Smart Contracts for Data Accountability and Provenance Tracking

Section 1 Summary

Use Case Summary			
Use Case ID:	DTM-001	**Use Case Type:**	*Horizontal*
Submission Date:	December 14, 2018	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Smart contracts for data accountability and provenance tracking	**Domain:**	*Data processing, storage and management*
Status of Case	*Proof-of-concept*	**Sub-Domain**	
Contact information of person submitting/ managing the use-case	*Full Name: Ricardo Neisse* *Job Title: Scientific Project Officer* *E-mail address: ricardo.neisse@ec.europa.eu* *Telephone number: +39 0332 78 9592* *Social media: https://twitter.com/EU_ScienceHub* *Web site:* https://ec.europa.eu/jrc/en		
Proposing Organization	*European Commission Joint Research Center, Ispra, Italy*		
Short Description	*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.*		
Long description	*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.*		
SDG in Focus (when applicable)	*Goal 16: Promote just, peaceful and inclusive societies*		
Value Transfer:	*Fingerprints of digital identity and personal data items*	**Number of Users:**	*Large scale including citizens of many EU countries*
Types of Users:	*Data Subjects, Data Controllers, and Data Processors*		
Stakeholders	*Citizens, enterprises handling digital identity and personal data items, government institutions auditing privacy practices of enterprises.*		

Data:	*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.*
Identification:	*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.*
Predicted Outcomes:	

Overview of the Business Problem or Opportunity
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. *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.*
Why Distributed Ledger Technology?
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.

Section 2 Current process

Current Solutions
Not available.

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

Process scheme (as-is)

Data and information (as-is)		
Data	Type	Description

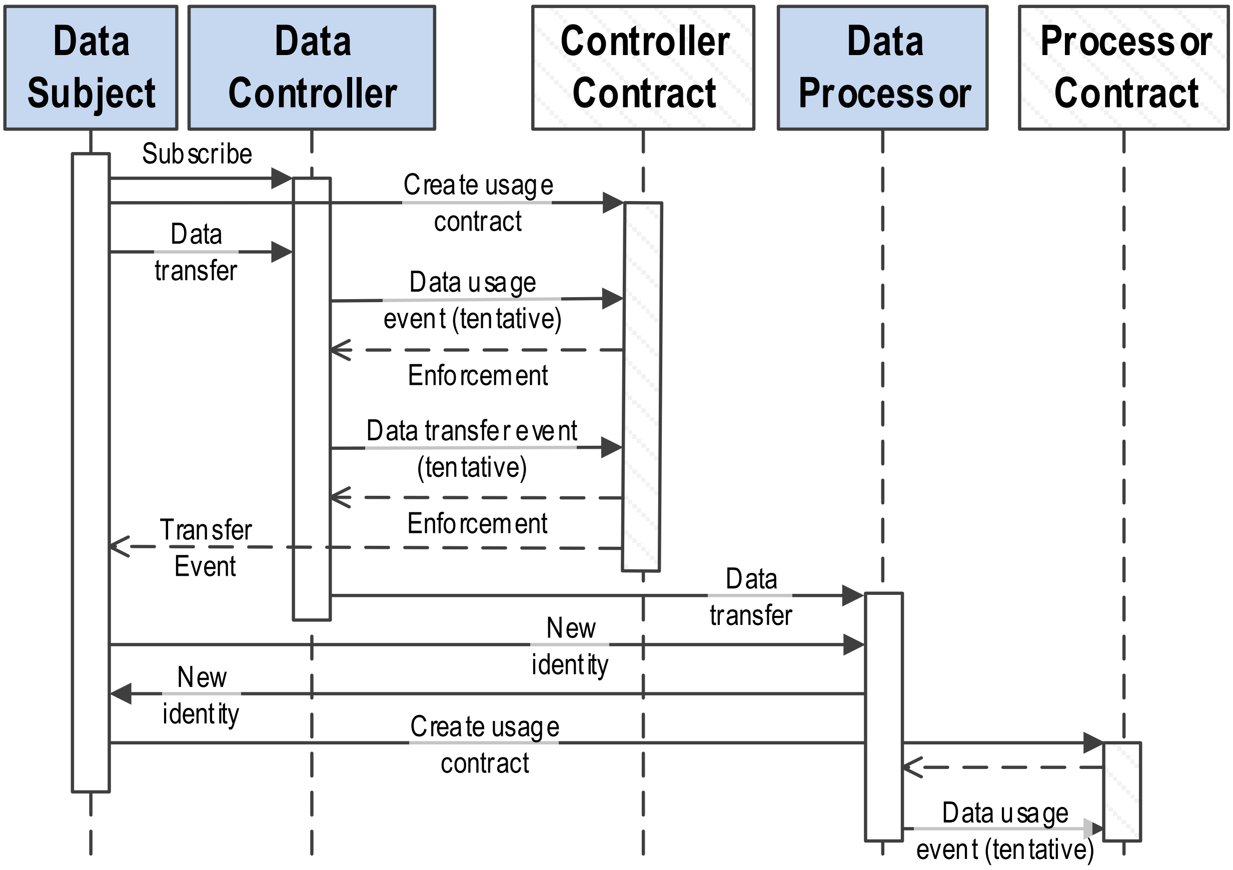
Participants and their roles (as-is)		
Actor	Type/Role	Description

