders	<i>Government, Researchers, ...</i>		
Data:	In My Health Data the information is always stored under this primary key and with the permission of the key owner. The system, based on the patient's permissions, controls access to medical records, permits the inclusion, removal and reading of medical records by the patient or third parties, makes the sale of such data available to third parties, where negotiation is done directly between interested parties, but always preserving the identity and anonymity of those who make them available.		
Identification:	<i>Identification mechanism and rules; ability of participants to be anonymous, etc.</i>		
Predicted Outcomes:			

Overview of the Business Problem or Opportunity	
<i>The platform that consists of a smart contract that not only validates operations, but also stores and creates a patient-centred health data network that can be used in a variety of applications such as academics surveys, hospitals, laboratories and the pharmaceutical industry.</i>	
Why Distributed Ledger Technology?	
<i>Due to the characteristics of the DLT, such as immutability, transparency, security, distribution, verifiable, technology can take these characteristics to medical data ensuring safety, ensuring that the patient knows who is accessing their data and ensuring universal access from anywhere in the world, anytime.</i>	

Section 2: Current process

Current Solutions
<i>If there are existing systems which automate the above business problem/opportunity.</i>

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	<p><i>The patients information have been spread out in different silos, which are Labs, hospitals, doctor offices.</i></p> <p><i>As consequence, the patient does not have access to all his/her information when needed, mostly when they are sick.</i></p> <p><i>This decentralization generates the lack of interoperability and lack of control over health information, that causes a fact known as asymmetry of information.</i></p>	<i>Decentralization of health data in different silos, such as hospitals, clinics, laboratories, doctors offices.</i>
2.		

Process scheme (as-is)

Data and information (as-is)		
Data	Type	Description
1	<i>Documents: There is no pattern</i>	<i>Documents and data spread out in different silos.</i>
2	<i>Payment transactions</i>	

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Patient</i>	Patient has no control or possession over his/her health data.
2	<i>Hospital/Clinic/Doctor Office</i>	Health data are stored in a decentralized way, each entity storing it in their respective silos.

Other Notes
<i>Any assumptions, issues</i>

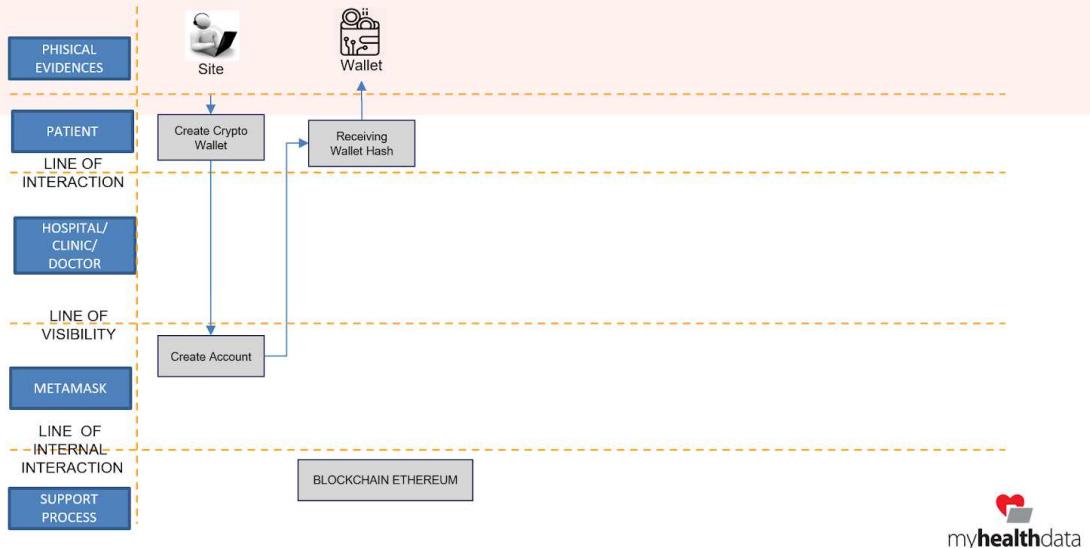
Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	<p>My Health Data proposes, through the empowerment of the patient, making them the sole owner of their medical data, solving the above mentioned problems of information silos, interoperability and asymmetry of information, having developed, for that purpose, a smart contract, published in the blockchain Ethereum network, which is capable of providing a patient-centered medical data repository system, having as primary key its Ethereum account.</p> <p>The My Health Data smart contract has been structured in a way that any entity can develop applications on it, as long as the information is always stored under this primary key and with the permission of the key owner (the patient). Thus, the system, based on the patient's permissions, as described above, controls access to medical records, permits the inclusion, removal and reading of medical records by the patient or third parties, makes the sale of such data available to third parties, where negotiation is done directly between interested parties, but always preserving the identity and anonymity of those who make them available.</p>	Install and create a Metamask application and access https://abezzerrademenezescavalcanti.github.io/saudechain
2.		

Process scheme (to-be)

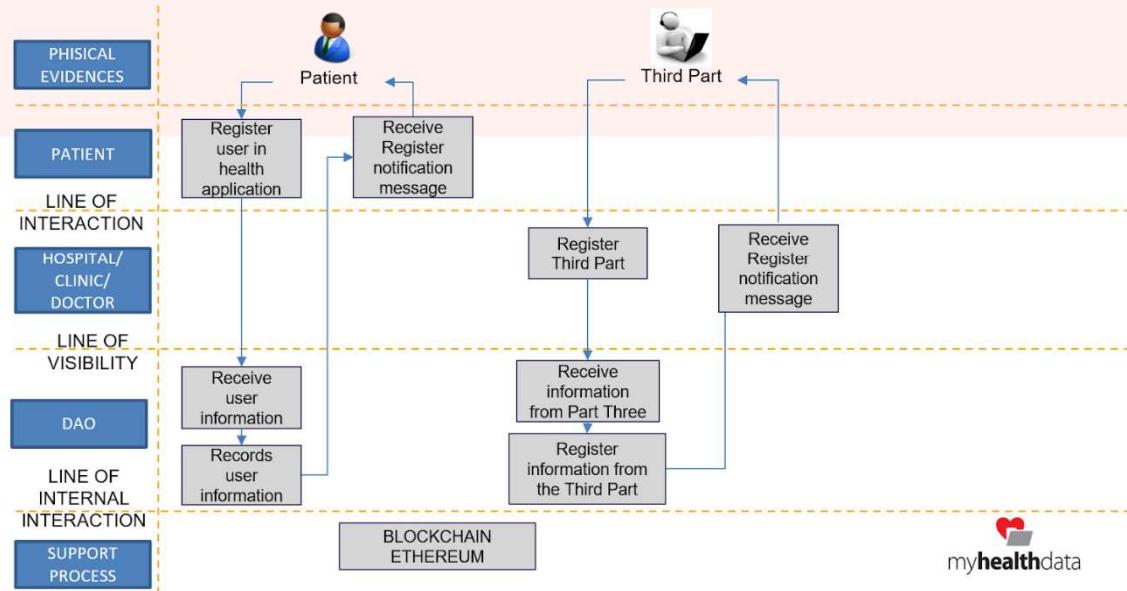
Master Account Creation

Service Blueprint Process – Creating Master Account

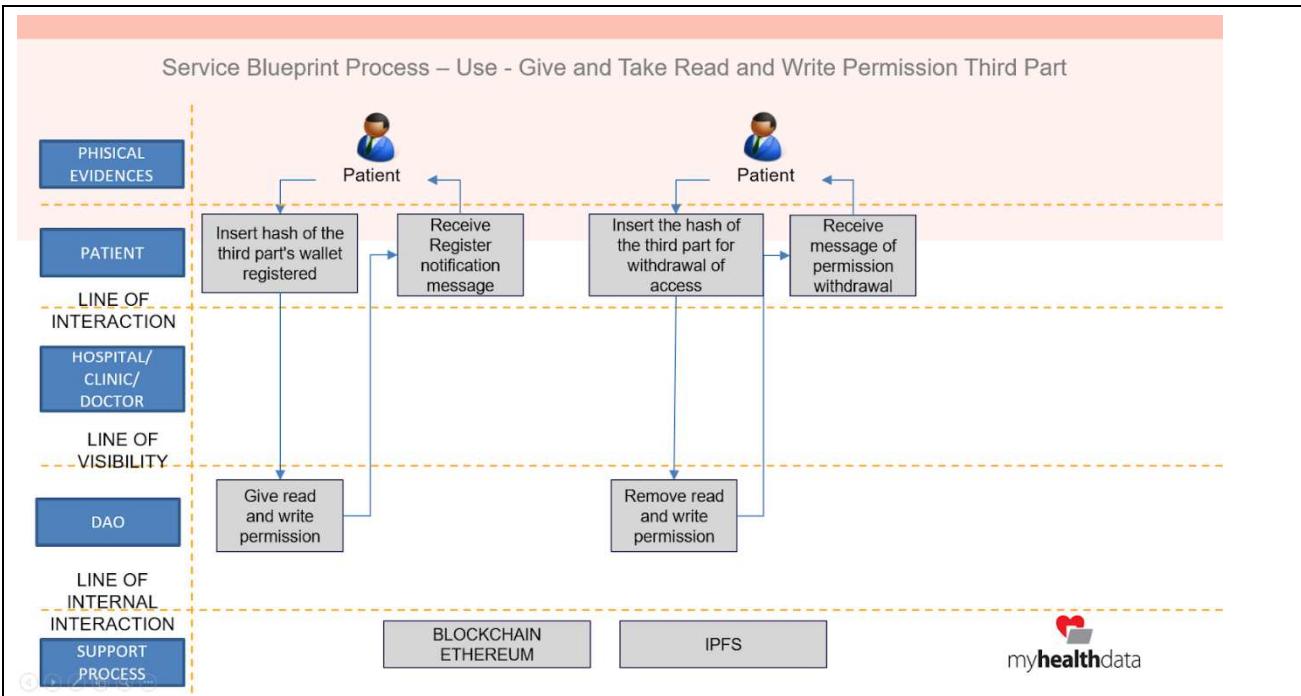


Patient and Third Part Registration

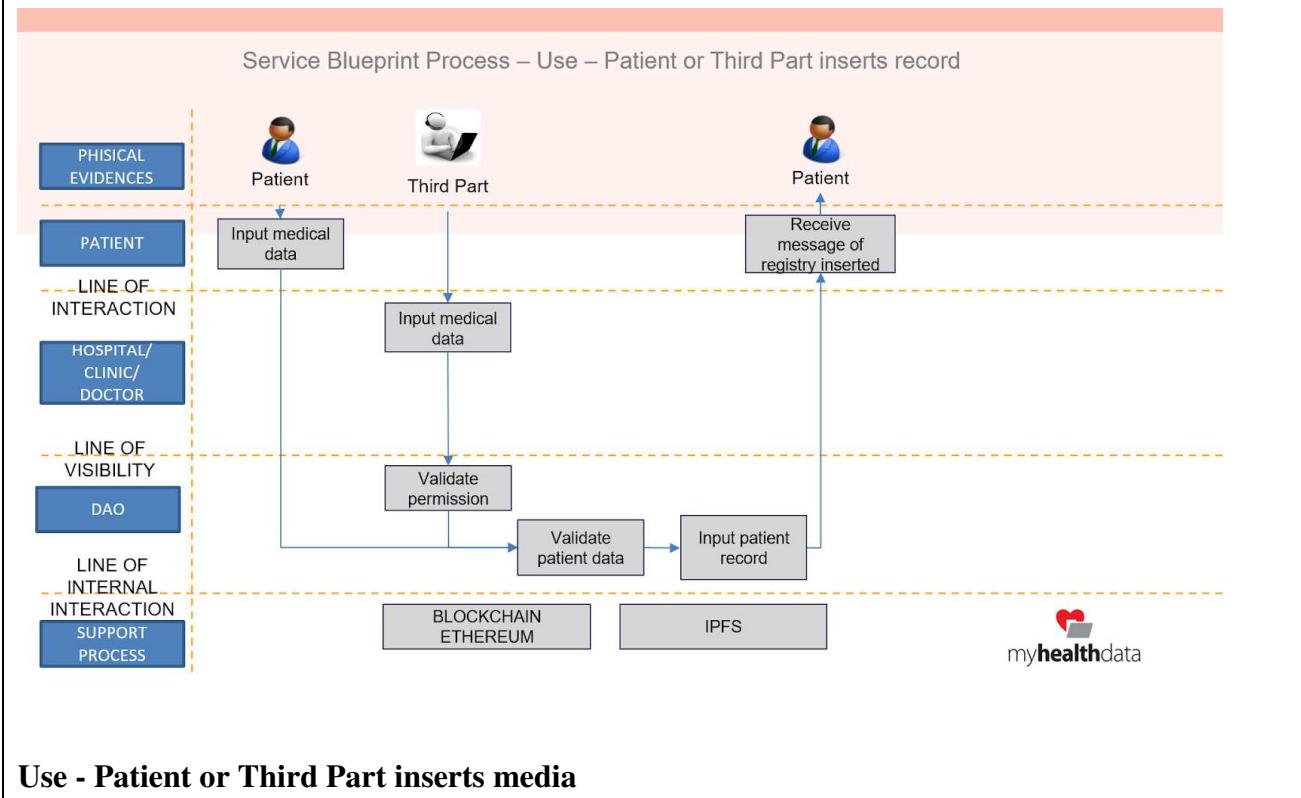
Service Blueprint Process – Register



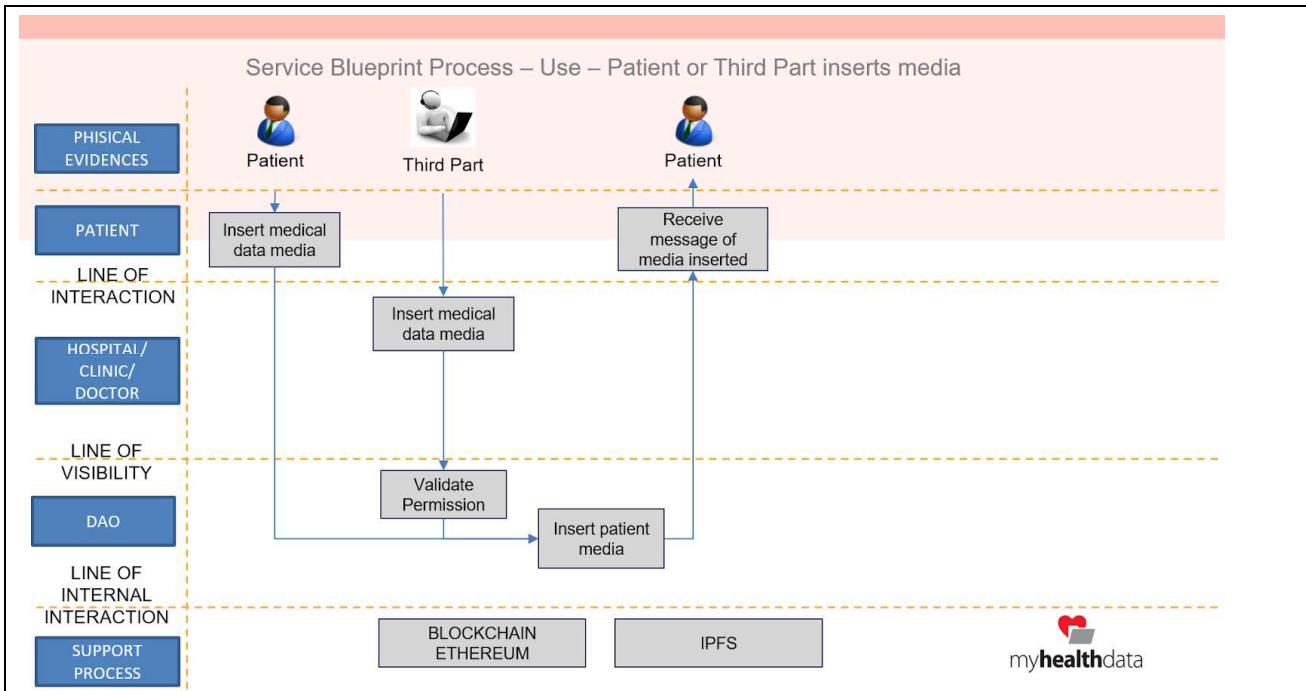
Use - Third Part reading and writing permission



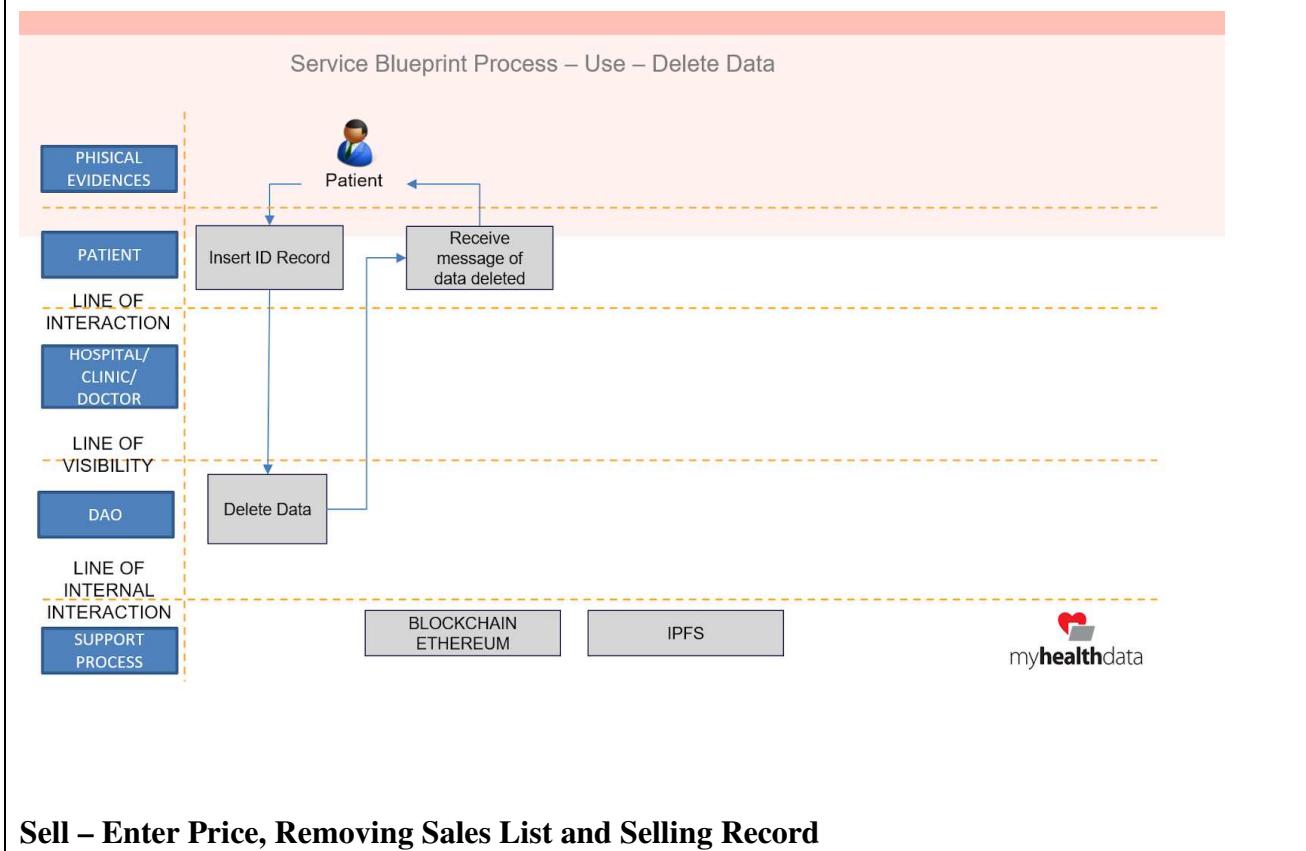
Use – Patient or Third Part inserts record



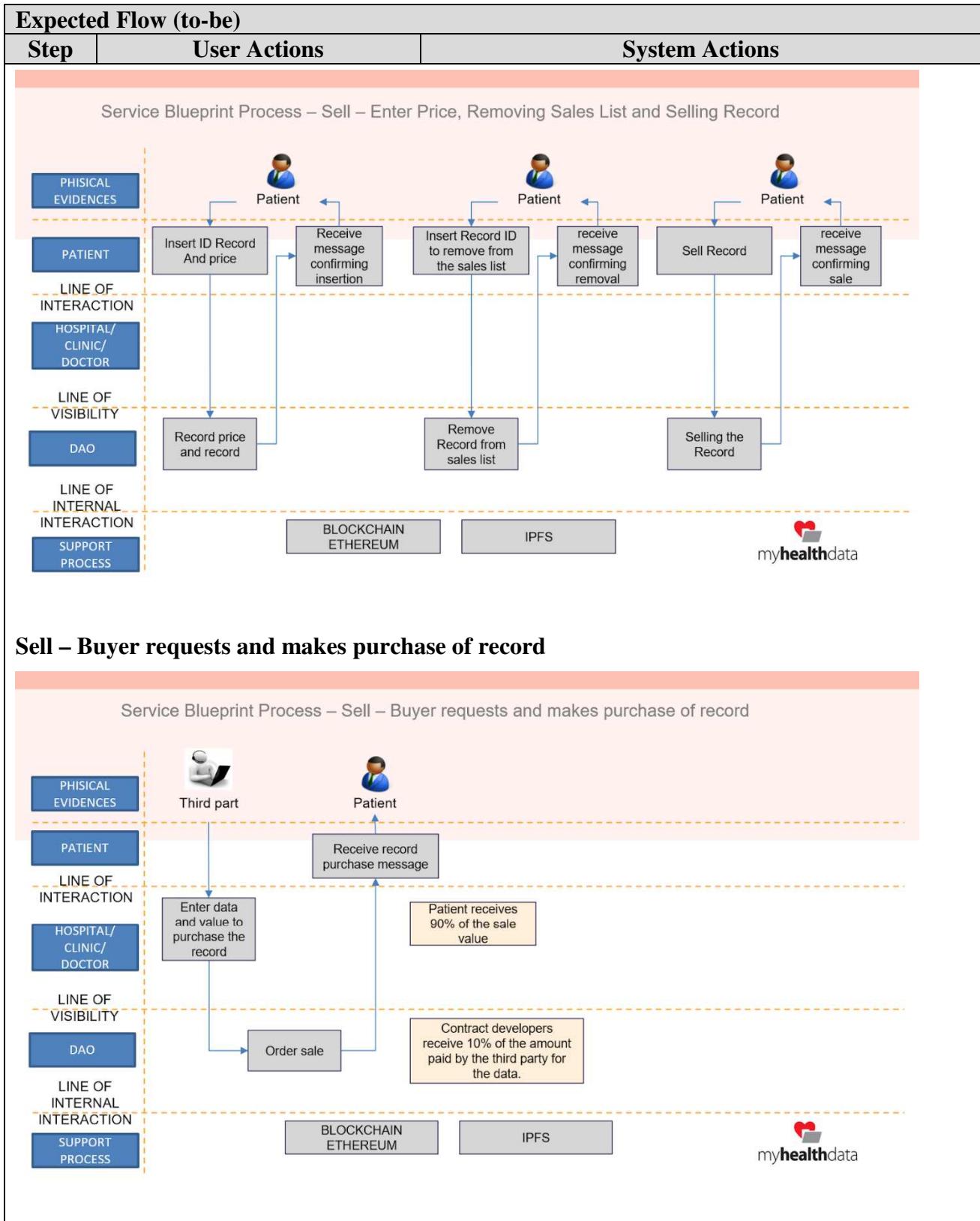
Use - Patient or Third Part inserts media



Use - Delete Data



Sell – Enter Price, Removing Sales List and Selling Record



Participants and their roles		
Actor	Type/Role	Description
1	Patient	Patient can create register, give third party permission to read and insert data, sale permission and delete data.

Participants and their roles		
Actor	Type/Role	Description
2	<i>Hospital/Clinic/Doctor Office</i>	Receive permission from patient to read and insert data and buy data.
3		

Data and information		
Data	Type	Description
1	<i>Documents</i>	
2	<i>Payment transactions</i>	

Security and privacy
1.

Main Success Scenario + expected time line
<i>Description of DLT-based solution, which potentially will be created</i>

Conditions (pre- or post-)
1.

Performance needs
<i>What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.</i>

Legal considerations
<i>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.</i>
1.

Risks
<i>Legal, business and technical risks related to use case</i>

Special Requirements
<i>Business and technical requirements of use case</i>

External References and Miscellaneous

List of references for standards or well-defined mechanisms if any of requirements calls for the implementation of a standard or protocol or other well-defined mechanism. If the use case needs non-standard consensus mechanisms or cryptographic tools, such information should be included here. Also such section may be used to provide more information regarding the use case including links to any kind of related materials, terms and descriptions or any other related information.

Other Notes

Any assumptions, issues

Global Market Place for Mobile Operators and Service Providers

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-001	Use Case Type:	Vertical
Submission Date:	October 11, 2018	Is Use Case supporting SDGs	No
Use Case Title:	Global market place for mobile operators and service providers	Domain:	IT & Telco
Status of Case	PoC	Sub-Domain	Mobile roaming Digital Services
Contact information of person submitting/managing the use-case	Full Name: Alexander Yakovenko Job Title: Project Director E-mail address: ayakovenko@clementvale.com Telephone number: +7-985-991-2048 Social media: https://www.linkedin.com/in/alexander-yakovenko Web site: https://www.blockchaintele.com		
Proposing Organization	Clementvale Baltic OU, Estonia		
Short Description	This use case is a proposal to create global market place for mobile operators and service providers with the use of private Blockchain ecosystem by changing traditional roaming rules and creating new sales channels, using a stable coin for immediate payments.		
Long description	This use case is a proposal to create global market place for mobile operators and service providers with the use of private Blockchain ecosystem. The main goal is to enable mobile operators and service providers to interact directly and securely without any agreements, intermediaries and complex integration via smart contracts. This solution significantly simplifies all processes, eliminates old-fashioned roaming technology, shifts principles of interaction, reduces costs on all levels, gives an easy and quick access to global market for all players in a short period of time with almost zero investment, gives a good opportunity for mobile subscribers to use services at reasonable rates worldwide, changes principles of settlements, making them in real time in stable coin. We created one of the stable token that equals 1 SDR used in telecommunications, which is tied to the basket of five world currencies. We named it SDRt (SDR Token). It's the unit of payment given to providers for their services, i.e., the price of services is measured in these units.		

SDG in Focus (when applicable)			
Value Transfer:	SDR tokens representing fiat money	Number of Users:	100+
Types of Users:	Any MNO/MVNO and/or service provider, mobile subscribers		
Stakeholders	Any MNO/MVNO and/or service provider		
Data:	Offers on mobile and non-telecom services published by operators and service providers, Requests on services, User ID, Service provider's digital code, SDR tokens flow, Other transactions related to rendering services		
Identification:	Nodes verify all transactions via consensus algorithm		
Predicted Outcomes:	<ul style="list-style-type: none">- Elimination of any agreements, intermediators and complex integration- Change of traditional roaming rules- Reduction of mobile services costs- Secure and direct interaction between mobile operators or operators and service providers via smart contracts- Quick access to global market for small and medium-sized mobile operators and service providers- Provision of own subscribers with local rates around the world in a short period of time with almost zero investments- New sales channels for service providers		

Overview of the Business Problem or Opportunity

Current problems:

- Long and complicated process to implement mobile services in roaming, requiring negotiation between operators, signing a lot of roaming agreements, physical interconnection of networks, different tests and other integration processes;
- High rates for mobile subscribers in roaming, which increase cost of this service and cause big inconvenience for end users;
- Low consumption of services, which effects on decreasing of mobile operator's revenue due to huge amount of "silent roamers";
- Huge expenditures on infrastructure support;
- Necessity for mobile operators to have a large staff to maintain commercial, legal and technical processes of mobile roaming services;
- Marketing expenditures for service providers to promote their services

Blockchain technology is a platform to construct a global trusted marketplace, where mobile operators and service providers can interact directly with each other without agreements, intermediators and costly integration.

Opportunities:

For mobile operators:

- Simple and low-cost access to global roaming market.
- Provision of own mobile services to subscribers of other operators worldwide.
- Possibility to resell mobile and non-telecom services from global providers to own subscribers.

For service providers (content providers, software vendors, insurance, transportation, etc):

- New sales channels to subscribers of mobile operators.

For subscribers:

- To get high quality mobile and non-telecom services worldwide at affordable prices.

For all participants:

- Elimination of intermediaries in sales chains.
- Reduced time and costs for mutual settlements between participants.
- Significantly reduced costs on technical, legal and commercial levels

Why Distributed Ledger Technology?

- Community-controlled DLT system ensures participants that the system operates according to the strictly defined software-driving rules.
- Unlike classical centralized approach, there is no party or organization that could change rules on its own. Therefore, there are minimal risks for participants and their investments.
- Minimal investments into hardware and software infrastructure.
- Exceptional reliability of the system because of inherent security, redundancy and self-restoring capability of DLT platform.

Section 2 Current process

Current Solutions

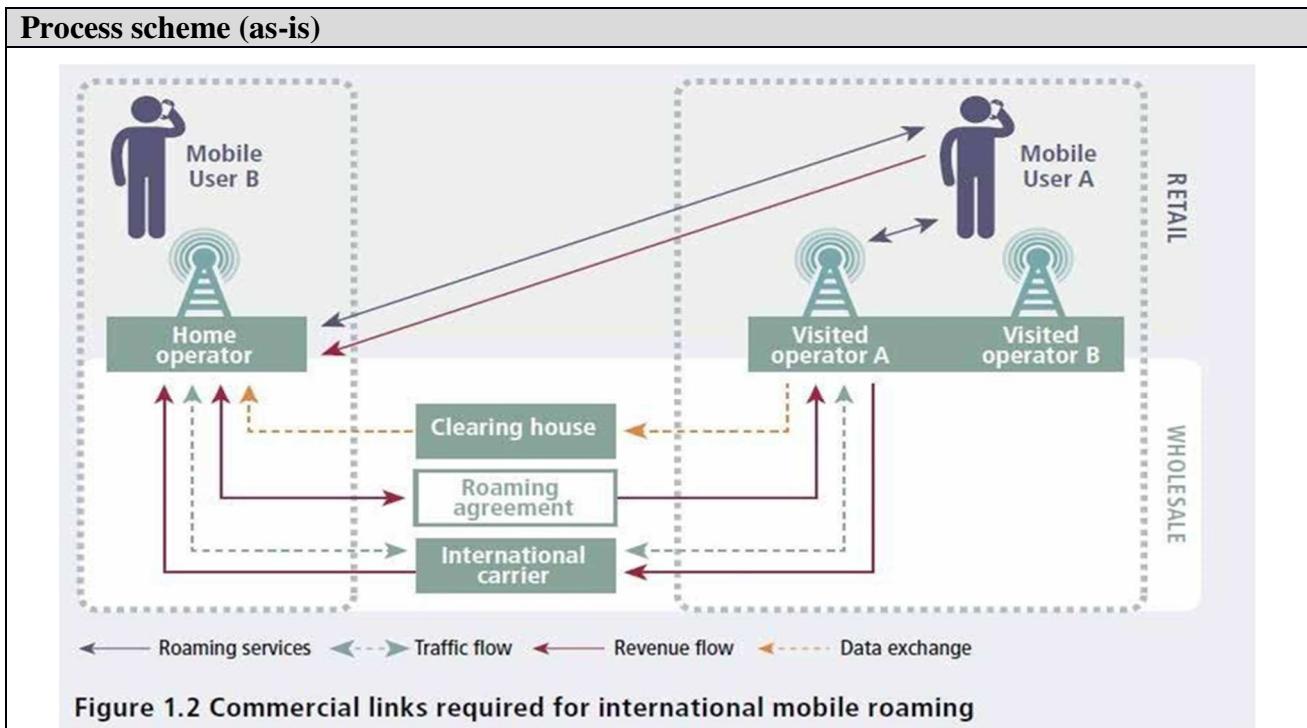
Current roaming technology is cumbersome, expensive and hard to implement as it requires a long process, including negotiations between mobile operators, approval of business cases, commitments, legal confirmation, signing hundreds of roaming agreements with each operator in each country, necessity to be a GSMA member, interconnection of networks, technical tests on different levels, proper equipment and other integration processes. It bears cost on the integration of carriers, measured in years and millions of dollars. As a result, the roaming services market has become virtually monopolized by the major carriers, and it is closed to regional carriers. The latter actually lose their subscribers at a time when they are traveling abroad.

As for service providers it takes time and bears additional cost and efforts to reach customers.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	MNO/MVNO determines a contact and negotiates with another international MNO/MVNO	n/a

Existing Flow (as-is)		
Step	User Actions	System Actions
2.	MNO/MVNO of one country signs roaming agreement with another international MNO/MVNO	n/a
3.	Mobile operators of both countries arrange interconnection of their networks and conduct necessary technical tests to provide roaming services	n/a
4.	Mobile operators of both countries exchange rates for their services and establish tariff plans for own subscribers	Tariff plans are published on operator's server
5.	Mobile subscribers choose/buy tariff plans via operator's user interface (web account or application) and travel abroad	Mobile subscribers of Home operator are registered in the network of Visited operator on arrival
6.	Mobile operators render roaming services based on agreed terms	n/a
7.	Mobile operators exchange invoices and make settlements	n/a



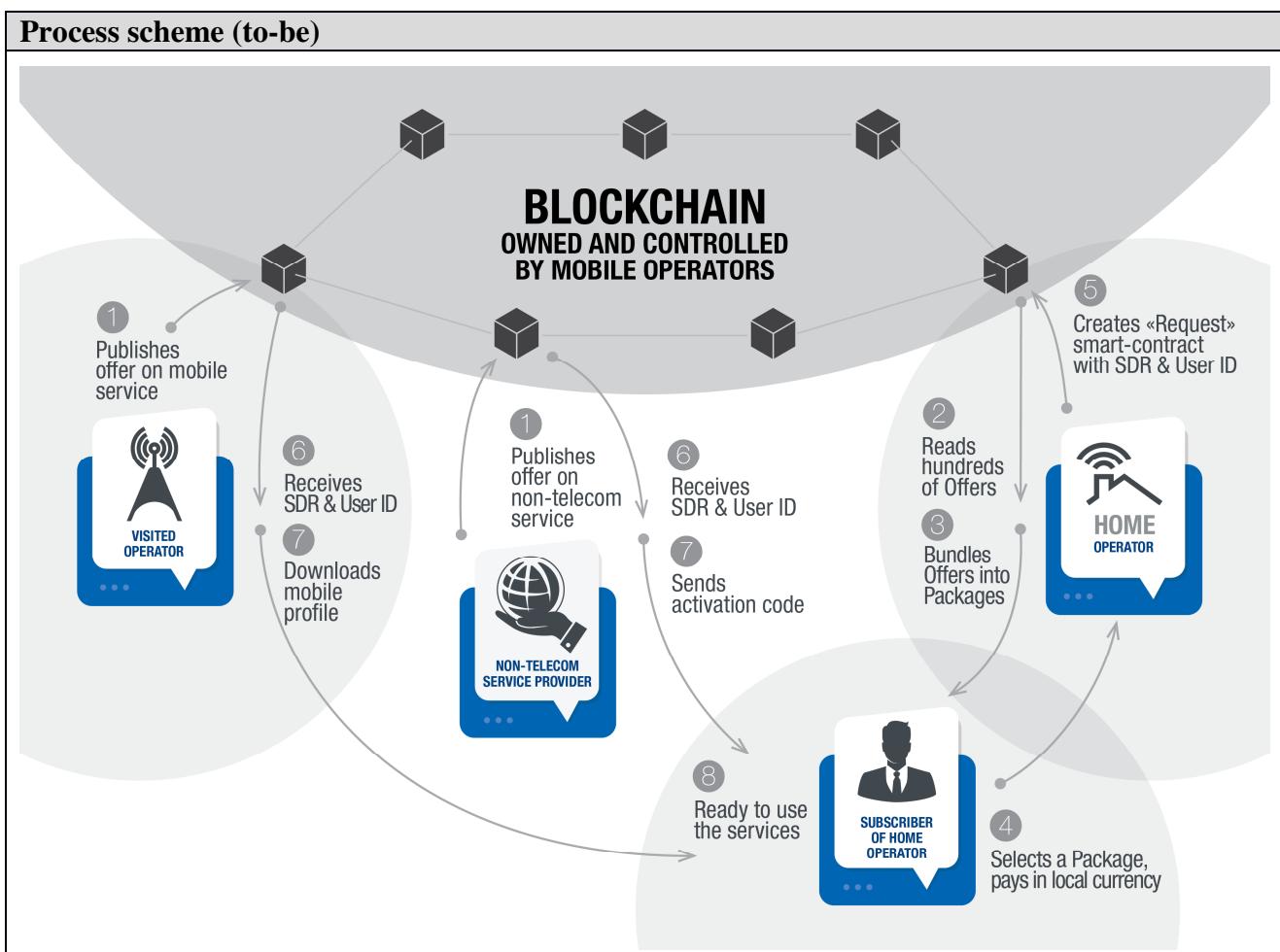
Data and information (as-is)		
Data	Type	Description
1		
2		

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	MNO/MVNO	Any mobile network operator or mobile virtual network operator providing its own subscribers with international roaming services
2	Mobile subscribers	Mobile subscribers consuming international roaming services

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Any MNO/MVNO (Visited operator) and/or service provider (SP) publishes Offer on its own mobile services/non-telecom services onto Blockchain	“Offer” smart contract is created in Blockchain and system verifies it by all nodes
2.	Any MNO/MVNO joined Blockchain reads Offers published by another MNO/MVNO and/or SP via Blockchain account	n/a
3.	Any MNO/MVNO (Home operator) chooses Offers, edits them, bundles into packages and proposes them to its own subscribers with the use of User interface (web or app)	n/a
4.	Mobile subscriber of Home operator selects a package and pays for it in local currency	n/a
5.	Home operator creates Request smart contract with the user ID, other technical information and SDRT payment and sends it to Blockchain	“Request” smart contract is created in Blockchain and systems verifies it by all nodes
6.	Visited operator or SP receives request via Blockchain and accepts request supplying encrypted mobile profile data or SP's code and other technical information necessary to get a service	“Accept” smart contract is created in Blockchain, system verifies it and matches to “Request” smart contract created at previous step
7.	Home operator downloads mobile profile received from Visited operator to subscriber's multi-SIM via OTA platform and/or activates SP's code.	n/a
8.	Mobile subscriber of Home operator is activated in the Visited operator's network on arrival or in the SP's system	n/a

Expected Flow (to-be)		
Step	User Actions	System Actions
9.	Visited operator or SP serves the subscribers of Home operator according to the contract purchased and reports service consumption to the Blockchain.	Transactions about service consumption are published in Blockchain. SDR tokens are transferred from account of Home Operator to account of Visited Operator according to consumptions.



Participants and their roles		
Actor	Type/Role	Description
1	MNO/MVNO	Any mobile network operator or mobile virtual network operator providing its own subscribers with international roaming services
2	Mobile subscribers	Mobile subscribers, consuming international roaming services
3	Nodes / Validators	Nodes ensure data integrity and provide consensus.

Participants and their roles		
Actor	Type/Role	Description
4	Service provider	<u>Any service provider, such as content providers, software vendors, insurance companies, logistic or transport organizations, hotels, etc.</u>

Data and information		
Data	Type	Description
1	Offer	Service with detailed description and price (in SDRt) published by any MNO/MVNO
2	Request	Order on an Offer selected by a subscriber of any MNO/MVNO
3	SDRt	SDR token – a stable token tied to SDR (Special Drawing Rights). This token is used for payment for services of mobile operators and service providers
4	User ID	Logical entity used to identify a user on a software, system, website or within any generic IT environment. It is used within any IT enabled system to identify and distinguish between the users who access or use it.
5	Mobile profile	Set of keys for secure registration of a SIM-module in the mobile network of Mobile Operator who owns this Mobile profile
6	Smart Contract	Computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a <u>contract</u> . Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.
7	SP's code	Special digital code of service provider needed for service activation

Security and privacy
Sensitive information is encrypted. All transactions are signed by digital signatures of all participants. Personal data of end user dose not store in Blockchain. Only internal ID of end user is transmitted for further direct identification by Visited operator or SP in its network/system.

Main Success Scenario
<ol style="list-style-type: none">1. Mobile operators and service providers interact directly and securely without agreements, intermediators and additional integration via smart contracts.2. Any small and medium-sized MNO/MVNO and/or service provider becomes global in a very short period of time.3. Mobile subscribers get high quality services from mobile operators and service providers at affordable rates.

Conditions (pre- or post-)

n/a

Performance needs

Fast transactions and confirmations from DLT system are necessary.

Currently it takes 3-5 seconds of delay for transaction' confirmation and in average about 10 000 transactions per second, which is enough for all expected technical loads.

Legal considerations

n/a

Risks

Special Requirements

- It is necessary for Home Mobile operator to produce and distribute [Multi-Account SIM-cards](#) or [eSIMs](#) among its subscribers;
- It is necessary for Home Mobile operator to have OTA (over-the-air) platform to upload mobile profiles.

External References and Miscellaneous

https://wiki.blockchaintele.com/index.php/Main_Page

https://wiki.blockchaintele.com/index.php/Use_cases#Global_coverage_with_local_rates_for_subscribers

Other Notes

Open questions:

- Settlement in SDRt is a subject of further study and implementation.

Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers

Section 1: Summary

Use Case Summary					
Use Case ID:	ICT-002	Use Case Type:	<i>Vertical</i>		
Submission Date:	July 14, 2019	Is Use Case supporting SDGs	<i>no</i>		
Use Case Title:	Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers	Domain:	1-c 3-f		
Status of Case	PoC	Sub-Domain	<i>If necessary</i>		
Contact information of person submitting/managing the use-case	Shahar Steiff E-mail address: ssteiff@pccwglobal.com Telephone number:+85263888875 Social media: Web site: www.pccwglobal.com	AVP New Technology			
Proposing Organization	PCCW Global Limited. Hong Kong				
Short Description	PoC conducted at MEF18 event that demonstrated Automatic Discovery, Quote, Ordering and Settlement in a Mesh of Interconnected ICT Service Providers resulting in a significant decrease in time compared to legacy manual processes.				
Long description	<p>On October 2018 a team of 7 Carriers (PCCW Global, Infonas, Liquid Telecom, Singtel, Sparkle, and Tata Communications) together with two technology partners (Cataworx and Clear Blockchain Technologies) has presented a PoC where the process of obtaining a quote, ordering of a service, invoicing for such service, invoice reconciliation and final settlement for service delivered through a partial mesh of interconnected carrier networks were conducted through an automated system.</p> <p>Each carrier network was operating a catalogue of available services and upon receiving an inquiry from its customer through an eNNI it would search the catalogue for a matching entry and return a price if found. If no matching entry was found, the catalogue would then initiate an inquiry to its neighbour eNNI connected carriers that will then repeat this process until a matching entry is found in one of the catalogues (or until a pre-defined threshold has been reached, either time, or number of hops). If a price is returned by an downstream catalogue, the originating catalogue would then mark the price up according to defined commercial rules, and provide a quote to the upstream catalogue. This cascade of inquiries and quotes eventually provides the ultimate customer a quote for an end-to-end service that may span across multiple carrier networks.</p> <p>Once the ultimate customer places an order – a cascade of orders is placed downstream with all participating carriers.</p>				

	<p>Once service is terminated – invoices are being generated by each carrier based on their measured utilization (a combination of time, throughput and SLA metrics) and is then being reconciled with the measurement of the neighbour eNNI carriers.</p> <p>Once reconciliation is complete – the invoices are settled.</p> <p>The above proceeds, when handled manually on Carriers' legacy OSS/BSS platforms, may take weeks to complete.</p> <p>The PoC has demonstrated that the inquiry, quote and ordering take less than 30 seconds, and invoicing and reconciliation takes less than two minutes.</p> <p>This may result in a significant reduction in both time and HR, as not only that the process is accelerated, it is also automated.</p> <p>The information is exchanged through private permissioned ledgers between each pair of carriers and this is a flat-hierarchy architecture with no top-level orchestrator. Reflecting the commercial environment of the wholesale ICT market. There is complete isolation of information and visibility and no one has end-to-end visibility and control.</p>		
SDG in Focus (when applicable)	Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation		
Value Transfer:	The solution includes financial settlement between each pair of entities.	Number of Users:	Millions
Types of Users:	<p>End users: Private, Enterprise and Wholesale ICT SPs.</p> <p>ICT SPs: Connectivity SPs (carriers), Compute and Storage SPs (Public and Private Cloud).</p>		
Stakeholders	<p>End users: Ability to buy on-demand services. Ability to pay per-use.</p> <p>ICT SPs: Ability to deliver on-demand services and Yield new revenue from existing infrastructure.</p> <p>IoT SPs: Ability to use managed-services on-demand.</p>		
Data:	<p>Inquiry details, Quote details, Order details, Utilization records, SLA performance, Invoice details, Settled amount.</p> <p>The respective data models are service-type specific (connectivity DM differs from Compute DM that differs from Storage DM). The information is shared between the two eNNI partners only.</p> <p>Catalogue interaction will be through an API.</p> <p>End user interaction is expected to be through an intent-based interface.</p>		
Identification:	<p>This is a permissioned ledger. Only pre-accepted members can participate. Governance is managed through a board consisting of representatives of members of the ledger.</p>		
Predicted Outcomes:	<p>As demonstrated in the PoC – Manual processes replaced by automation significantly accelerate enabling a host of new applications that are currently dependent on best-effort, unmanaged, resources.</p>		

Overview of the Business Problem or Opportunity

Problem:

Most ICT services traverse more than one network domain. Each such network domain (a carrier network, a data centre, a radio link, an enterprise LAN) is typically operated by a different administration and is using different methods to transport, process and manage the flows of information.