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.

Process scheme (to-be)



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

Data and information		
Data	**Type**	**Description**
1.	*Subject, controller, and processor identities*	Unique identities for subjects, controller, and processor that are not re-used for other contracts in order to avoid linkability.
2.	*Data type and value fingerprints*	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.	*Usage control policy*	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
The data items and identities stored in the blockchain are obfuscated to allow a privacy-by-design approach for the use case.

Main Success Scenario + expected time line
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. *There is currently no expected time line since this is a research prototype.*

Conditions (pre- or post-)
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. *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.*

Performance needs
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.

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

Risks
No legal, business and technical risks related to use case were identified.

Special Requirements

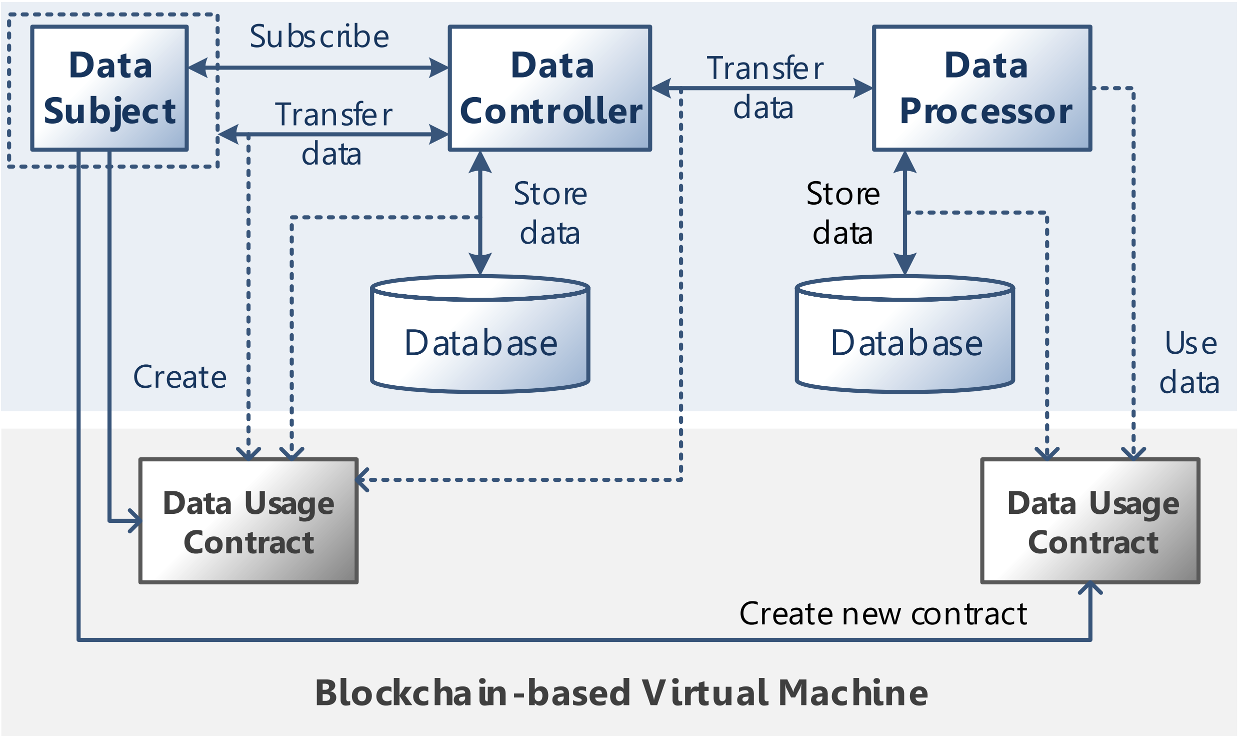
No special business and technical requirements of use case were identified.