It is very seldom that all administrations along the information flow path use a common language/process to define and manage their portion of the end to end path. Furthermore – it is very seldom that true end-to-end visibility and management is available across all administrations.

The typical process-flow is such that each two consecutive administrations along the end-to-end path have bilateral commercial and operational relations with each other that have overcome some of the differences in language/process. These relations are heavily dependent on manual processing of requests, manual provisioning of services, manual management, semi-manual invoicing and manual settlement. Such manual laden process-flow is time consuming and does not allow services to be activated on-demand but rather requires orders to be placed in advance, then be subject to delivery lead-times of weeks or months. For services that span across multiple administrations – the problem is further amplified as the service-related information now flows through a cascade/chain of bilateral agreements. Timelines stretch even further and management of the end to end service characteristics becomes very difficult.

Today's applications require resources to become available within minutes/seconds. Waiting months before establishing a video connection is not an option. While compute and storage resources are already available for on-demand consumption, and can be made ready for use within minutes or even seconds of notice, managed connectivity between the user and the compute/storage resources cannot be delivered instantly due to the reasons stated above. As a result – if managed connectivity was not made available in advance, the applications resort to the use of the public internet, which on one hand offers always-on any-to-any connectivity, but on the other hand offers no effective measures to manage the connectivity and guarantee performance.

Opportunity:

If we were able to guarantee quality of the end-to-end service, through management of each individual segment in the overall path, we could create an eco-system where all parties involved could benefit: The user will experience better quality services for which they will be willing (or forced) to pay. The ICT service providers will be able to charge for the use of their segments, provided that they manage and guarantee the quality and performance of their respective segment.

Why Distributed Ledger Technology?

ICT SPs operate in an equal-level playing field. There is no top-level administration that controls other administrations. Each ICT SP (administration) manages its own platforms as a “silo” using its own management system. No one will be willing to allow other administrations to administer their resources and services.

This creates a challenge when it comes to managing information flows across a chain of distributed administrations that have no hierarchy. That is where blockchain can play a role as a trusted mechanism to convey and manage information in a distributed environment. The fact that the information is owned by everyone and all nodes are at an equal hierarchical level makes it possible for administrations to exchange information related to services, and blockchain can then ensure integrity of the information across those multiple administrations.

The PoC has demonstrated how Quote, Order, Invoice, Reconciliation and Settlement information is exchanged across a chain of ICT SPs with timelines down to seconds on a per-pair of SPs basis, and minutes on a multi-SP environment.

Section 2: Current process

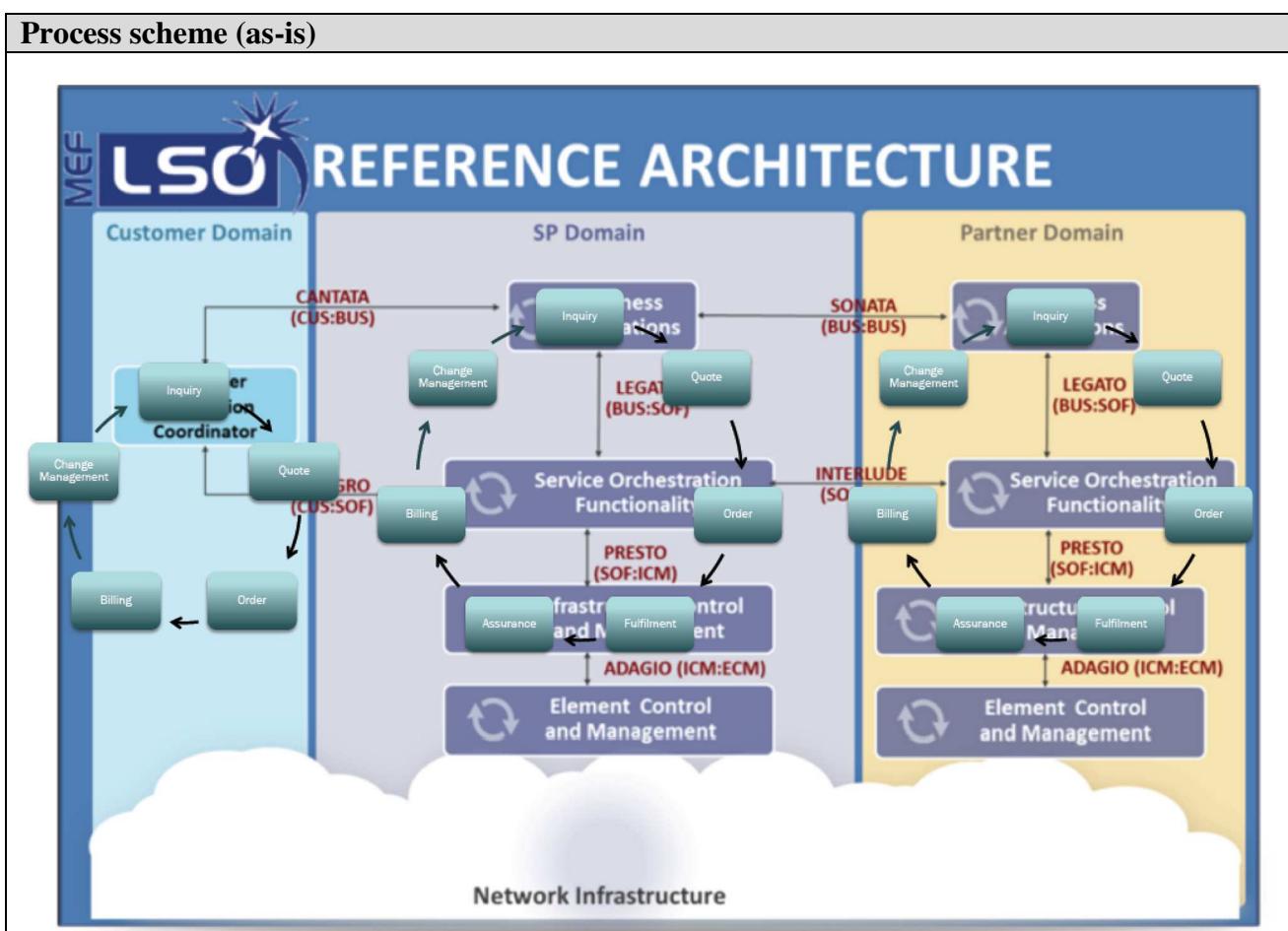
Current Solutions

Today there is no system offering end-to-end automation. There are automation platforms in existence that automate some (or all) of the lifecycle of services within a single administration, but each is confined to the limits of its own administration.

Existing Flow (as-is)

Step	User Actions	System (administration) Actions
1.	Make an Inquiry with an administration about availability and cost of a certain Service. User may send the same inquiry to multiple potential supplier administrations.	Manual processing of request. Analysis of the elements. Design a solution. Obtain cost of the solution-elements, including on-net (offered within the administration) and off-net (obtained from other administrations). Off-net inquiries trigger the same process with the downstream administration which may trigger additional processes with additional downstream administrations. The end result is that (if a solution is found and available) a Quote is returned to the User. This quote may include off-net quotes obtained from downstream administrations and may include mark-up of such quotes.
2.	Place an Order with the supplier administration.	Receive Order, send on-net elements of the order to provisioning, place order(s) for off-net elements with other administration(s). Those orders, once received by those other administration(s) may trigger additional orders with additional downstream administrations. Once the service has been provisioned and tested end to end it is handed-over to the user.
3.	Pay invoice on pre-agreed intervals (excluding SLA remedies)	Generate invoice on pre-agreed intervals based on agreement. Deduct SLA remedies if applicable. Pay invoices received from downstream administrations.

Existing Flow (as-is)		
Step	User Actions	System (administration) Actions
4.	Request termination of service from supplier administration (may be subject to term commitments).	Receive request for termination. Terminate on-net elements of service. Send termination requests to downstream suppliers for the off-net elements of service. The downstream supplier may then send termination requests to additional downstream suppliers. Off-net termination requests are subject to term commitments which do not necessarily correspond to the term commitment for the service ordered by the User.



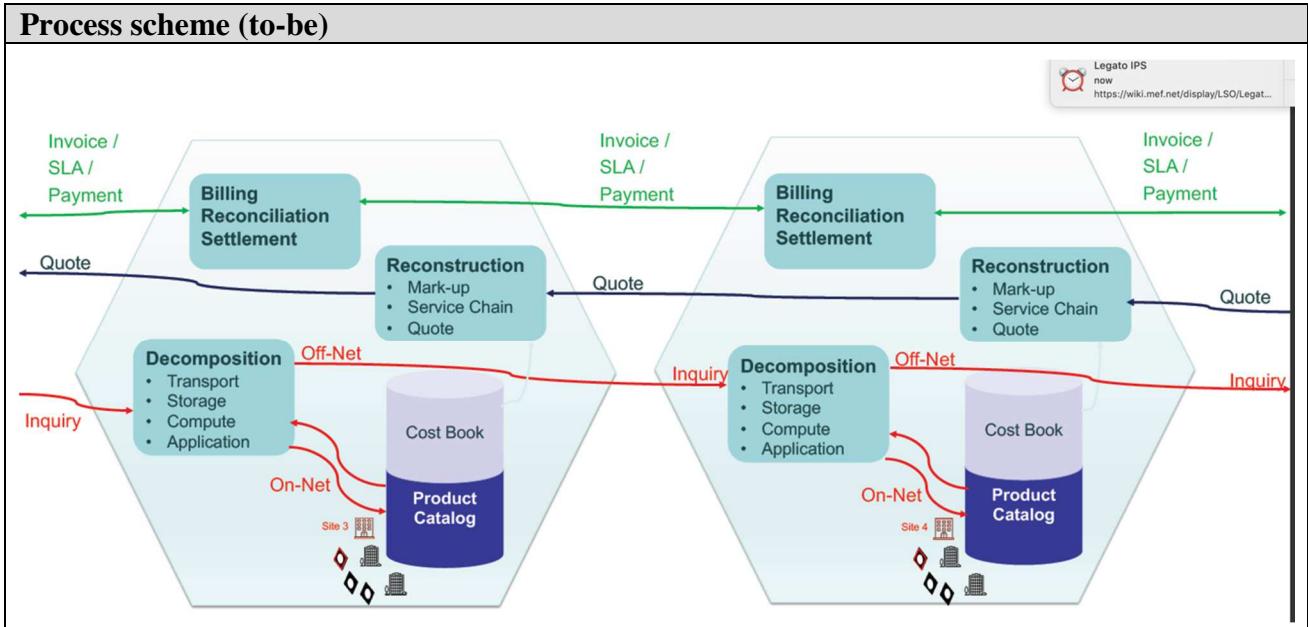
Data and information (as-is)		
Data	Type	Description
1	Documents	Cost books (Excel, PDF, on-line). Order forms (Excel, Fax, on-line). Invoices (PDF, on-line). Solution diagrams (Visio, PPT). Inventory management (on-line, Excel)
2	Payment transactions	Manual processing of invoices (that are generated automatically or semi-automatically)

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Users</i>	An individual, and SME, a large enterprise, a Telecom carrier, Governments, Universities and any other entity that may buy ICT services from Administrations that supply ICT services.
2	<i>Administrations</i>	Entities that provide and sell ICT services.

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.a	Request a Quote for on-demand (Immediate or Delayed activation. No term commitment) using a portal	Automatic parsing of the requirement (possibly using an intent-based parser). Automatic quoting of on-net elements based on a product/service catalogue. Automatic request of a quote for off-net elements from downstream administrations. Return quote to user if end-to-end solution is found.
1.b	Activate an app based on a pre-existing rate schedule for on-demand services without term commitments.	Detect activation of app and initiate activation of services to support the app. Request activation of off-net elements from downstream administrations.
2.a	Request Activation of service based on Quote received.	Initiate activation of services to support the order. Request activation of off-net elements from downstream administrations.
2.b	(n/a)	
3.a	Request termination of service	Automatically terminate service and send termination requests to downstream administrations. Initiate invoicing for service based on commercial terms and measured usage (time, volume, bandwidth, distance etc.)
3.b	Close app	Automatically turn down the services that supported the app. send termination requests to downstream administrations. Initiate invoicing for service based on commercial terms and measured usage (time, volume, bandwidth, distance etc.)
4.	Pay invoice	Receive payment



Participants and their roles		
Actor	Type/Role	Description
1	<i>Users</i>	An individual, and SME, a large enterprise, a Telecom carrier, Governments, Universities and any other entity that may buy ICT services from Administrations that supply ICT services.
2	<i>Administrations</i>	Entities that provide and sell ICT services.

Data and information		
Data	Type	Description
1	<i>Documents</i>	On-net Catalogues, electronic quotes, electronic orders, SLA
2	<i>Payment transactions</i>	Blockchain based (may use crypto currency or FIAT currency)

Security and privacy		
1.	Based on a Permissioned ledger.	
2.	Each pair of administrations runs a bilateral blockchain session.	
3.	Shared ledger used for failover, ZKP and reputation	

Main Success Scenario + expected time line		
PoC successfully presented at MEF18 event in October 2018.		
On-going standardization work initiated at MEF.		

Conditions (pre- or post-)		
1.	Requires agreement of all involved parties on common Service definitions, Common Information and Data models and a common Process.	

2. Plenty of Standardization work is still ahead of us.

Performance needs

The solution is based on off-the-shelf servers such as those offered by public cloud providers.

Legal considerations

This is automation of an existing process so there are no legal complexities that have not already been solved.

Governance of the code, ledger membership and IP rights requires agreement between participating administrations.

Risks

Not that I can think of.

Special Requirements

See “Conditions” above

External References and Miscellaneous

MEF 6.2, MEF 7.4, MEF MCM, MEF 50.1, MEF 55, ONF TAPI

Other Notes

Wholesale Voice Settlement

Section 1 Summary

Use Case summary			
Use Case ID:	ICT-003	Use Case Type:	Vertical
Use Case Title:	Wholesale Voice Settlement	Domain:	IT & Telco; Finance
Stakeholder:	Wholesale voice carriers		
Value Transfer:	Money transfer	N. of participants:	1000+
Data:	Carrier identities, commercial relationships, their terms, and settlement results are stored in DLT, some encrypted or hashed. CDRs (Call Detail Records/Call logs), settlement process are stored outside DLT but can be referenced by DLT		
Users:	Wholesale carriers		
Identification:	Carriers are identified, however the peers of a specific bilateral relationship are not necessarily specifically known, only their membership in the global carrier group is known. Some information about the voice call supply chain may be shared.		
Predicted Outcomes:	Implementation of global DLT system will automate existing manual processes and consolidate (currently disperse) systems, thus streamlining, increasing efficiency and reducing costs. It will also reduce human errors and time spent resolving disputes, further improving efficiency. Through transparency and short turnaround - fraud may be reduced and dissolved.		

Overview of the Business Problem or Opportunity	
Though the underlying systems involved in bilateral wholesale voice trade are mostly automated, some of the handoff of information from one system to another is not yet fully automated, and the settlement and dispute resolution are handled mostly through a labour intensive manual process. Through DLT technology, certain elements of this process may be streamlined and automated.	
Why Distributed Ledger Technology?	
The commercial interactions between carriers are carried out in an environment of mutual suspicion. Settlement between disparate systems operated by mutually-suspecting commercial entities requires either a trusted, neutral (but paid for), third party, or a lengthy laborious bilateral manual process to resolve commercial disputes and reach settlement.	
Certain bilateral processes, primarily in the mobile communications sector, use a centralized party to resolve disputes and reach settlement. However – the charges levied by such centralized parties amount to a significant (and growing) part of the ever thinning margins of the wholesale mobile business. The margins in the wholesale voice business are even thinner than those in the wholesale mobile business, rendering a paid-for centralized entity a non-viable solution.	
In addition to that – the current wholesale voice business process involves multiple disparate functions, each performed by a disparate system, that still require sequential treatment of data and feeding the output of one system to the next system in the sequence (e.g. CDR collection on voice	

switch fed to rating engine that feeds the invoicing systems that leads to manual dispute-resolution that eventually leads to settlement).

A DLT solution may be used for multiple purposes:

1. Create a common interchange and enforcement mechanism without a trusted third party.
2. Integration of the functionality of multiple disparate systems into a single system that performs a streamlined process that rates the CDRs, compares with the bilateral carrier, identifies and resolves disputes, then settles the account.
3. Settlement can be handled through automated FIAT currency transactions by APIs to Banks' swift clearing systems, through automated DLT transactions of electronic versions of FIAT currencies, or through crypto-currency transactions using either an existing cryptocurrency or one that will be created for the purpose of wholesale telecommunications settlements.

Section 2 Current process

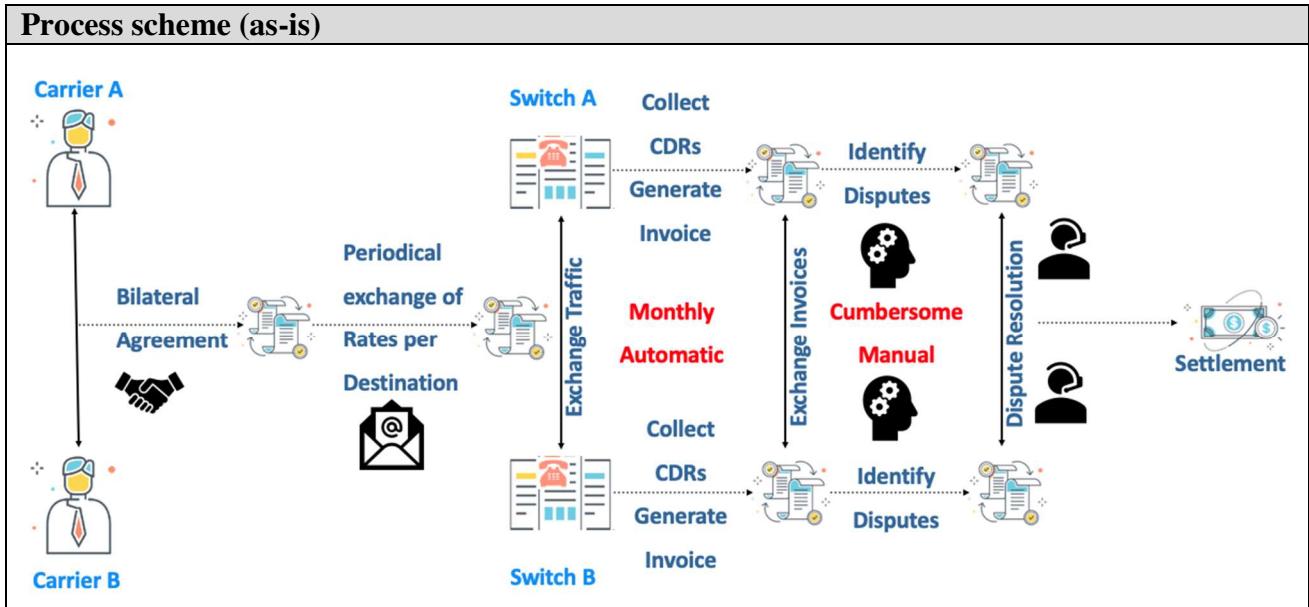
Current Solutions

Carriers have rating systems which perform automated analysis of CDRs, and automatically generate invoices. Such invoices are only seldom accepted by the recipient carrier and are often disputed. Disputed invoices then undergo a manual dispute resolution process during which both carriers negotiate, try to identify the reasons for the disputes and then reach settlement. It is not uncommon to see such negotiations stretch over months and at times both parties end up in court.

It is estimated that the wholesale voice industry as a whole is spending an order of magnitude of the equivalent of 10 years of HR every month resolving disputes.

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Telephone call is made	CDR is collected and stored (Automatic)
2.	(periodical, typically monthly)	All collected CDRs are rated based on comparison of the destination of the call with the agreed upon rate to that destination, and multiplication of the rate by the duration of the call, taking into account agreed upon rounding of duration (typically on a 1 second or 5 second basis). (Automatic) CDRs are being separated to inbound (for which the carrier is expecting to be paid by the bilateral carrier) and outbound (which the carrier expects to be invoiced for by the bilateral carrier). (Automatic)

Existing Flow (as-is)		
Step	User Actions	System Actions
3.	(periodical, typically monthly)	All rated inbound CDRs are collected and summed up. An invoice is generated for the sum of all rated CDRs and sent to the bilateral carrier. (Automatic) All rated outbound CDRs are collected and summed up but no invoice is generated. The sum of those rated CDRs is the amount the carrier is expecting to be invoiced for by the bilateral carrier. (Automatic)
4.	(periodical, typically monthly)	Invoices are exchanged between the bilateral carriers. (Automatic or semi-auto).
5.	An invoice from a bilateral carrier is received.	Compare the invoice received with the amount the carrier is expecting to be invoiced for (as calculated in step 3 above) and identify differences, if any exist. (Manual)
6.	If disputes are found	Negotiate with bilateral carrier. Try to identify the reason for the dispute. Agree which carrier made the error that caused the dispute. Re-calculate the invoice amount after correcting the error and repeat step 5 above. (Manual)
7.	Disputes have been resolved or no disputes	Settle the outstanding undisputed invoices. (Manual)



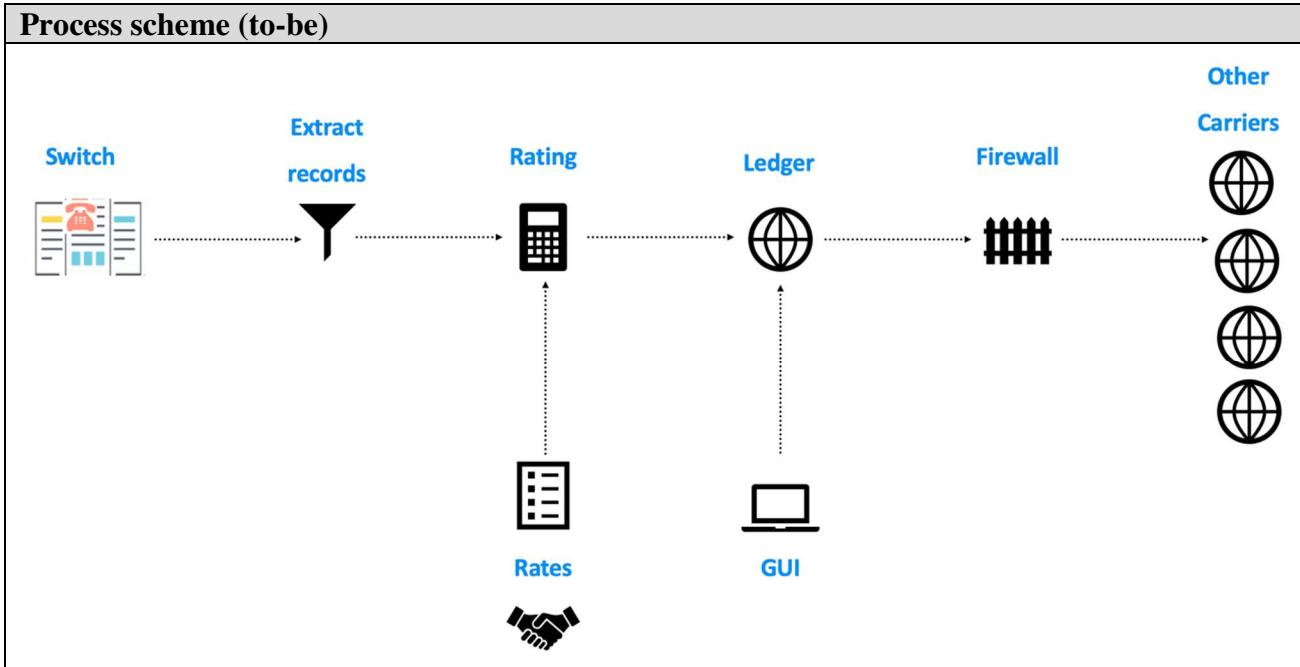
Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	<p>MSA (Master Service Agreement) or T+C (Terms and Conditions). Defines the rules of engagement, credit and payment terms, dispute resolution methods, rating methods, governing law.</p> <p>CDR – Call Detail Record. Includes information of the originating telephone number, the destination telephone number, the identity of the carrier sending the call, the identity of the carrier receiving the call, call start time, call end time (or call duration), result of call (success, fail, RNA [Ring No Answer]).</p> <p>Rate-Sheet. Periodically exchanged between bilateral carriers and defining the rate-per-minute of voice traffic sent to certain destinations.</p> <p>Rated-CDR. Excludes information of source and destination telephone numbers. Includes the commercial value of the call through multiplication of the call duration by the agreed upon rate appearing in the current bilateral rate sheet.</p>
2	<i>Payment transactions</i>	<p>Invoice. The sum of all rated CDRs for a period.</p> <p>Settlement. Payment of undisputed Invoices.</p>

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Originating Carrier</i>	The carrier sending voice traffic to another carrier.
2	<i>Recipient Carrier</i>	The carrier receiving voice traffic from another carrier.

Other Notes		
		In a bilateral relationship a carrier can be both an Originating Carrier and a Recipient Carrier.
		A Carrier can have relationships with multiple carriers.
		Tripartite relations may exist where two carriers agree to exchange traffic through a third, transit, carrier. In such case there may be separate agreements between the three carriers (Originating, Transit, Recipient).

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Telephone call is made	CDRs are collected and stored (Automatic)
2.	(periodical, PoC has proven that the period can be as short as 15 seconds)	All collected CDRs are rated based on comparison of the destination of the call with the agreed upon rate to that destination, and multiplication of the rate by the duration of the call, taking into account agreed upon rounding of duration (typically on a 1 second or 5 second basis). (Automatic) CDRs are being separated to inbound (for which the carrier is expecting to be paid by the bilateral carrier) and outbound (which the carrier expects to be invoiced for by the bilateral carrier). (Automatic)
3.	(periodical, same frequency as above)	All rated inbound CDRs are collected and summed up. An invoice is generated for the sum of all rated CDRs and sent to the bilateral carrier using a bilateral DLT. (Automatic) All rated outbound CDRs are collected and summed up but no invoice is generated. The sum of those rated CDRs is the amount the carrier is expecting to be invoiced for by the bilateral carrier. (Automatic)
4.	An invoice from a bilateral carrier is received through DLT.	Compare the invoice received with the amount the carrier is expecting to be invoiced for (as calculated in step 3 above) and identify differences, if any exist. (Automatic)
5.	If disputes are found	Apply a dispute-resolution algorithm (described separately). (Automatic with certain exceptions)
6.	Disputes have been resolved or no disputes	Settle the outstanding undisputed invoices using DLT. (Automatic or Manual)



Participants and their roles		
Actor	Type/Role	Description
1	<i>Originating Carrier</i>	The carrier sending voice traffic to another carrier.
2	<i>Recipient Carrier</i>	The carrier receiving voice traffic from another carrier.
3	<i>Bank</i>	In certain scenarios DLT settlement may initiate an API call to a Bank's SWIFT service to perform FIAT currency payment.
4	<i>IMF (International Monetary Fund)</i>	In certain scenarios DLT settlement may take place using an electronic version of SDR (a currency defined by IMF).

Data and information		
Data	Type	Description
1	<i>Documents</i>	<p>MSA (Master Service Agreement) or T+C (Terms and Conditions). Defines the rules of engagement, credit and payment terms, dispute resolution methods, rating methods, governing law.</p> <p>CDR – Call Detail Record. Includes information of the originating telephone number, the destination telephone number, the identity of the carrier sending the call, the identity of the carrier receiving the call, call start time, call end time (or call duration), result of call (success, fail, RNA [Ring No Answer]).</p> <p>Rate-Sheet. Periodically exchanged between bilateral carriers and defining the rate-per-minute of voice traffic sent to certain destinations.</p> <p>Rated-CDR. Excludes information of source and destination telephone numbers. Includes the commercial value of the call through multiplication of the call duration by the agreed upon rate appearing in the current bilateral rate sheet.</p>
2	<i>Payment transactions</i>	<p>Invoice. The sum of all rated CDRs for a period exchanged thru DLT.</p> <p>Settlement. Payment of undisputed Invoices performed through DLT.</p>

Security and privacy
1. <i>The use case assumes a Permissioned Private DLT that uses PoA (Proof of Authority) with multiple signatures and DBFT consensus mechanism.</i>
2. <i>Access to the platform is only allowed to Carriers identified as such by other carriers and is administered by a SPV (Special Purpose Vehicle) that includes Carriers members of the DLT.</i>

Main Success Scenario
Interoperable private blockchains
<ul style="list-style-type: none"> <i>Between bilateral Carriers, using interoperable protocol.</i> <i>Bilateral transactions are carried out on a bilateral DLT (one per pair).</i>
Open-source shared blockchain
<ul style="list-style-type: none"> <i>Failover to Shared blockchain.</i> <i>Permissioned network using open-source Ethereum nodes.</i> <i>Also used for dispute resolution using ZKP for Transit traffic.</i>
Pluggable Commercial Logic and Ingestion
<ul style="list-style-type: none"> <i>Single shared network with variety of products and interactions</i> <i>Dispute resolution may use AI/Heuristics algorithms and can include failover to manual resolution based on criteria.</i>

- *Dispute resolution algorithms may differ on a partner-Carrier and destination basis.*

Conditions (pre- or post-)

1. *Participating Carrier must be accepted to the DLT platform based on criteria set forth by SPV.*
2. *Participating Carrier must provide a Dedicated or Virtual compute resource that meets the requirements set forth by SPV, either on-premise or in Cloud, and load the software provided by SPV on the compute resource.*

Performance needs

Based on estimated volume of traffic and number of bilateral connections the compute resources can be sized with accuracy. The PoC has proven that an off-the-shelf standard configuration VM in public clouds is sufficient for the task.

Legal considerations

1. *The PoC is implemented using existing legal contracts between Carriers.*
2. *The use of crypto-currency is an option that may be subject to certain legal restrictions in specific geographies,*

Risks

International Wholesale Voice trading (IDD) is a well-established business that has its roots in the days of national operators (PTTs), and although it has gone through deregulation in most countries, it is one of the most supervised and controlled environments in the telecom business. Automation of elements of this business, through use of DLT or without it, does not change the legal frameworks the IDD business is established upon.

The only exception to the above is the use of DLT to settle commercial transactions using Crypto-Currencies. Reason being that such transactions may be banned in some geographies due to local regulations. Said risk can be mitigated as Crypto-Currency is not a mandatory method for settlement, and as discussed above, settlement can also be executed through API based automated SWIFT bank transactions, through electronic versions of FIAT currencies or even manually as is done today.

Other risks may be related to acceptance of suspicious carriers to the DLT, who may try to perform fraudulent IDD transactions. This is an existing risk and the move to DLT-based automation will neither increase the risk itself, nor will it risk an increase in its occurrence. On the contrary – DLT-based automation will shorten the cycles by which fraudulent activity can be identified, thus reducing the exposure ion case of such activities. Add to that the reputation management that is embedded into DLT which will allow carriers to easily verify the reputation of a potential bilateral partner prior to establishing a business relation.

Special Requirements

The PoC has demonstrated that no special requirements exist. Considering a full-scale system – the compute resources and data transport resources required for proper functionality of the system are within what is currently available off-the-shelf as public-cloud based VMs or commercially and publicly available blades and servers to be installed in a private cloud or a data centre. Connectivity wise – the PoC has demonstrated that a 1Gbps link should suffice to carry the entire global CDR exchange between carriers using DLT.

External References and Miscellaneous

Other Notes

Appendix 1

Domains 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 and logistic
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

Horizontal:

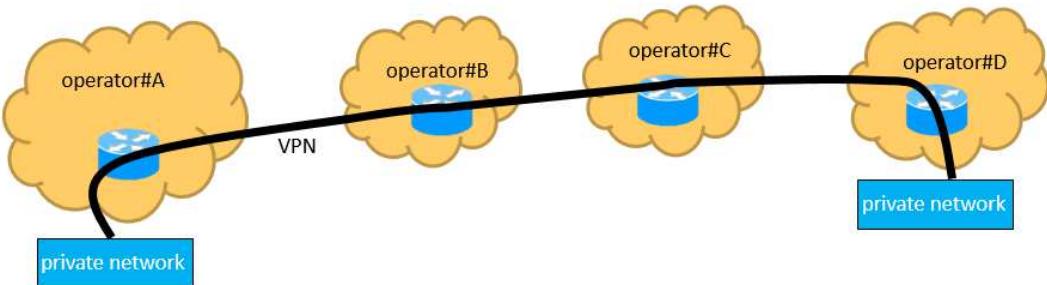
1. Identity Management
 2. Security Management
 - a. Public Key Infrastructure
 3. Internet of Things
 4. Data storage (Inter-organizational data management)
-

Distributed Ledger based Online Trading System for Cross-domain VPN Provision

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-004	Use Case Type:	Vertical
Use Case Title:	Distributed Ledger based Online Trading System for Cross-domain VPN Provision	Is Use Case supporting SDGs	Yes
Status of Case	Proof-of-Concept	Domain:	Industries
Contact information of person submitting/managing the use-case	<i>Xinpeng Wei</i> <i>Bingyang Liu</i>	wexinpeng@huawei.com liubingyang@huawei.com	
Proposing Organization	Huawei		
Short Description	This use case is a proposal for utilizing DLT-based online trading system for cross-domain VPN (Virtual Private Network) provision services, which enables a customer to purchase cross-domain VPN service on-demand and flexibly.		
Long description	<p>A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Usually the VPN connection will cross one or more networks operated by different operators, and the operators should have SLAs between each other to setup of end-to-end VPN connection for customers, the process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will be maintained for a very long time, so the time taken for VPN setup is acceptable.</p> <p>But as the new cases that VPN should be setup in a more flexible and on-demand way, the existing solution for VPN setup is no longer acceptable, because it is usually unknown which operator's network to traverse and whether the en-route operators have SLAs between each other.</p> <p>This document provides a use case that DLT is used for on-demand VPN connection setup across different domains.</p>		
SDG in Focus (when applicable)	Goal 9: Industry, Innovation and Infrastructure 9.3 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:	Token which is used to pay for VPN service.	Number of Users:	thousands
Types of Users:	enterprise, residential customer network, network operator		
Stakeholders	enterprise, residential customer network, network operator		
Data:	1. The data that VPN user sends to network operator for VPN provision. 2. The Service Level Agreement signed between different network operators.		
Identification:	Full identification of each entity is required.		
Predicted Outcomes:	1. Minimize time to negotiate VPN provision process. 2. Eliminate the need of pre-sign SLAs between customer and service providers.		

Overview of the Business Problem or Opportunity	
<p>Currently in order to establish VPN connection across more than one operators' network, because the QoS of VPN connection needs to be provided along the whole connection path, so operators should have SLAs between each other and each operator makes its own provisions for the VPN connection. The process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will maintained for a very long time, so the time taken for VPN setup is acceptable.</p>	
	
<p>Figure 1: VPN connection across different operators' network</p> <p>But for the new use case of on-demand VPN connection, the existing solution is hard to satisfy the requirements for the following reasons:</p> <ol style="list-style-type: none"> 1. The on-demand VPN is very dynamic, and it is hard to predict with network it will traverse. 2. The on-demand VPN could only exist for a short time, e.g. only a few days, so the time cost of establishing such as connection should be low enough. 	
Why Distributed Ledger Technology?	
<p>DLT is to build a trust infrastructure, which helps the private network to set up trust relationship with the network providers for establishing VPN connection, and enables fast on-line trading between them to realize automatic VPN provision.</p>	

Section 2 Current process

Current Solutions

The current solution depends on the operators' SLA pre-signed with each other.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	The VPN user (owner of private network) sends out a request to the operator it directly connected to establish VPN connection between private networks.	N/A
2.	The network operator provision its own network devices to provide VPN connection and ask for the next network operator to provide VPN connection in its network according to SLA, and so on until the end-to-end VPN is fully provisioned.	N/A

Process scheme (as-is)

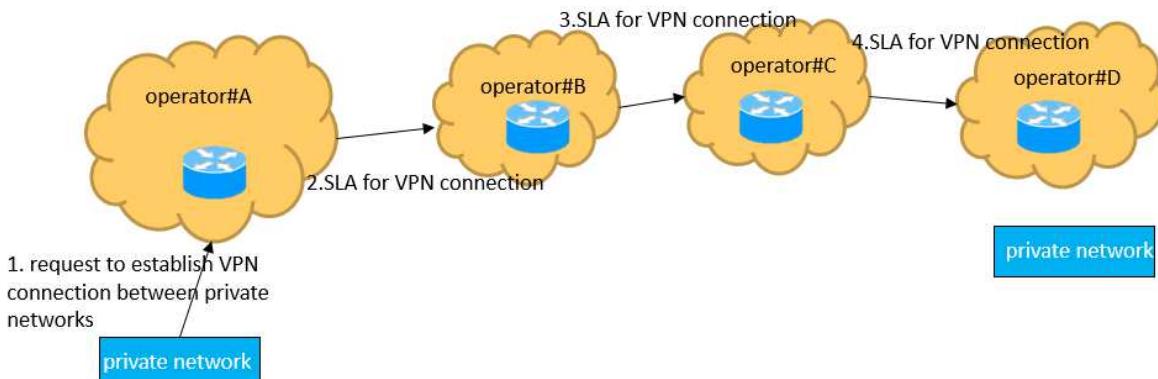


Figure 2: VPN provision procedure

Data and information (as-is)

Data	Type	Description
1	VPN provision request	The data that VPN user sends to network operator for VPN provision.
2	SLA	The Service Level Agreement signed between different network operators.

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	VPN user	The entity who wants to establish VPN connection.
2	Network operator	The entity who operates the network.

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	VPN user gets en-route networks' information between private networks.	Ledger records networks' information about the VPN service they can provide.
2.	VPN user sends request to network operator's smart contract to establish VPN connection between private networks. The VPN configuration-related parameters will be included in the request.	Ledger checks the VPN user is authorized to send out the transaction, and the target network operator's smart contract exist. If true, DLT record the transaction.
3	Network operator gets VPN configuration-related parameters from the ledger.	Ledger provides VPN configuration-related parameters information to network operator.
4	Network operator acknowledges VPN service.	Ledger records network operator's transaction for VPN service acknowledge.

Process scheme (to-be)

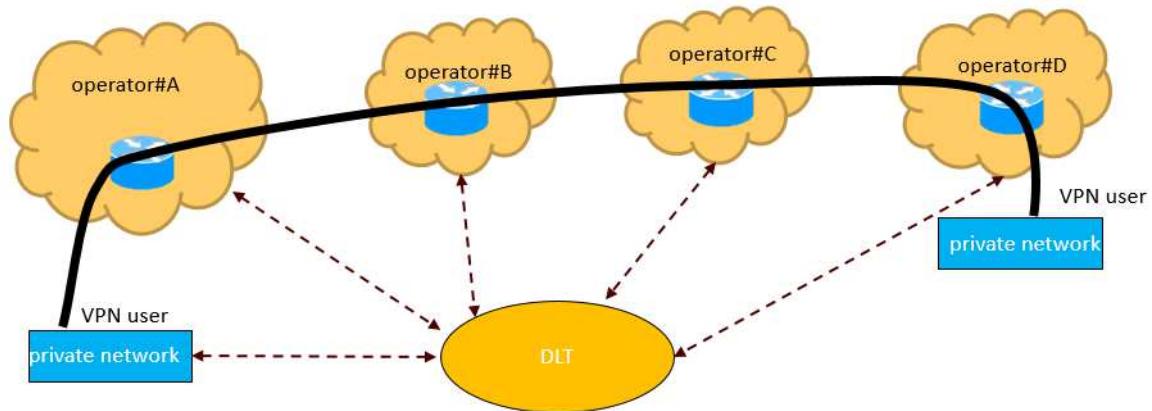


Figure 3: Overview of DLT and VPN Provision System

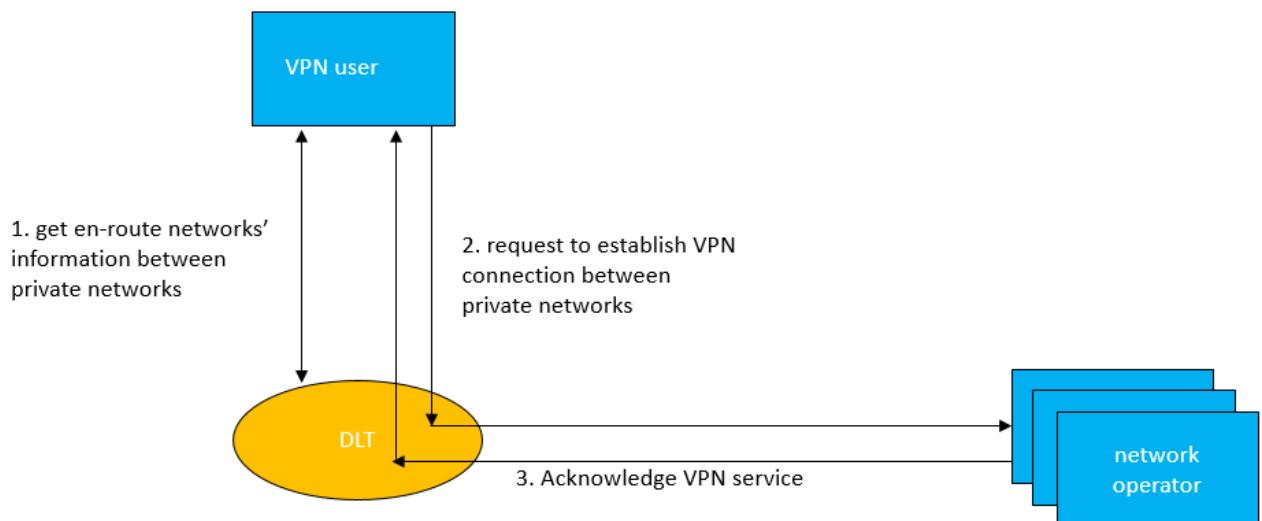


Figure 4: Procedures of VPN Provision Service

Participants and their roles

Actor	Type/Role	Description
1	VPN user	The entity who wants to establish VPN connection.
2	Network operator	The entity who operates the network.

Data and information

Data	Type	Description
1	Token account	Token representing money value. It is used to transfer value between VPN users and network operator.

Data and information		
Data	Type	Description
2	Service request transactions	The VPN users use service request transaction to ask for VPN provision service from network operators, and payment for the service will also be included.
3	VPN service information	The information is maintained at the smart contract in ledger, it includes the SLA that the network operator can provide for VPN provision.
4	Network-related information	Each network provides its own network information to the Ledger, this information is used by VPN users to figure out the en-route networks that the VPN connection will traverse.
5	VPN configuration-related parameters	These parameters are used to configure VPN connection properly, the VPN user decide these parameters and the Ledger will record these parameters.
6	VPN service acknowledge transaction	This transaction is used by network operator to accept the VPN provision request from VPN user.

Security and privacy
1. The network operator's service information recorded in DLT system should be trustable.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode.
2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way.
2. All parties are connected to DLT system.
3. All parties should have a recognizable identity.

Performance needs
1. Transactions processing near real time;
2. 24/7/365 availability;
3. Volume of transactions > 1000 TPS.

Legal considerations
N/A

Risks

1. DLT-related security risk.

Special Requirements

N/A

External References and Miscellaneous

N/A

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)

Distributed Ledger based Online Trading System for DDoS Mitigation Services

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-005	Use Case Type:	Vertical
Use Case Title:	Distributed Ledger based Online Trading System for DDoS Mitigation Services	Is Use Case supporting SDGs	Yes
		Domain:	Industries
Status of Case	Proof-of-Concept	Sub-Domain	IT and telco
Contact information of person submitting/managing the use-case	<i>Xinpeng Wei</i> <i>Bingyang Liu</i>	<u>wexinpeng@huawei.com</u> <u>liubingyang@huawei.com</u>	
Proposing Organization	Huawei		
Short Description	This use case is a proposal for utilizing DLT-based online trading system for DDoS mitigation services, which enables a victim network to on-demand purchase DDoS mitigation services close to the attack sources.		
Long description	This use case describes how DLT is used in DDoS mitigation service. Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS mitigation service aims at mitigating DDoS attacks for the victim network. By using DLT, it's much easier to mitigate attack at the point of attack sources, and prevents the attack traffic from consuming bandwidth resources of the intermediate networks.		
SDG in Focus (when applicable)	Goal 9: Industry, Innovation and Infrastructure 9.3 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:	Tokens which is used to pay for DDoS Mitigation service	Number of Users:	thousands
Types of Users:	Network operators, OTT (Over The Top), Internet users, enterprise, residential customer network		

Stakeholders	Network operators, OTT, Internet users, enterprise, residential customer network
Data:	<p>Token balance to each account.</p> <p>Service smart contract: Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim.</p> <p>Service smart contract include information about the service and price that DDoS mitigation service provider can provide.</p> <p>IP prefix-related information: The DLT records information about IP prefix and AS (Autonomous System) numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.</p>
Identification:	Full identification of each entity is required.
Predicted Outcomes:	<ol style="list-style-type: none"> Minimize time to negotiate DDoS mitigation service. Eliminate the need of pre-sign SLAs between customer and service providers.

Overview of the Business Problem or Opportunity	
<p>Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS can exhaust not only the resources of victim networks but also of the uplinks. Mitigation near attack sources is better than near attack targets, because it prevents the attack traffic from consuming bandwidth resources of the intermediate networks. Besides, the burden of DDoS mitigation is shared, so the required service capacity of single provider will not be so challenging.</p>	

Figure 1: Overview of DDoS Protection System

However, near-source DDoS mitigation requires a business model that the victim network to purchase mitigation services from multiple providers close to the multiple source networks, which can be any of the tens of thousands of autonomous systems (ASes). There are two challenges:

First, the victim network has to set up business relationship with the remote providers, who may be unknown to the victim;

Second, different attacks have different sources, and thus require setting up business relationship with different providers. Due to the challenges, existing mitigation services are typically provided closed to the victim networks.