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://anonette.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/anonette/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)	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) Goal 9: resilient infrastructure (9.1, 9.3, 9a -c) Goal 11: inclusive and safe settlements and safeguarding of cultural and natural heritage (11.1, 11.3, 11.4, 11a) Goal 13: combat climate change (13.b) Goal 15: sustainable use of terrestrial ecosystems(15.6, 15.9) Goal 16: effective, accountable institutions (16.6, 16.7)		
Value Transfer:	Assets changing ownership	**Number of Users:**	Users registered on the permissioned Hypereldger 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:	The contract includes human actors and external data from Sentinel 2A satellites and online services (Twitter, Weather, Cryptocurrency exchanges). 1. Sentinel 2A data shared over an API service developed for the project (http://anonette.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://anonette.net:3000/explorer/ - only authorized users). 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. 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). 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.		
	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.		

Predicted Outcomes:	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, retails 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 timestampted 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

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-consensyss-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)

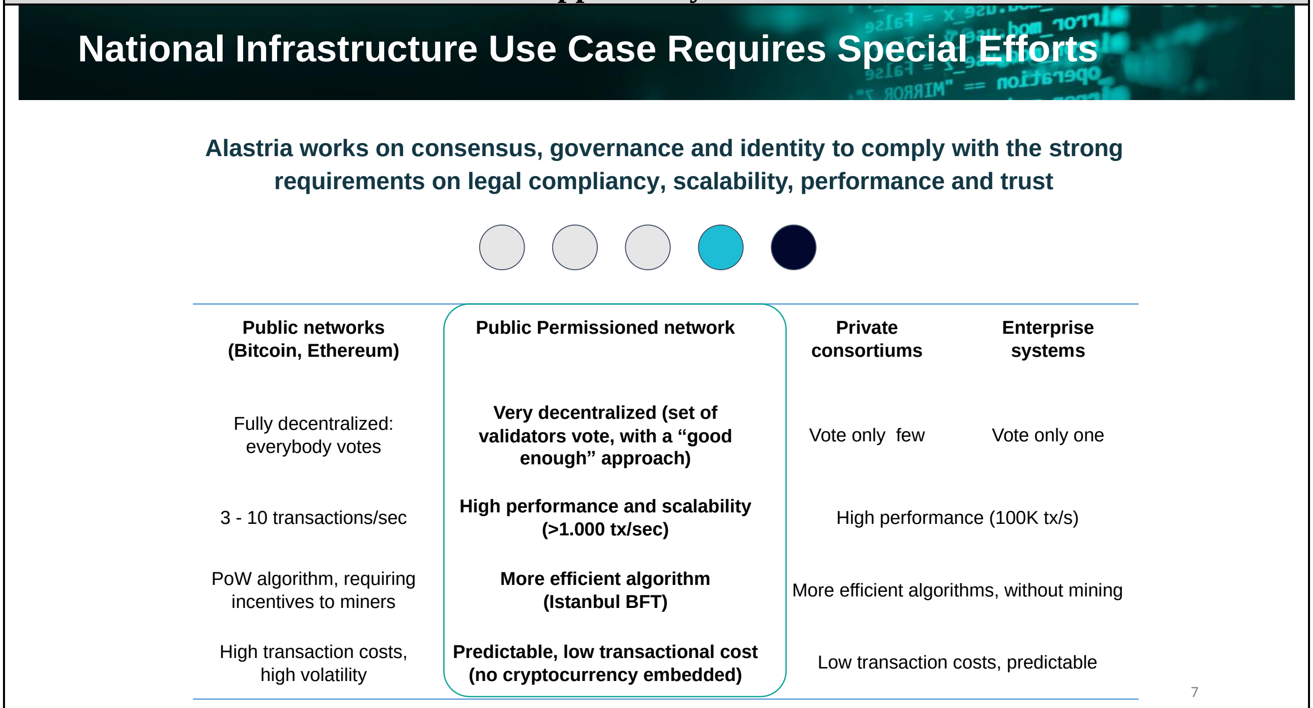
Alastria ID

Section 1: Summary

Use Case Summary			
Use Case ID:	IDM-001	**Use Case Type:**	*Horizontal*
Submission Date:	January 4, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Alastria ID	**Domain:**	*1*