Why Distributed Ledger Technology?

DLT is to build a trust infrastructure, which helps the victim network to set up trust relationship with the remote providers, and enables fast on-line trading between them to start DDoS mitigation as soon as possible.

Section 2 Current process

Current Solutions

In the current solution, victim network has to set up business relationship with the DDoS mitigation service providers, and when the DDoS attack happens, the victim network sends request to the specific DDoS mitigation service provider.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	DDoS victim pre-signes SLA with DDoS mitigation providers	N/A
2.	Request for DDoS mitigation service	N/A
3	Provide DDoS mitigation service based on request	N/A

Process scheme (as-is)

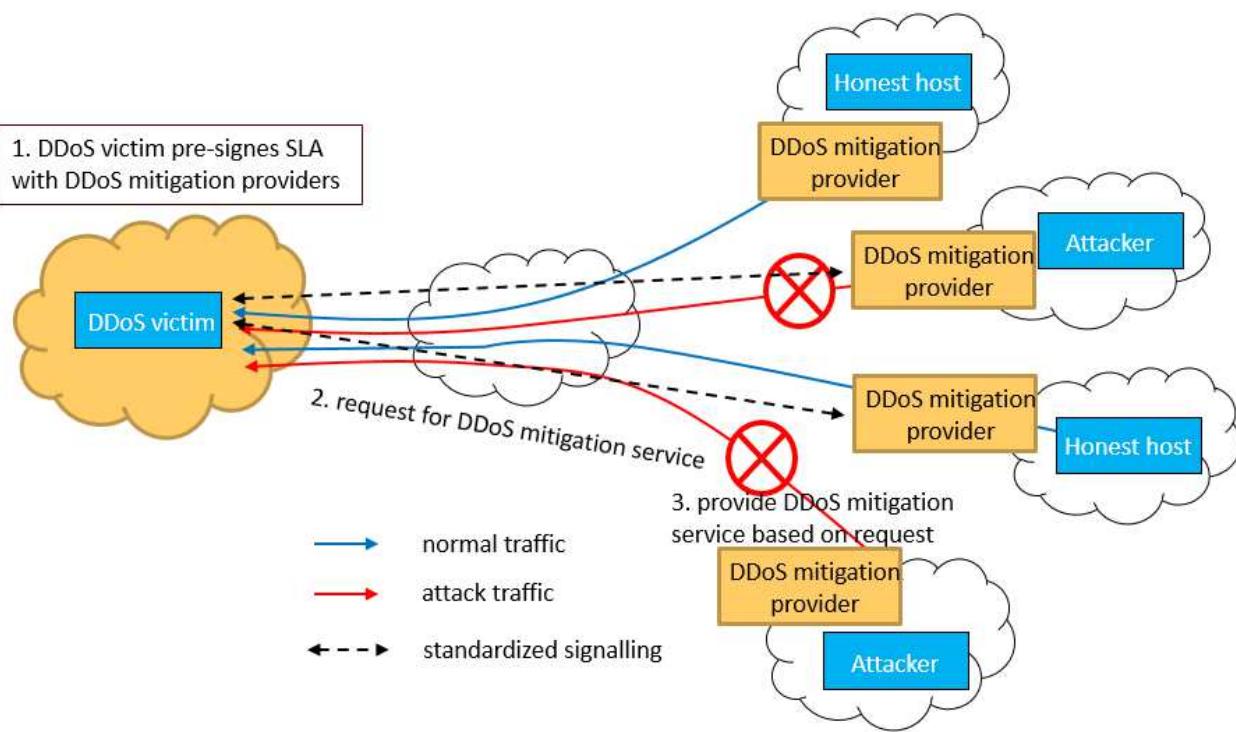


Figure 2: The Existing Distributed DDoS Mitigation Solution

Data and information (as-is)

Data	Type	Description
1	DDoS mitigation service request	The victim send this request to service provider for DDoS mitigation service.

Participants and their roles (as-is)

Actor	Type/Role	Description
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Other Notes

N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	DDoS victim initiates a transaction to DDoS mitigation provider's smart contract to request for DDoS mitigation service.	DLT checks the DDoS victim is authorized to send out the transaction, and the target DDoS mitigation provider's smart contract exist. If true, DLT record the transaction.
2.	DDoS mitigation provider evaluates DDoS victim's credibility verifying that the DDoS victim has the ownership of the attacked IP address.	N/A
3	DDoS mitigation provider initiates a transaction with the DDoS victim to agree to provide DDoS mitigation server.	DLT checks the transaction sent by DDoS mitigation provider is valid, and then record the transaction. After that the DDoS mitigation provider's smart contract will be executed, and token will be transferred from DDoS victim's account to DDoS mitigation provider's account.

Process scheme (to-be)

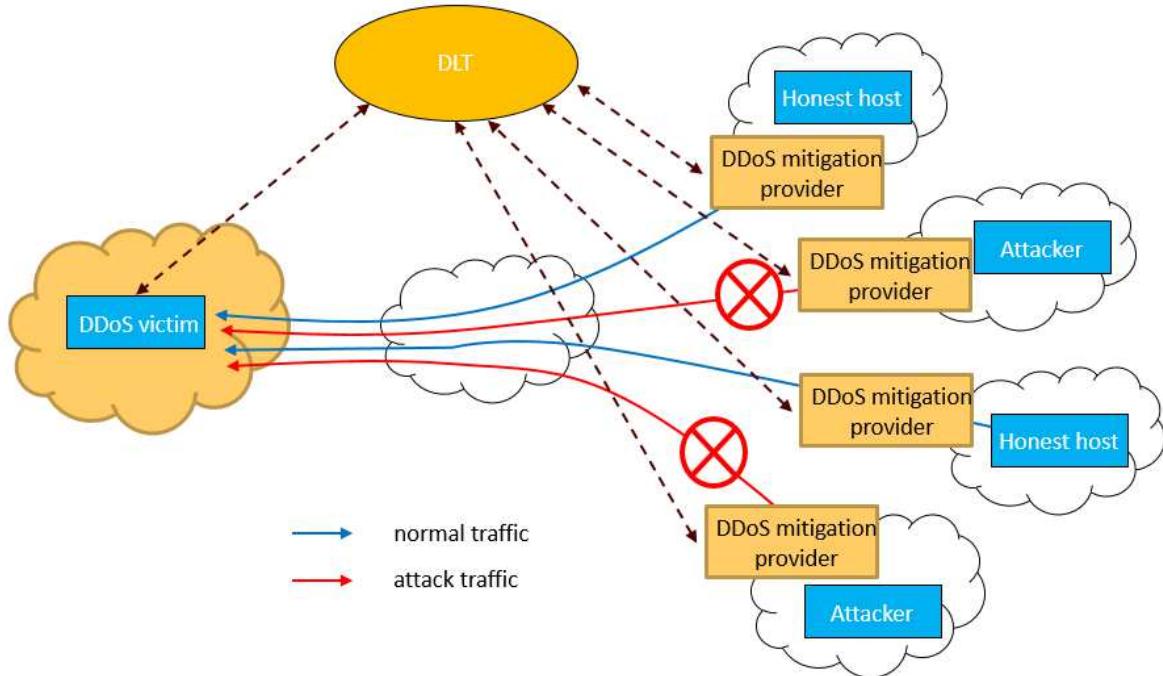


Figure 3: Overview of DLT and DDoS Mitigation System

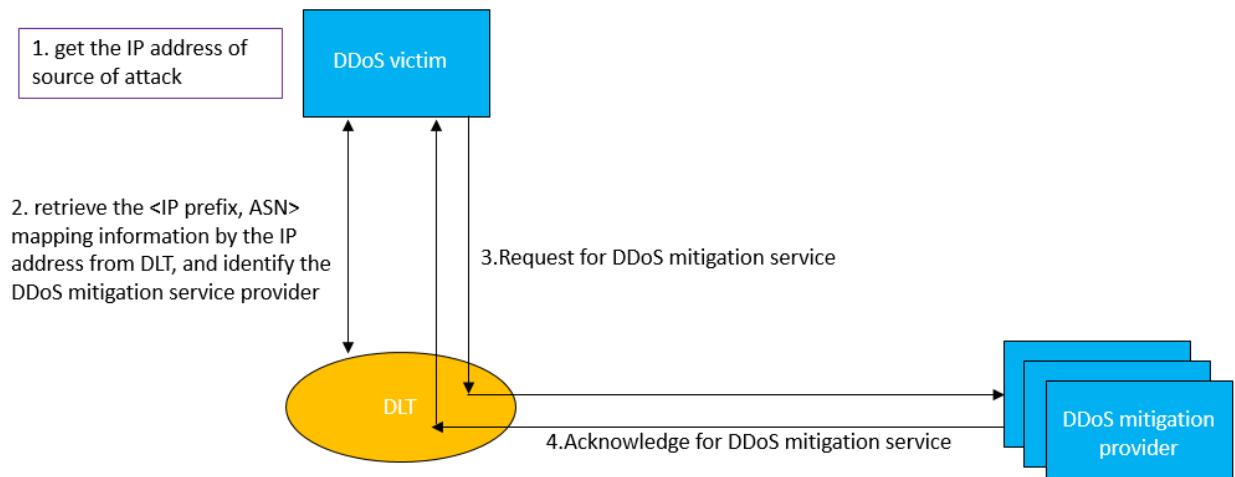


Figure 4: Procedures of DDoS Mitigation Service

Participants and their roles

Actor	Type/Role	Description
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.

Participants and their roles		
Actor	Type/Role	Description
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Data and information		
Data	Type	Description
1	token	Token representing money value. It is used to transfer value between DDoS victims and DDoS mitigation providers.
2	Service request transactions	The DDoS victim use service request transaction to ask for DDoS mitigation service from DDoS mitigation service provider, and payment for the service will also be included.
3	Service acknowledge transactions	The DDoS mitigation service provider use service acknowledge transaction to agree for DDoS mitigation service to DDoS victim.
4	Service smart contract	Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim. Service smart contract include information about the service and price that DDoS mitigation service provider can provide.
5	IP prefix-related information	The DLT records information about IP prefix and AS numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.

Security and privacy
1. The DDoS mitigation provider's service ability recorded in DLT system DDoS mitigation provider should be trustable.
2. The IP prefix-related information recorded in DLT system should be trustable.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode.
2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way.
2. All parties are connected to DLT system.
3. All parties should have a recognizable identity.

Performance needs

1. Transactions processing near real time;
2. 24/7/365 availability;
3. Volume of transactions > 1000 TPS.

Legal considerations

N/A

Risks

1. DLT-related security risk.

Special Requirements

N/A

External References and Miscellaneous

N/A

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)

VisionNG DLT for Number Assignment, Services and Number Portability

Section 1: Summary

Use Case summary			
Use Case ID:	ICT-006	Use Case Type:	Vertical
Use Case Title:	VisionNG DLT for number assignment, services and number portability	Domain:	Telecommunications
Stakeholder:			
Value Transfer:	Yes, currently not in use	N. of participants:	3
Data:	Contractual rules, chain of contracts, services type		
Users:	30000		
Identification:	You can participate anonymously only for specific services		
Predicted Outcomes:	Fast assignment, number and service portability with legacy fall back on DNSSec		

Overview of the Business Problem or Opportunity
Fast and scalable system for service and number portability
Why Distributed Ledger Technology?
There is no current solution for global number and service portability that provides fast cost effective and scalable technology that provides for global services deployment.

Section 2: Current process

Current Solutions
There are some parts available that provide some services like number resolution, but don't support any contractual system like number assignment or portability

Existing Flow (as-is)		
Step	User Actions	System Actions
1.	Manual interaction	Manual action via operator
2.		

Process scheme (as-is)
Single regions Sparse service

Data and information (as-is)		
Data	Type	Description
1	Documents	Manual, physical paper work
2	Payment transactions	Billing for services

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	Telecommunications operators	Provide numbering resources and services
2	Users	Request and receive resources and services from operators

Other Notes

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Interact with the system via contract backed by smart contracts	Issues keys, and store and executes smart contract roles, stores record and syncs with legacy systems
2.		

Process scheme (to-be)

Participants and their roles		
Actor	Type/Role	Description
1	Telecommunications operators	Make arrangements to enable keys to be issued, to store and execute smart contract roles, to store records and sync with legacy systems
2	Users	Interact with the system via contract backed by smart contracts

Data and information		
Data	Type	Description
1	Transactions	Assignments, reclamations, changes, etc.

Data and information

Data	Type	Description

Security and privacy

Entities are represented by cryptographic keys and specific smart contract are issued per region / service

Main Success Scenario

Number resource is available on Global Cloud DLT DApp platforms for global application and service delivery

Conditions (pre- or post-)

Performance needs

Current number portability solutions take days where semi distributed system like DNS take milliseconds

Legal considerations

Must comply with national regulatory requirements

Risks

Special Requirements

Implementing Number and services management platform to interact with the existent DLT systems

External References and Miscellaneous

Other Notes

Appendix 1

Domains for use cases categorization

Blockchain/DLT offers capabilities suitable for a wide variety of uses and purposes in many different domains and types of applications. There are 2 main types of DLT-based applications and services:

- Vertical applications and services (e.g., telco, fintech, supply chain, energy)
- Horizontal (infrastructural) applications and services (e.g., data usage control, identity management, security)

Vertical use cases could be categorized to domains according to the list below (note, that the list is not exhaustive):

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
3. Voting
4. Smart manufacturing
5. Intellectual property management (Digital rights management)
6. Supply chain and inventory management
7. Media
8. Energy
9. Government and public sector
 - a) Taxes
 - b) Government and non-profit transparency
 - c) Legislation, compliance & regulatory oversight
10. Real estate
11. Taxation and customs

Horizontal use cases could be categorized to domains according to the list below:

1. Identity Management
2. Cybersecurity
3. Big data

錯誤! 所指定的樣式的文字不存在文件中。

4. Data storage (Inter-organizational data management)
 5. IoT
-
-

Alastria ID

Section 1: Summary

Use Case Summary			
Use Case ID:	IDM-001	Use Case Type:	<i>Horizontal</i>
Submission Date:	January 4, 2019	Is Use Case supporting SDGs	<i>Yes</i>
Use Case Title:	Alastria ID	Domain:	<i>I</i>
Status of Case	<i>e.g., Concept, PoC, Pilot, Implementation</i>	Sub-Domain	<i>Not Applicable</i>
Contact information of person submitting/managing the use-case	<i>Full Name: Ismael Arribas Web site: https://alastria.io standards@alastria.io</i>		
Proposing Organization	“Consorcio Red Alastria” Association (Kingdom of Spain). G-87936159		
Short Description	Alastria can be summarized as an independent, public, permissioned and neutral Blockchain/DLT framework for networks.		
Long description	<p><i>Thanks to the diversity of its stakeholders and associates, Alastria has granted an infrastructure for Self-Sovereign Identity management. As a network it is duly authenticated in the Spanish market and European Union, however the partnership with LAC countries which is a fact of the SDG 17 scope for Alastria is the consequence for being a framework of networks. Alastria is the first multisectoral Association promoted by organizations and institutions for the establishment of a public Blockchain/DLT infrastructure, supporting services with legal effectiveness in the Spanish scope and according with the European regulation.</i></p> <p><i>The Consortium is open to any organization that wishes to have available a fundamental tool for the development of its own blockchain/DLT strategy with the aim of distributing and organizing products and services.</i></p>		
SDG in Focus (when applicable)	<i>SDG3, SDG4, SDG5, SDG6, SDG7, SDG8, SDG11, SDG 13, SDG16, SDG17.</i>		
Value Transfer:	We will transfer claims off-chain with on-chain proofs. Ponderation of attributes by causality. Verified authority to attest and authenticate an attribute.	Number of Users:	First PoC will happen in Spain (>45MM) but this solution aims to establish a global Identity system as an interplanetary badge. European Population and LAC.

Types of Users:	People, Organizations, Public Administration & Objects (IoT) and processes.
Stakeholders	<i>As we are proposing a Self-Sovereign Identity-based interconnected Blockchain Platform(s), with the right Governance, all type of users are also stakeholders</i>
Data:	https://github.com/alastria/alastria-identity/wiki <i>Privacy by design: unlinkable actions.</i>
Identification:	<i>Identification mechanism and rules; ability of participants to be anonymous, etc.</i> Non-interactive Zero-Knowledge Proof, in essence it refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information which needs to be kept confidential, and without any interaction between prover and verifier. https://snark.network/
Predicted Outcomes:	MAIN NET and various PoC with succeed in different verticals like Healthcare, Education, Energy, E-Money and others. eIDAS Bridge Pilot as a reference for the ESSIF (European Self Sovereign Identity Framework)

Overview of the Business Problem or Opportunity

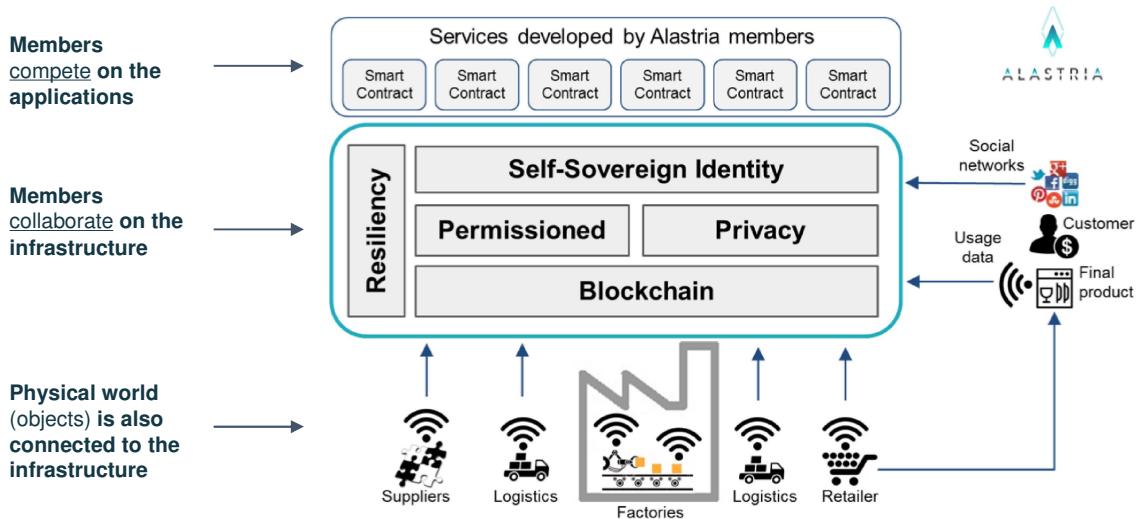
National Infrastructure Use Case Requires Special Efforts

Alastria works on consensus, governance and identity to comply with the strong requirements on legal compliancy, scalability, performance and trust

Public networks (Bitcoin, Ethereum)	Public Permissioned network	Private consortiums	Enterprise systems
Fully decentralized: everybody votes	Very decentralized (set of validators vote, with a “good enough” approach)	Vote only few	Vote only one
3 - 10 transactions/sec	High performance and scalability (>1.000 tx/sec)	High performance (100K tx/s)	
PoW algorithm, requiring incentives to miners	More efficient algorithm (Istanbul BFT)	More efficient algorithms, without mining	
High transaction costs, high volatility	Predictable, low transactional cost (no cryptocurrency embedded)	Low transaction costs, predictable	7

Why Distributed Ledger Technology?

A Shared National Infrastructure for public & private sectors



8

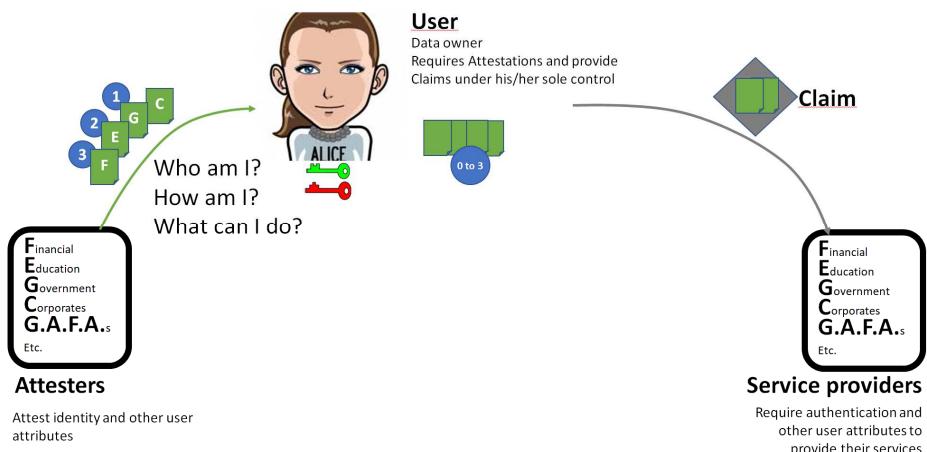
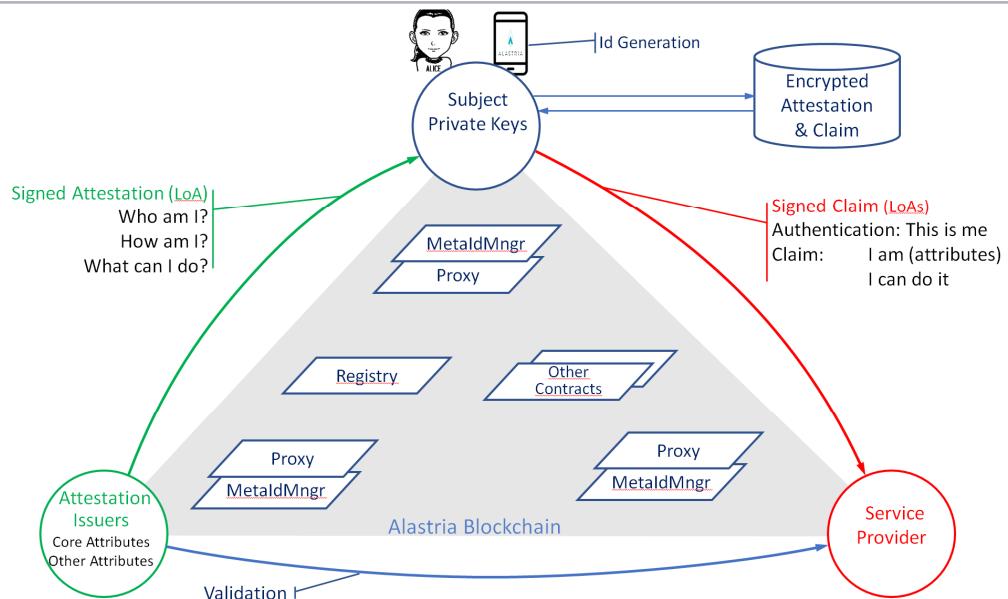
Section 2: Current process

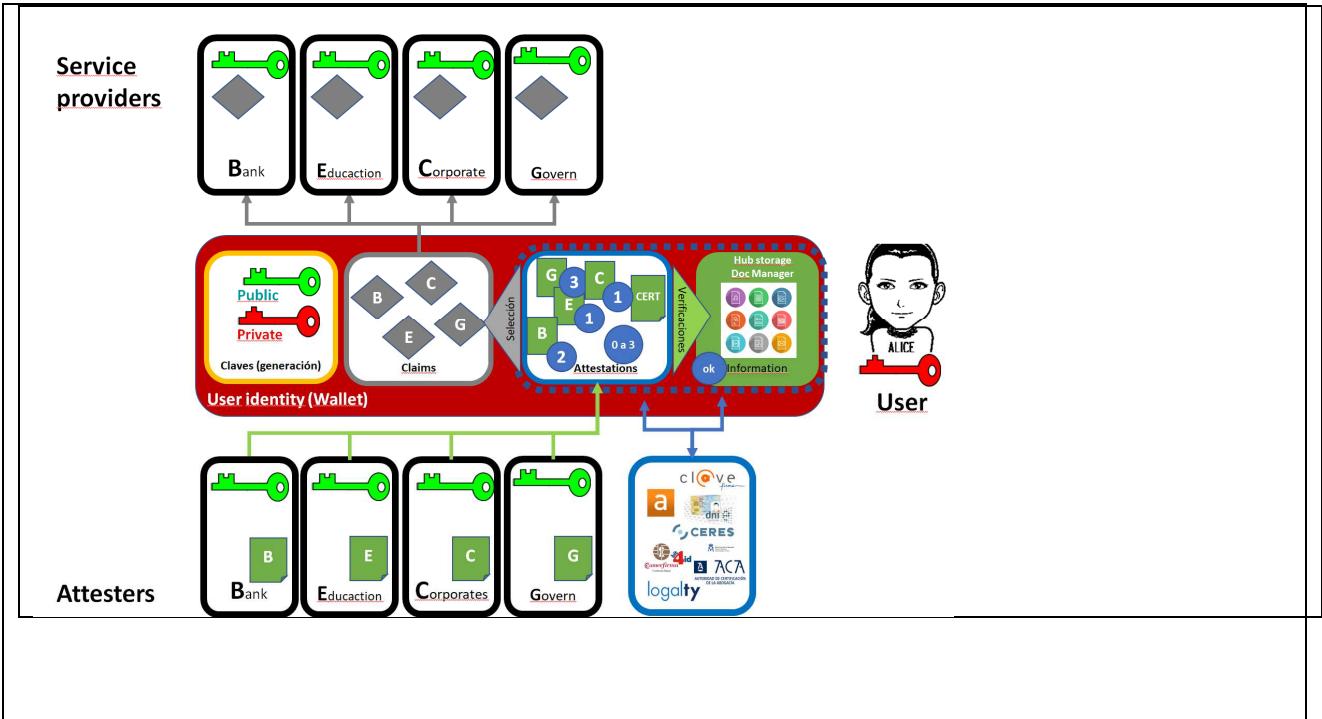
Current Solutions

There are a number of private consortiums and federated ones, but ALASTRIA is moderating the decentralization to a middle point between public and private permissioned infrastructure with all relevant participants for a country or jurisdiction like Public Notary, Corporate Registration Office and listed, medium and small and micro-enterprises, also covenants with other Public administration covering the possibility for a network for frameworks and vice-versa.

Section 2: Current process

Process scheme (as-is) and ROLES / DATA FLOW





Data and information (as-is)

Data	Type	Description
1	<i>Adhesion</i>	Normal standard document for being a member of Alastria See https://alastria.io/en/become-a-member/

Participants and their roles

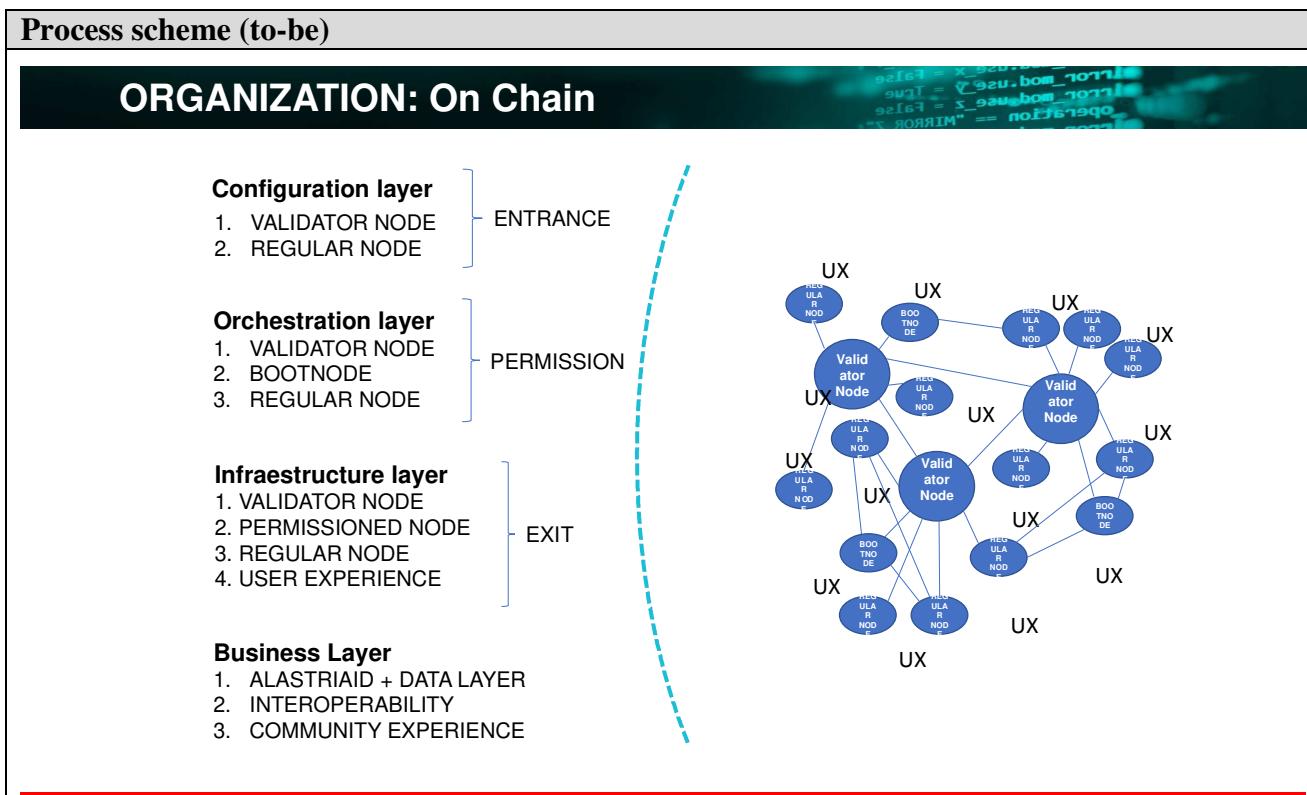
Actor	Type/Role	Description
1	<i>Commissions</i>	Deploy different areas of the infrastructure, technological area, resilience area, trust framework area, standards, sustainability area, risk and cybersecurity processing.
2	<i>Committees</i>	Coordination and Implementation of the decision making for administrative proposes.

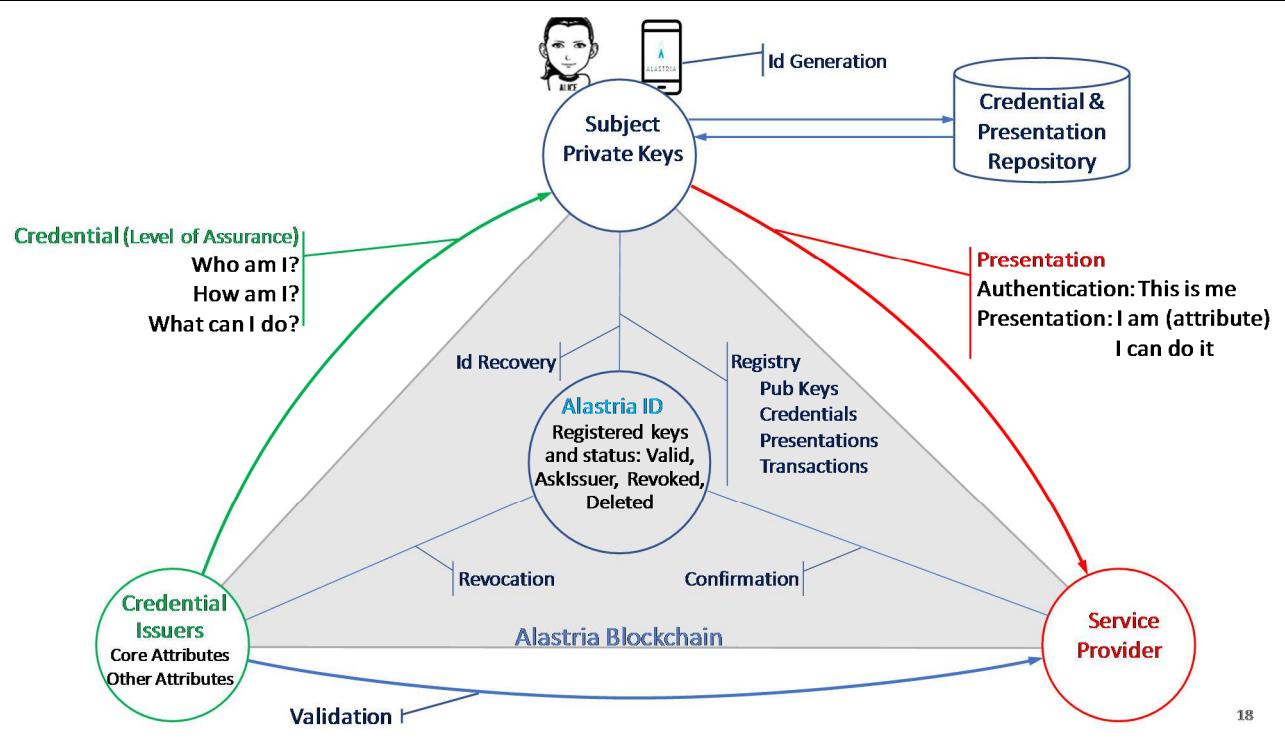
Other Notes

No.

Section 3: Expected process

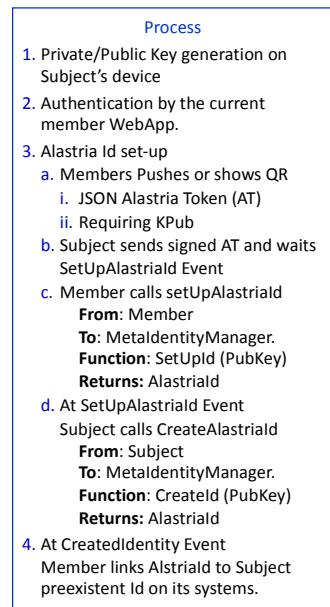
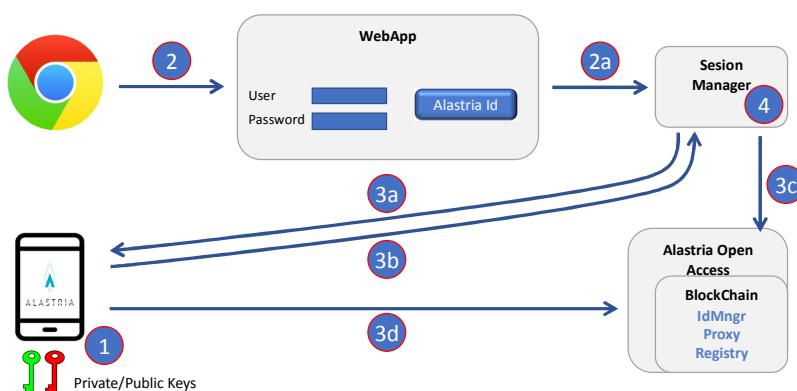
Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Generation	Alastria ID Generation
2.	Authentication	Verification and Validation
3.	Public Keys	Generation, Registration, Revocation and Deletion
4.	Credentials	Issuance, Registration, Revocation and Deletion
5.	Presentations	Issuance, Registration, Confirmation and Deletion.
6.	Identity and Private Key Backup & Recovery	Alastria Backup & Recovery ID.
7.	Signed transactions	Smart contracts and Dapps.





18

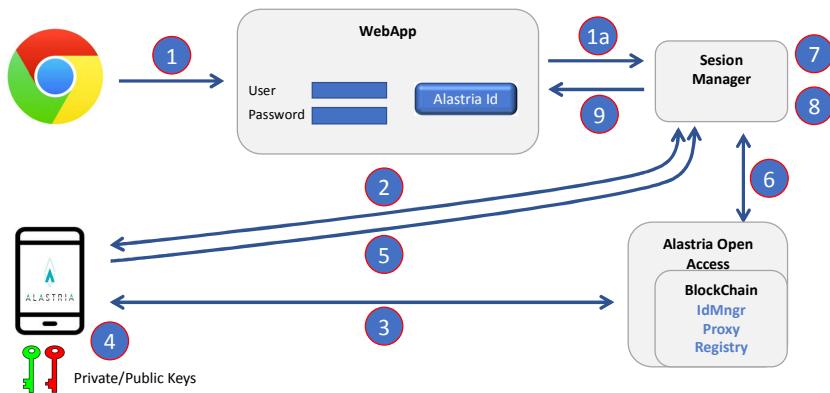
AlastriaId Generation



28

Process scheme (to-be)

Alastriald Authentication



Process

1. User connects to WebApp and selects Alastria Id.
2. Member pushes or shows QR signed JSON with:
 - a. Alastria Token
 - b. Requiring Subject's Alastriald & PubKey
3. Alastria App picks member's Public Key (Hash) through GW.
4. Step 2 signature is checked.
5. User sends Signed Alastria Session with:
 - a. Alastria Token
 - b. Alastriald + PubKey
6. Member picks subject's Public Key (Hash) through GW
7. Step 5 signature is checked
8. First time Alastriald authentication requires traditional authentication or reliable Credential. Alastriald must be linked to a preexisting Id.
9. Session token is sent to WebApp.

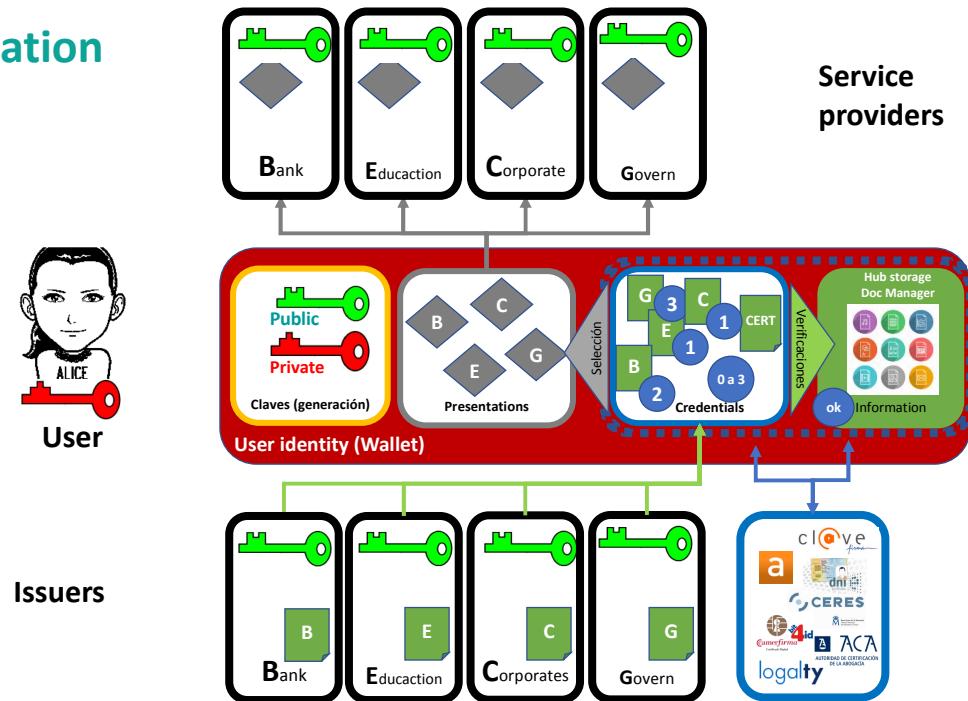
29

Participants and their roles

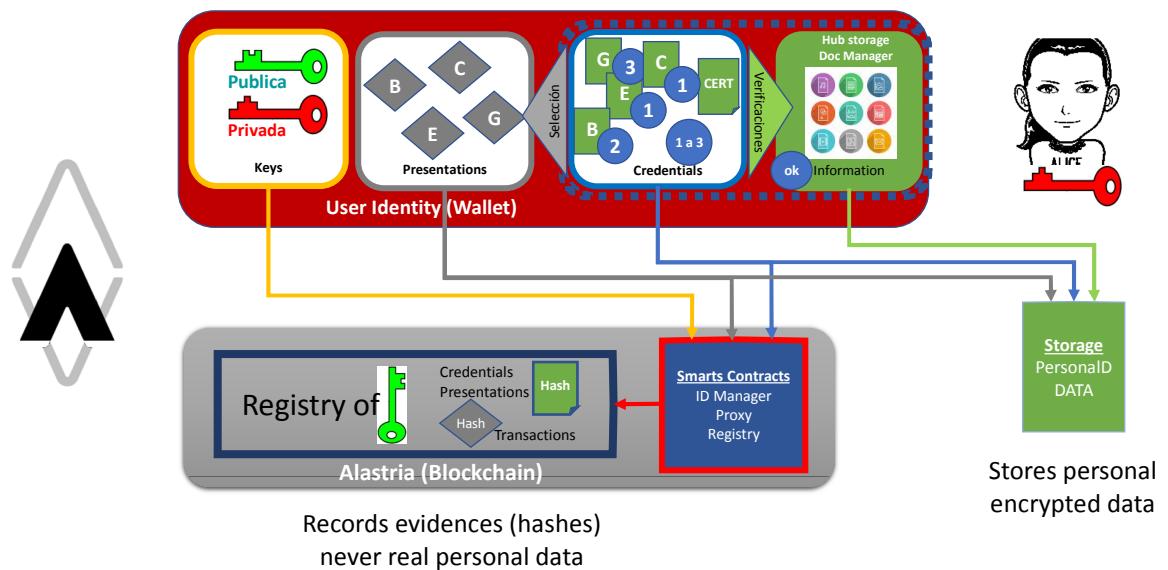
Actor	Type/Role	Description
1	User	ID generation
2.	Credential Issuer	Attributes and other events.
3.	Service Provider	Trust anchoring.
4.	AlastriaID	Registry, Recovery, Revocation, Confirmation, Deletion.

Data and information

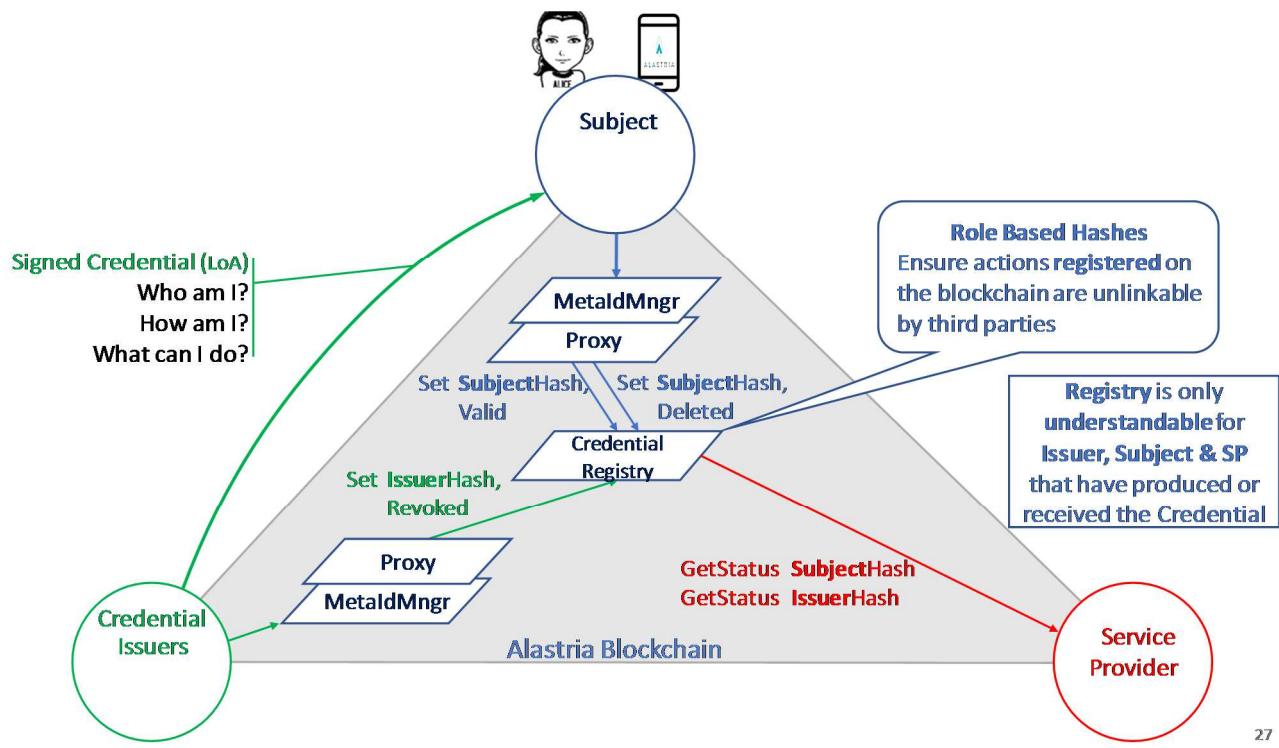
Information



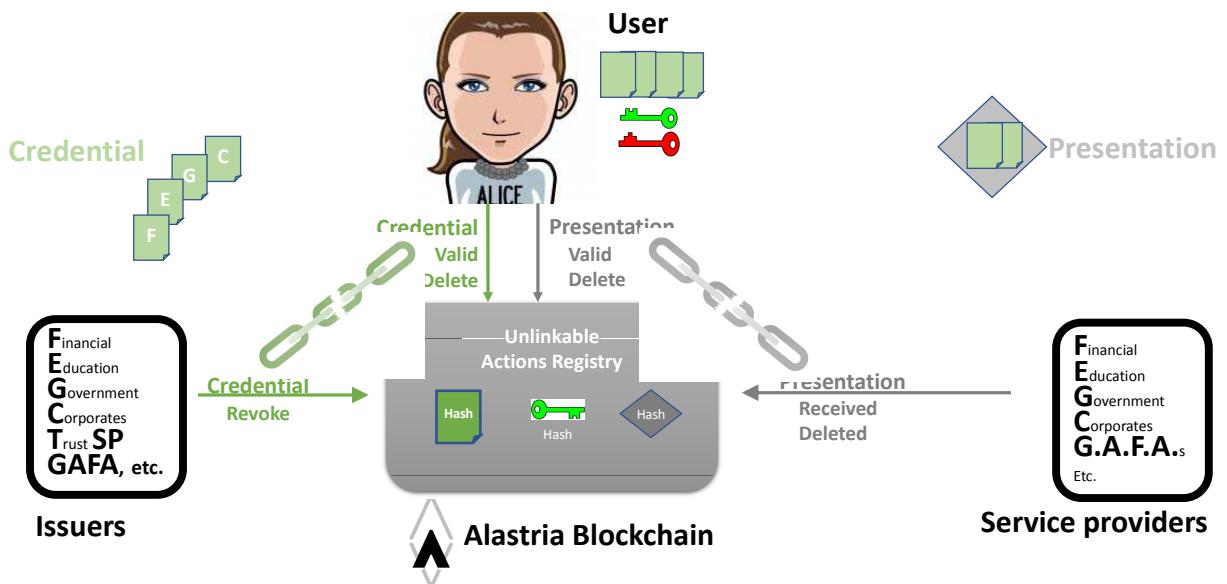
Information repositories

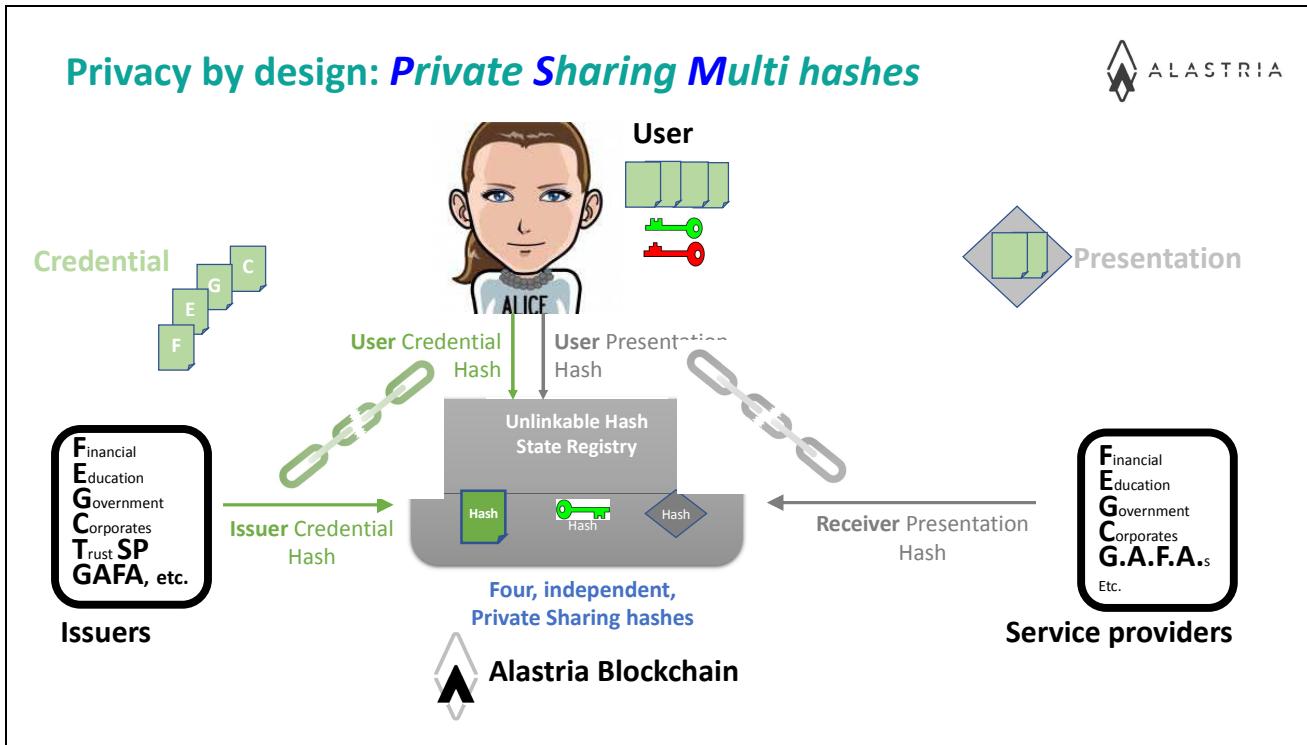


Security and privacy



Unlinkable actions on Credentials & Presentations





Main Success Scenario + expected time line

Various verticals are in production, Restricted MAIN-NET. Three test nets more for the framework of networks. LacChain Mainnet 2019. Testing two projects under European Blockchain Partnership. New Work Item at UNE CTN71/SC307 standard for decentralized ID.

Conditions (pre- or post-)

Public Permission Ecosystems are subject to some specific identification methods.

Performance needs

Extensibility and Scalability priorities. Healthcare PoC with the whole legal system of Spain for vaccines 'process, PoC for Traceability of Agrofood and Seafood, Sustainability transversal PoC for diplomas.

Legal considerations

Trust Framework Commission of Alastria is the tool that is creating all policies for interoperability. Legal and Compliance deployment and other legal checklist maintenance.

Risks

Uncertainty of regulation. Alternative Dispute Resolution must be efficient. Level of Assurance and Level of causalities.

Special Requirements

Not applicable

External References and Miscellaneous

ALASTRIA ID gives a complete compliance with GDPR and eIDAS.

Other Notes

This use case follows W3C Verifiable Credential and is compatible with EIP1812 for interoperability.

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)
-

Digital Identity as a Service

Section 1 Summary

Use Case Summary					
Use Case ID:	IDM-002	Use Case Type:	Horizontal		
Submission Date:	October 11, 2018	Is Use Case supporting SDGs	No		
Use Case Title:	Digital Identity as a service	Domain:	Cybersecurity		
Status of Case	PoC	Sub-Domain	Mobile roaming Digital Services		
Contact information of person submitting/managing the use-case	Full Name: Alexander Yakovenko Job Title: Project Director E-mail address: ayakovenko@clementvale.com Telephone number: +7-985-991-2048 Social media: https://www.linkedin.com/in/alexander-yakovenko Web site: https://www.blockchaintele.com				
Proposing Organization	Clementvale Baltic OU, Estonia				
Short Description	This use case is a proposal to implement Digital identity with the use of DLT and use it as a service				
Long description	This use case is a proposal to implement Digital identity with the use of DLT and use it as a service				
SDG in Focus (when applicable)					
Value Transfer:		Number of Users:	100+		
Types of Users:	Private users who need to supply personal data to get services, service providers.				
Stakeholders	Any service provider identifying their customers. Mobile operators validating their customers.				
Data:	Hashes of validated personal data				
Identification:	Mobile operator verifies personal data by request of their customer and publishes its hash in blockchain				
Predicted Outcomes:	Decentralized approach, which allows exchanging of personal data, compliant with “General Data Protection Regulation” (GDPR)				

Overview of the Business Problem or Opportunity

It is critical for mobile operators and mobile service providers to know with whom they are interacting. Growing IoT market and IoT services make this problem even more prominent. Traditionally a person who needs to identify himself must visit office of organization and present his passport and other documents. For private person this is inconvenient and time-consuming procedure. For organizations this is significant item of expenditure.

*Usually mobile operators possess all information necessary to identify their customers. They can use blockchain to effectively assist customers to identify themselves to other participants by supplying identity verification services. The approach is developed to be fully compatible with “General Data Protection Regulation”. **No actual transfer of personal information is expected between organizations.***

Why Distributed Ledger Technology?

Distributed Ledger is an optimal solution for this use case because:

- *Verification of identity information (without disclosing identity information itself) can be shared across all participants of decentralized platform.*
- *Different mobile operators as well as other authorized organizations can provide digital identity services in similar standardized way.*
- *Identity services are immediately available to multiple service providers and consumers through the same Distributed Ledger platform for telecom.*

Section 2 Current process

Current Solutions		
<i>Currently private users need to visit office of organization with identity documents, such as passport, driving license, social security, etc.</i>		
<i>Each organization providing online identification for their customers have to re-implement corresponded software platform and take care about fraud data.</i>		

Existing Flow (as-is)		
Step	User Actions	System Actions
1.		

Process scheme (as-is)		

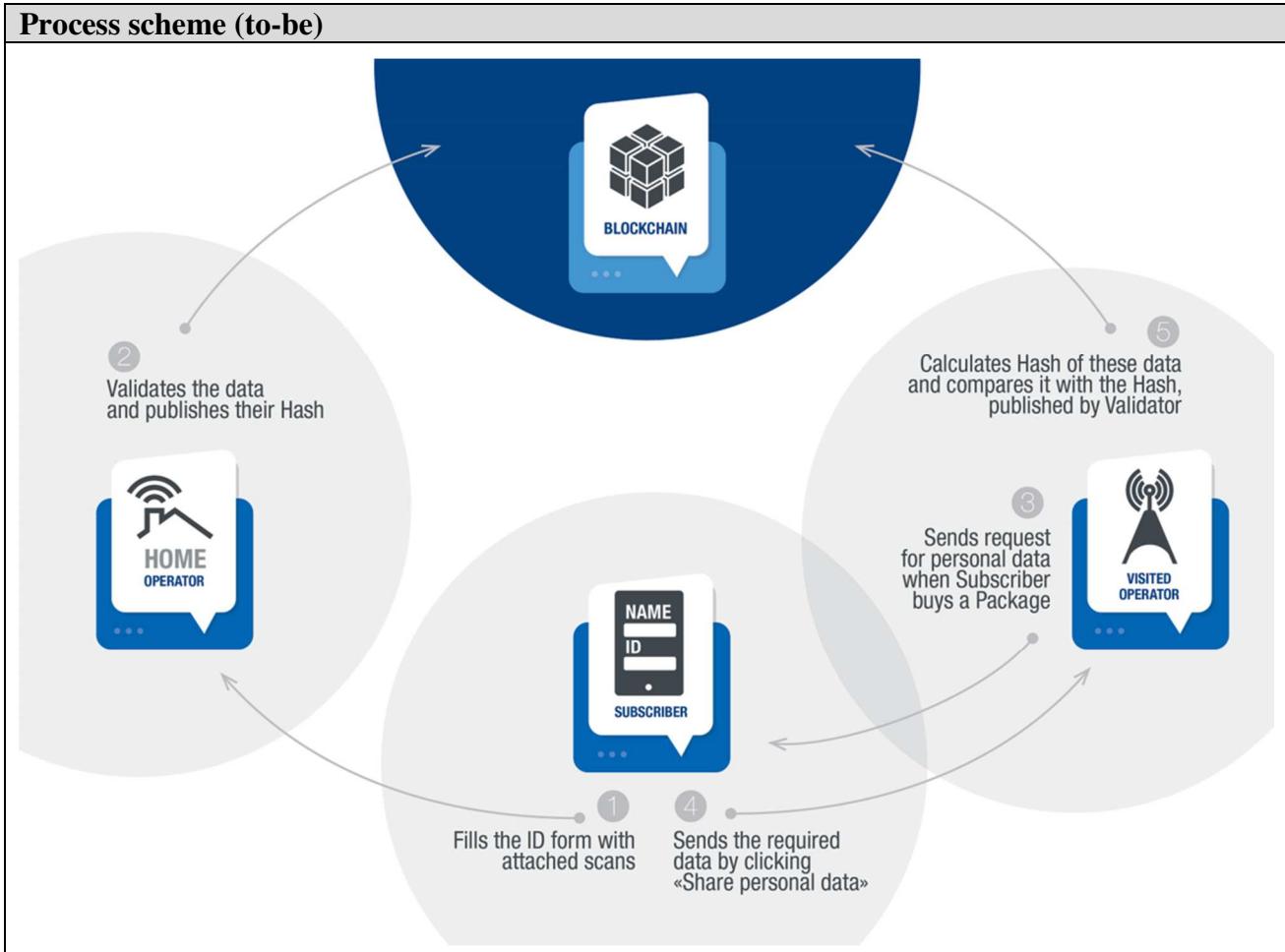
Data and information (as-is)		
Data	Type	Description
1		

Participants and their roles (as-is)		
Actor	Type/Role	Description
1		

Other Notes		

Section 3 Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Subscriber: Fills the ID form, attaches scans of passport and other documents, stores the ID file in his smartphone	n/a
2.	Subscriber: Sends the ID file to his home operator.	n/a
3.	Home operator: Verifies the data in ID file, calculates the hash of the data and sends hash to DLT system in signed transaction.	n/a
4.		Verifies digital signatures of transaction and makes hash of ID file available to all participants.
5.	Subscriber: On request to identify himself from visited operator or service provider, sends ID file prepared on step (1.)	n/a
6.	Visited operator: Calculates hash of ID file and requests DLT system for the validity of the hash	n/a
7.		Looks up hashes available and, if found, returns validity status of ID file along with validating organization details.



Participants and their roles		
Actor	Type/Role	Description
1	<i>Subscriber</i>	Subscriber of mobile service, who needs to identify himself.
2	<i>Home operator</i>	Mobile operator hosting Subscriber in his native country (or other authorized organization), which can identify Subscriber and verify identity information.
3	<i>Visited operator</i>	Another mobile operator (for example, foreign operator in visited country) or service provider which need to get identity information from a customer to supply services.

Data and information		
Data	Type	Description
1	<i>Documents</i>	<p>Scans of passport and any other documents which customer may be requested to present.</p> <p>It is essential that organizations never share those data with each other. Instead, they request customer to supply data to get some services and use DLT system to verify supplied data.</p>

Data and information		
Data	Type	Description
2.	<i>ID file</i>	A collection of documents stored in a special file at customer's smartphone.
3.	<i>Hash</i>	Digital hash of ID file transmitted via blockchain by home operator to make identification status available to other participants.

Security and privacy
1. <i>Identity status (hash of ID file) is protected by digital signature of home operator within corresponded transaction within DLT system</i>
2. No private data are stored in the DLT system.
3. No any personal data is transmitted from home operator to another operators or service providers
4. Hashes can be transmitted without any linkage to the person, so no one could actually use shared hashes unless the person explicitly decide to disclose his data to some participants.

Main Success Scenario
<i>DLT-based global market place where different mobile operators and other participants (telecom and non-telecom service providers, content providers, software vendors, etc) can supply their services to customers of other operators all over the world. Digital identity is an essential and integrated part of this solution.</i>

Conditions (pre- or post-)
<i>n/a</i>

Performance needs
<i>Although not strictly required, fast transactions (within a few seconds) are desirable to distribute identity status among participants.</i>

Legal considerations
<i>Solution is assumed to be compliant with "General Data Protection Regulation" because participants never share personal data with each other. They use DLT system only for validation of personal data supplied by customer.</i>

Risks
<i>n/a</i>

Special Requirements

- 1. Participants must agree about format of ID file*
- 2. Users must be supplied corresponded software to prepare ID files*
- 3. Hashing algorithm must be agreed or recorded in the ID file*

External References and Miscellaneous

<https://blockchaintele.com>

https://wiki.blockchaintele.com/index.php/Main_Page

https://wiki.blockchaintele.com/index.php/Use_cases#New_revenue_stream_on_.22Identity-as-a-Service.22

Other Notes

Using human factors and a social graph to bootstrap ID

Section 1: Summary

Use Case Summary					
Use Case ID:	IDM-004	Use Case Type:	<i>Vertical/Horizontal</i>		
Submission Date:	January 4, 2019	Is Use Case supporting SDGs	<i>Yes/no</i>		
Use Case Title:	Decentral Identification – Using human factors and a social graph to bootstrap ID.	Domain:	<i>4-B</i>		
Status of Case	<i>PoC, to be improved with use of Quorum</i>	Sub-Domain	<i>I</i>		
Contact information of person submitting/managing the use-case	Full Name: Christopher Hughes Job Title: CTO E-mail address: Christopher.hughes@gmail.com Telephone number: +13104083731 Social media: twitter.com/chews Web site: www.relateid.com				
Proposing Organization	JPMorgan Quorum Developers - New York				
Short Description	A human biometric system for creating a public/private keypair in a private blockchain.				
Long description	<p>Self-sovereign ID.</p> <p>Using a social bootstrapping mechanism (using a plurality of attestations) allow humans to self-initialize identification.</p> <p>This aids in identification of displaced people/refugees.</p> <p>Once ID layer is initialized; allow additional attestations for education, professional certifications, or other relevant social data points.</p>				
SDG in Focus (when applicable)	3. Improve health, attesting immunization records to RelateID 4. Improve education, attesting educational records to RelateID 5. Reduce gender inequality, using genderless ZKSnark matching. 10 Reduce race inequality, by using ZKSnark matching. 16 Improve voting, attesting educational records to RelateID				
Value Transfer:		Number of Users:			
Types of Users:	<i>Government actors, NGOs, aid organizations, health professionals, educators.</i>				
Stakeholders	<i>Displaced humans, new immigrants</i>				
Data:	RelateID acts as the tool to create the identity via a mobile app, that ID is stored on a quorum based chain, this application collects some biological data and hashes it with the local blockchains seed to create a localized				

	<p>identity. This IDs “trueness” is improved with attestations from humans within the social graph.</p> <p>Public/Private key's that cannot be lost because they are tied to human factors that don't change (Iris, heartbeat, and possibly DNA)</p> <p>Basic attestations (Name, Height, Weight, Eye color, Country of Origin)</p> <p>Immunization / Health attestations</p> <p>Professional attestations (education)</p>
Identification:	This is a fundamental ID mechanism, we would use human factors to establish them, and save those factors via a public/private key mechanism that is recoverable using those human factors.
Predicted Outcomes:	A simple and robust, yet non-central identification system can be “popped-up” as needed. These decentralized ID networks can but don't have to be interlinked.

Overview of the Business Problem or Opportunity	
<i>A robust and fair identification system that can be deployed quickly and interact with localized governments via APIs and reports. The hope here is to create an identification standard by which humans can self-initiate and benefit from.</i>	
Why Distributed Ledger Technology?	
Decentralized generation of Private/Public key, this system can rely on the participants to provide public keys (IDs) these IDs are portable, meaning they can be moved to future chains without needing to be re-established.	
Chains make use of attestations, that are basically transactions to establish further truth.	
These transactions act like a wallet of facts that exist within a temporary context but can be moved to public networks.	

Section 2: Current process

Current Solutions	
<i>We are unaware of systems to do this at present.</i>	

Existing Flow (as-is)		
Step	User Actions	System Actions
1.		
2.		

Process scheme (as-is)	

Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	
2	<i>Payment transactions</i>	

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

Other Notes
<i>Any assumptions, issues</i>

Section 3: Expected process

Expected Flow (to-be)		
Step	User Actions	System Actions
1.	User who wants to be ID'd submits bio-factors	Saves them to the quorum chain.
2.	Once bootstrapped, human asks social graph (who've also established IDs) to attest to related truths	Truths are saved to chain, confidence of truth improves.
3.	User goes for a health checkup, aid organizations add truths to human wallet, by providing some aid, the organization logs their work	Those transactions that collected immunization/health records attest to further truth
4.	User attends schools	Educational attestations are added to chain.

Process scheme (to-be)
A mobile app to collect the data, a mobile/web application to collect additional truths, and a set of easy to deploy quorum servers to collect this data.

Participants and their roles		
Actor	Type/Role	Description
1	<i>Users</i>	Humans who want to be IDd
2	<i>Educators</i>	Participants in system, who can attest to truth
3	<i>Aid Organizations</i>	Participants in system, who can attest to truth

Data and information		
Data	Type	Description
1	<i>Documents</i>	Health records, immunization records, human-factors

Security and privacy
1. Use of best of breed cloud hosted, but also locally available hardware.

Main Success Scenario + expected time line
A easy to bootup identification mechanism for displaced humans. Using a template on a cloud provider to establish the infrastructure, the mobile application can easily pair with the network

and provide the means to collect attestations. The mobile app acts as a wallet for truths, and as a means to create truth proofs for others.

Conditions (pre- or post-)

1.

Performance needs

Basic cellular coverage and yes, the internet is required.

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.

Risks

Centralized ID scares people, by using mobile devices, localized truth, and permissioned sidechains, these concerns can be overcome.

Special Requirements

none

External References and Miscellaneous

Checkout the work done by the RelateID foundation.

<http://www.relateid.com>

Other Notes

Any assumptions, issues

Energy Distribution with the Use of Smart Contracts

Section 1: Summary

Use Case Summary					
Use Case ID:	IND-001	Use Case Type:	<i>Vertical</i>		
Submission Date:	October 17, 2018	Is Use Case supporting SDGs	<i>Yes</i>		
Use Case Title:	Energy distribution with the use of smart contracts	Domain:	<i>Industry</i>		
Status of Case	PoC	Sub-Domain	<i>Energy</i>		
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	<p>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.</p> <p>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.</p> <p>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.</p>				

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:	<i>energy data</i>		
Identification:	energy producer (anonymous), energy consumer (anonymous), smart meter		
Predicted Outcomes:	<p>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:</p> <ul style="list-style-type: none"> • 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
<i>If there are existing systems which automate the above business problem/opportunity.</i>

Existing Flow (as-is)		
Step	User Actions	System Actions
1.		
2.		

Process scheme (as-is)

Data and information (as-is)		
Data	Type	Description

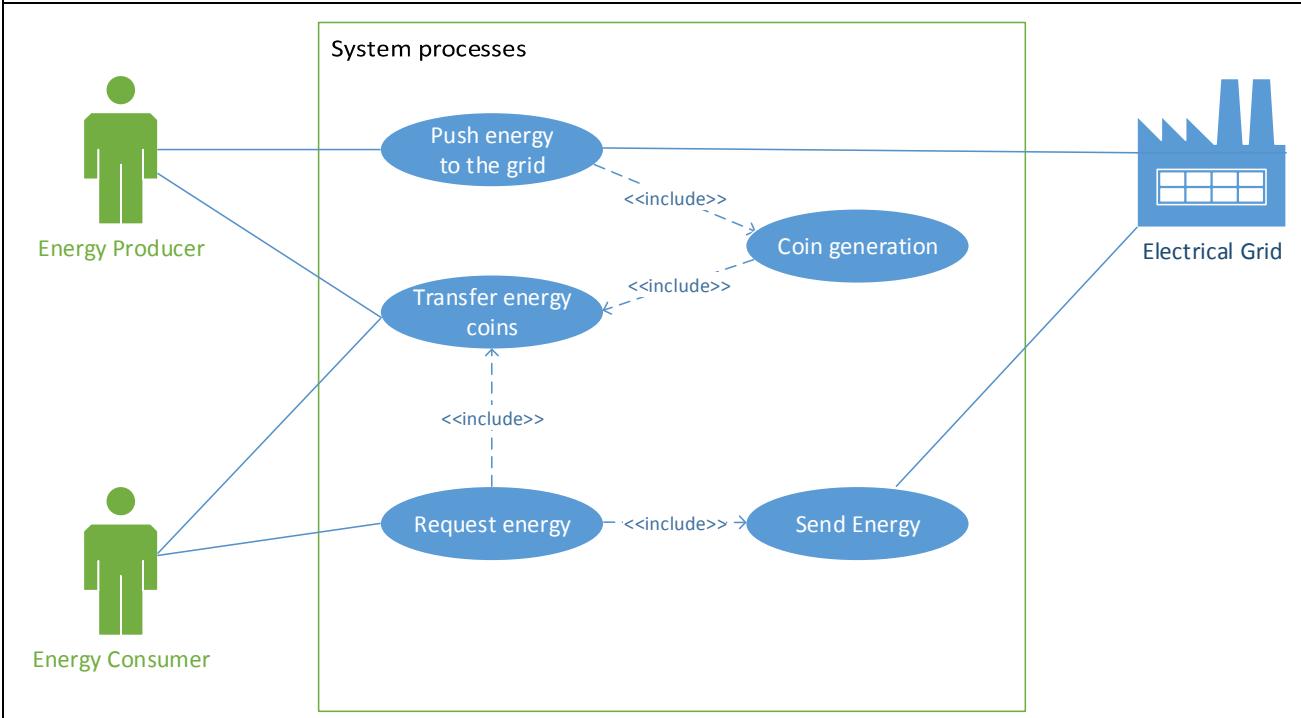
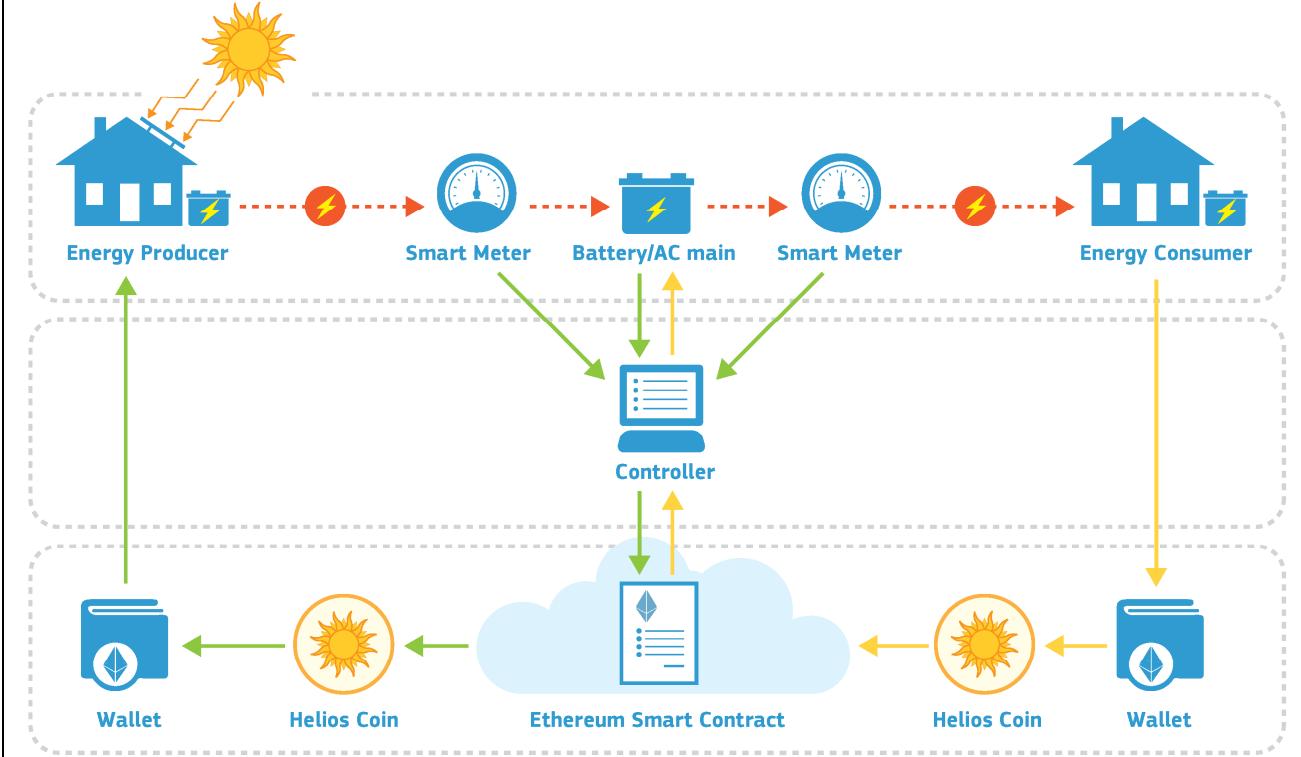
Participants and their roles (as-is)		
Actor	Type/Role	Description

Other Notes
<i>Any assumptions, issues</i>

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	<i>Energy Producer (user)</i>	The entity that produces energy and pushed it in the grid

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

Data and information		
Data	Type	Description
1	<i>Helios Coin</i>	A digital token that can be exchanged for a predefined amount of energy
2	<i>Energy Measurements</i>	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 a 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:	<i>Vertical</i>
Submission Date:	December 17, 2018	Is Use Case supporting SDGs	
Use Case Title:	P2P Energy Trading	Domain:	<i>Industry</i>
Status of Case	<i>Proof of Concept (PoC)</i>	Sub-Domain	<i>Energy</i>
Contact information of person submitting/managing the use-case	<i>Igor Ferreira [FOHAT] igor.ferreira@fohat.co https://www.linkedin.com/in/figor</i>	<i>Chief Executive Officer +55 41 9 9101-9222</i>	
Proposing Organization	<i>FOHAT Corporation</i>		
Short Description	<i>Usage of token (NRJ TOKEN) and DLT (EW CHAIN) for energy trading of the Distributed Energy Resources (DERs) inside Blockchain Microgrids.</i>		
Long description	<i>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.</i>		
SDG in Focus (when applicable)	7-11		
Value Transfer:	<i>Tokens</i>	Number of Users:	
Types of Users:	<i>Energy Traders, Prosumers</i>		
Stakeholders	<i>Development Bank, Utility Companies</i>		
Data:	<p>=> Shared Data (DLT)</p> <ul style="list-style-type: none"> ● Transaction history for audit purposes; <p>=> Use case specific DLT data:</p> <ul style="list-style-type: none"> ● Account; ● Token Balance; ● Forecasting; <p>=> External Data (not stored in DLT):</p>		

	<ul style="list-style-type: none">• Energy usage inside Microgrid;
Identification:	<i>KYC (Know Your Customer) for Energy Traders and Prosumers</i>
Predicted Outcomes:	<p>The predicted outcomes are:</p> <ul style="list-style-type: none">• 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;

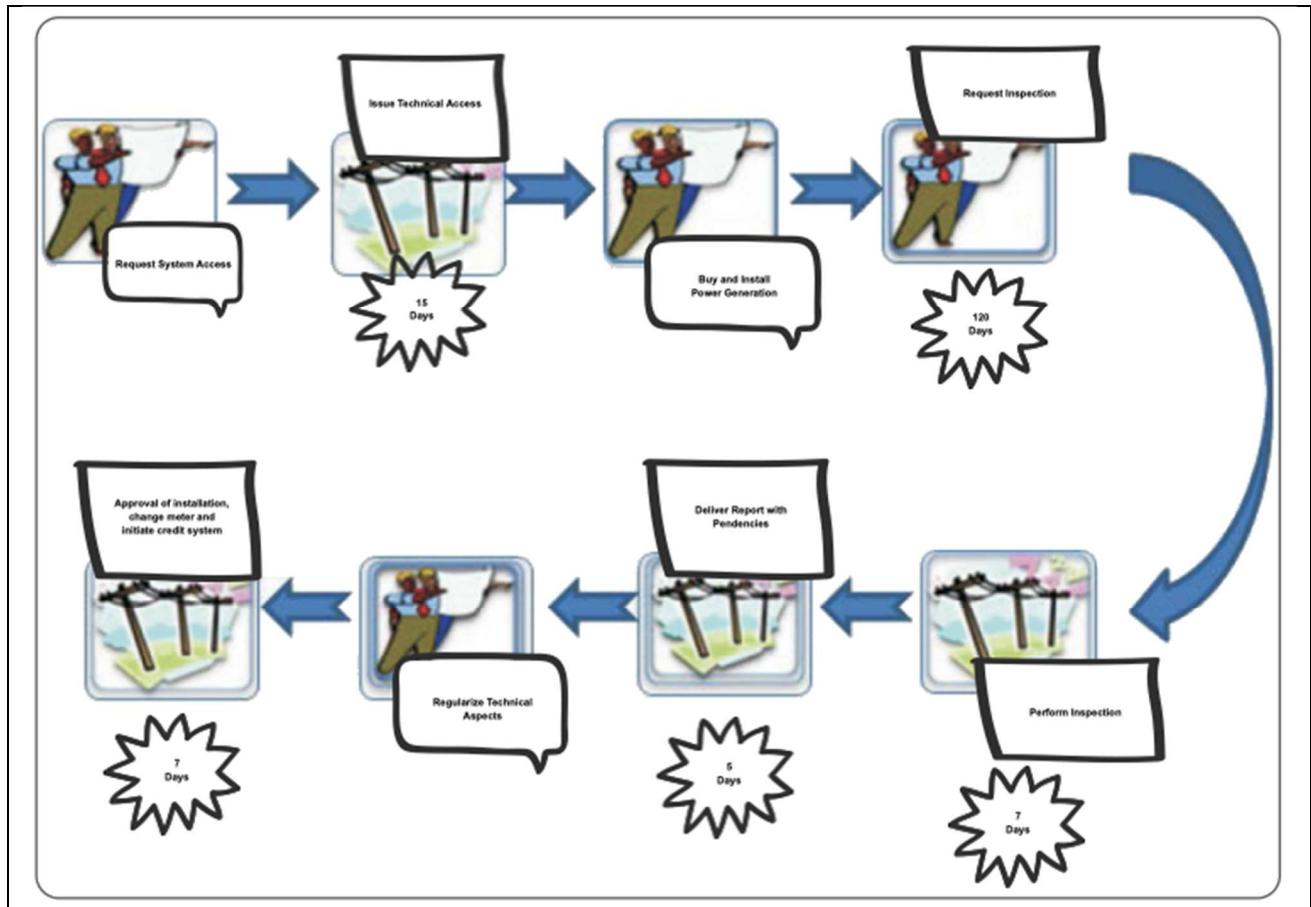
Overview of the Business Problem or Opportunity	
<p><i>The Energy Sector is key for the development of the society and to secure access to a comfortable life for everyone, is a key product/service that support people's life and the country growth.</i></p>	
<p><i>The world is moving from a Centralized 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..</i></p>	
Why Distributed Ledger Technology?	<p><i>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.</i></p>

Section 2: Current process

Current Solutions	
<i>Utility Companies - Distributed Generation Credit System</i>	

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)

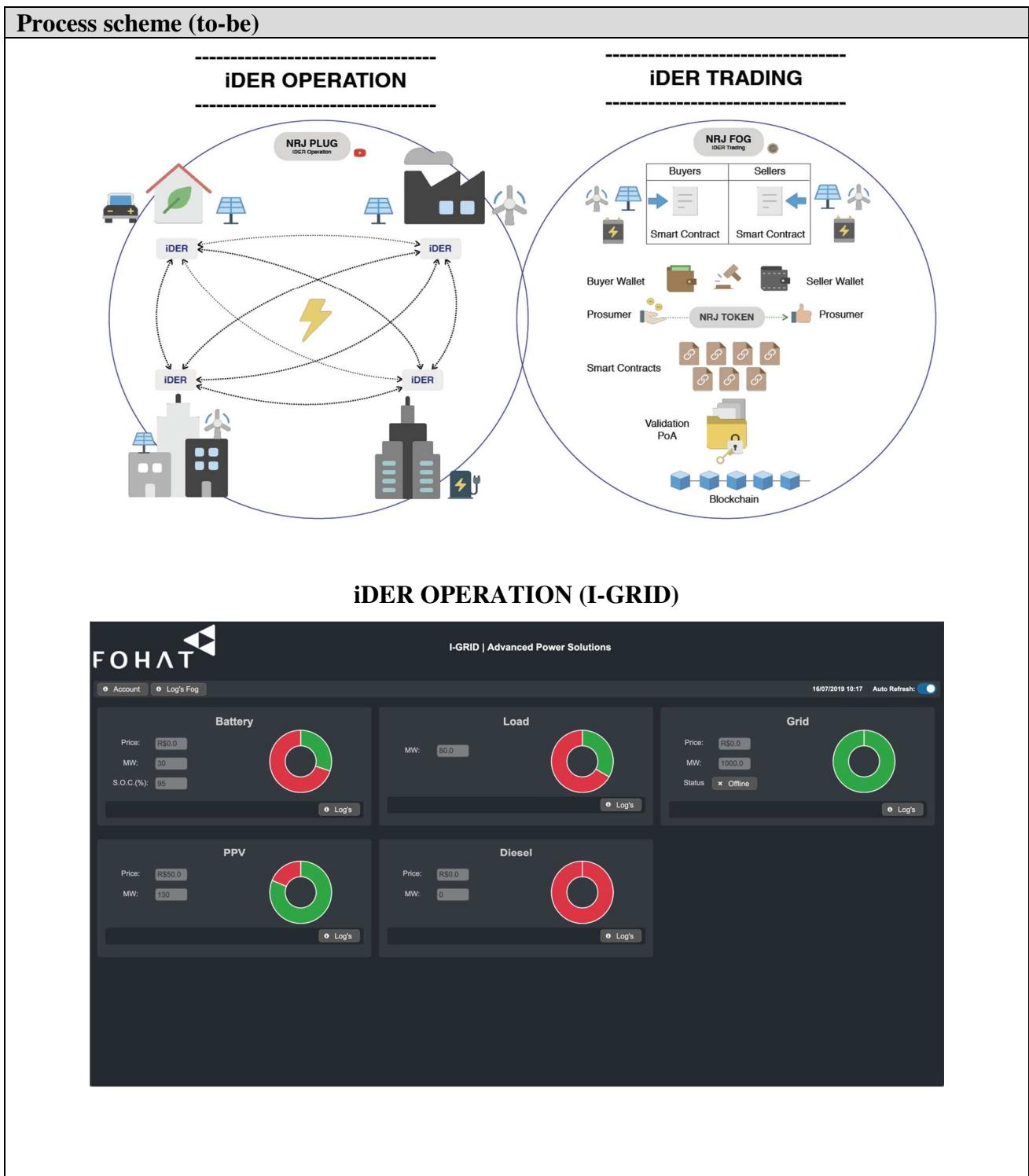
Actor	Type/Role	Description
1	Users	Prossumers (Producer and Consumer)
2	Utility	Energy distribution and power grant

Other Notes

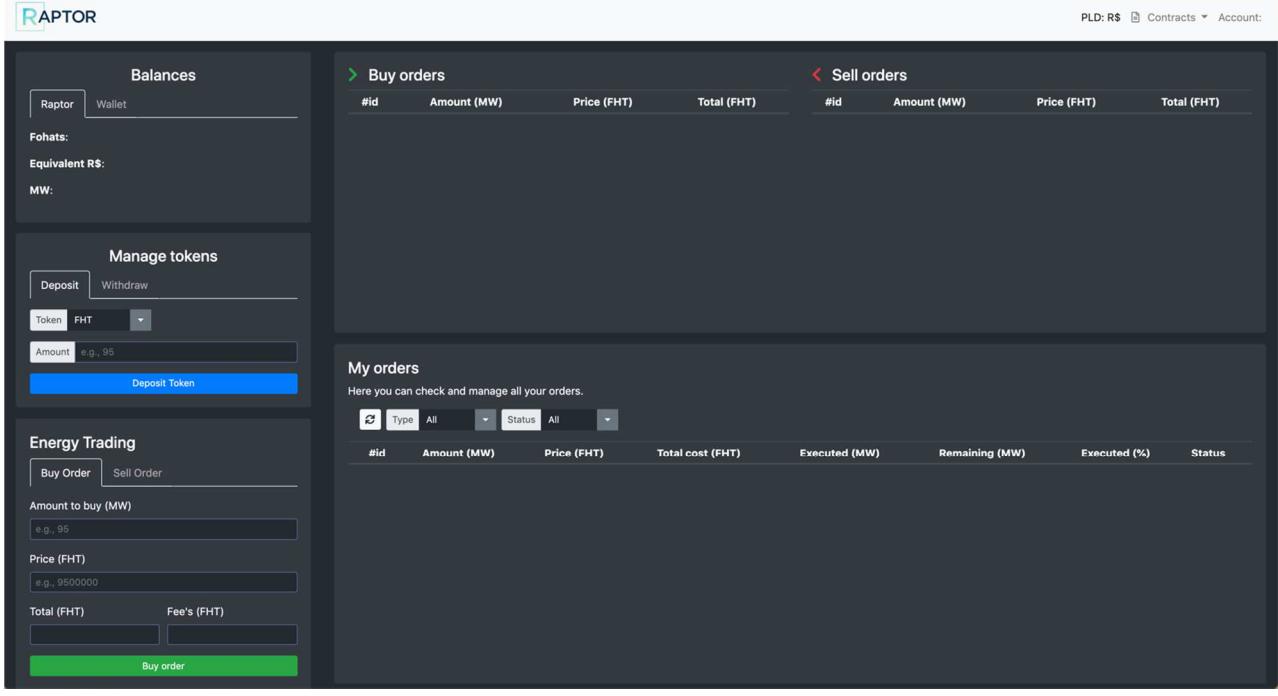
--

Section 3: Expected process

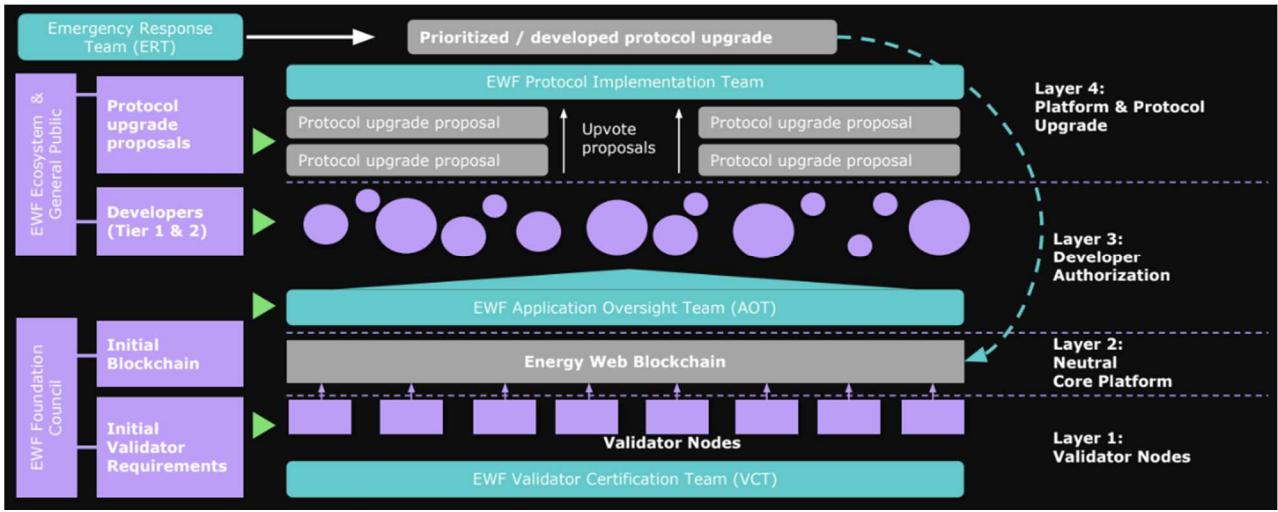
Expected Flow (to-be)		
Step	User Actions	System Actions
1.	Prosumers	Request access to the Microgrid
2.	Utility	Provide access to the Microgrid



iDER TRADING (RAPTOR)



EWF Solution



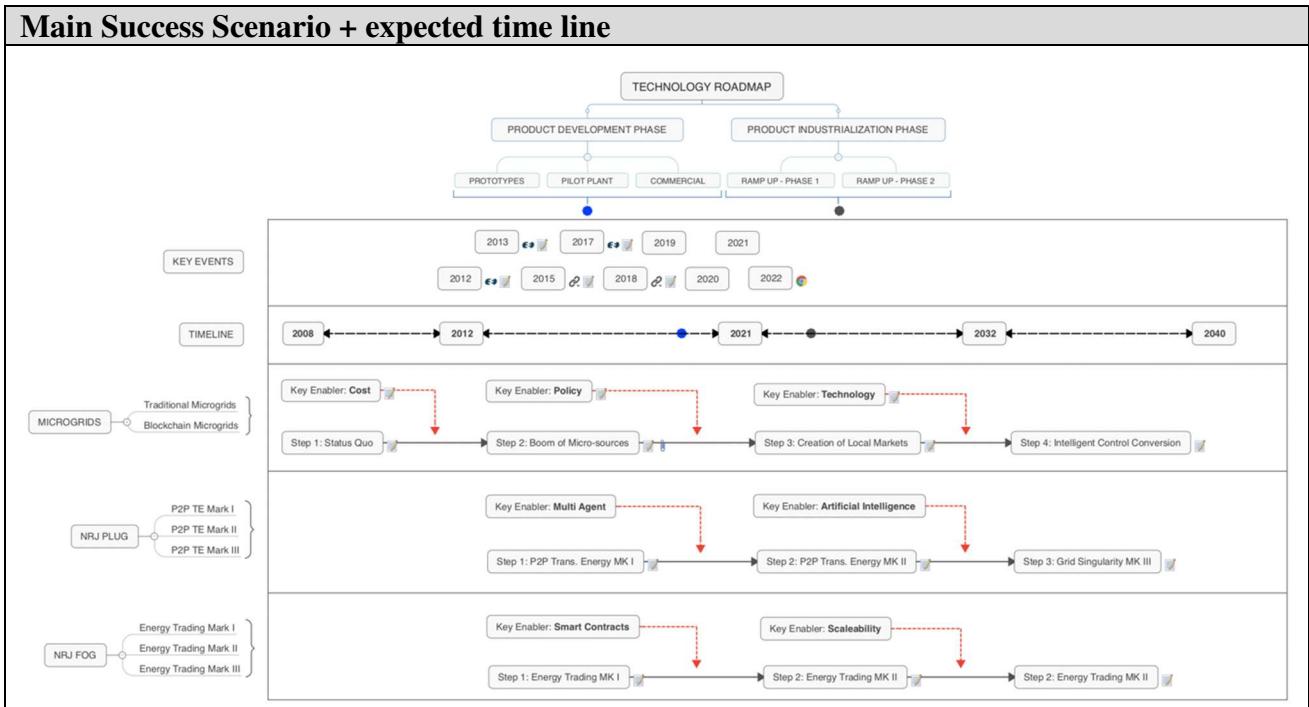
Participants and their roles		
Actor	Type/Role	Description
1	Prossumers	DER owners
2	Energy Retailers	Sell excess energy from DER Owners.

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



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



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)
-