Status of Case	*e.g., Concept, PoC, Pilot, Implementation*	**Sub-Domain**	*Not Applicable*
Contact information of person submitting/ managing the use-case	*Full Name: Ismael Arribas* *Web site:* **https://alastria.io** *standards@alastria.io*		
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	*Thanks to the diversity of its stakeholders and associates, Alastria has granted an infrastructure for Self-Sovereign Identity management. As a network it is dully 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.* *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.*		
SDG in Focus (when applicable)	*SDG3, SDG4, SDG5, SDG6, SDG7, SDG8, SDG11, SDG 13, SDG16, SDG17.*		
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	*As we are proposing a Self-Sovereign Identity-based interconnected Blockchain Platform(s), with the right Governance, all type of users are also stakeholders*
Data:	*https://github.com/alastria/alastria-identity/wiki* *Privacy by design: unlinkable actions.*
Identification:	*Identification mechanism and rules; ability of participants to be anonymous, etc.* 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



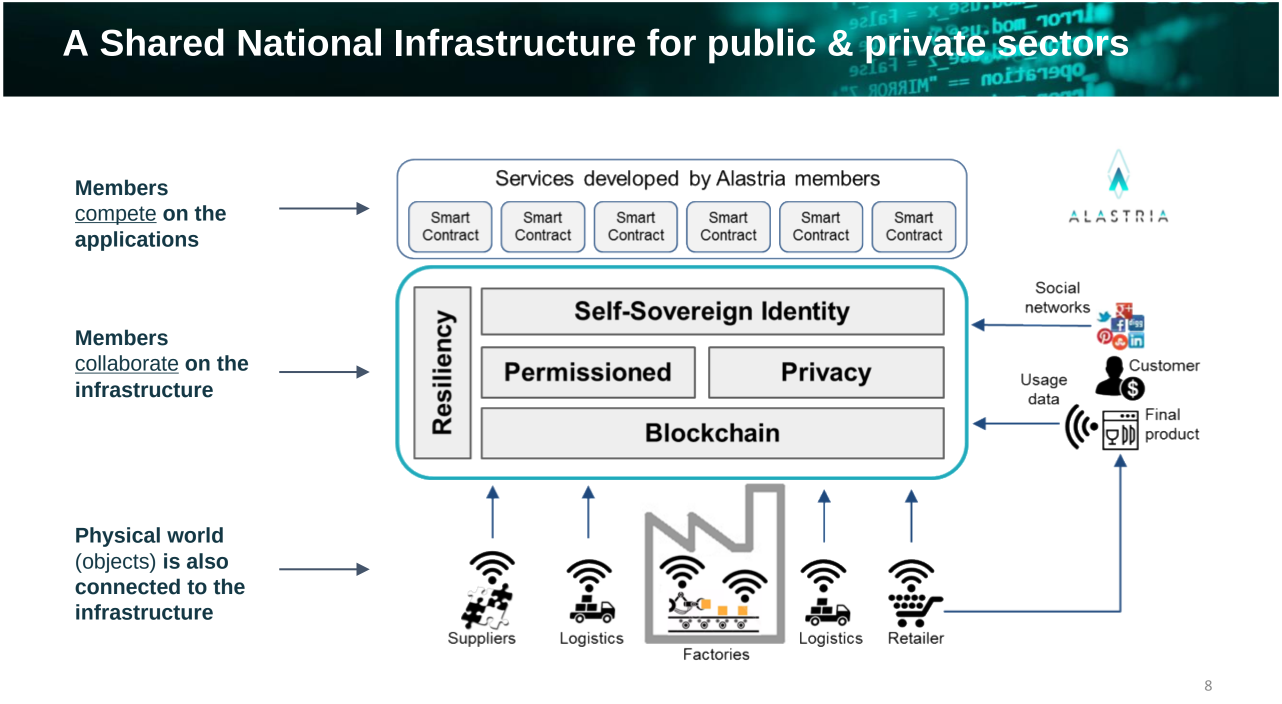
National Infrastructure Use Case Requires Special Efforts

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

Members compete **on the applications**

Members collaborate **on the infrastructure**

Physical world (objects) **is also connected to the infrastructure**

Services developed by Alastria members

Smart Contract | Smart Contract | Smart Contract | Smart Contract | Smart Contract | Smart Contract

Resiliency

Self-Sovereign Identity

Permissioned

Privacy

Blockchain

Social networks

Customer

Usage data

Final product

Suppliers

Logistics

Factories

Logistics

Retailer

ALASTRIA

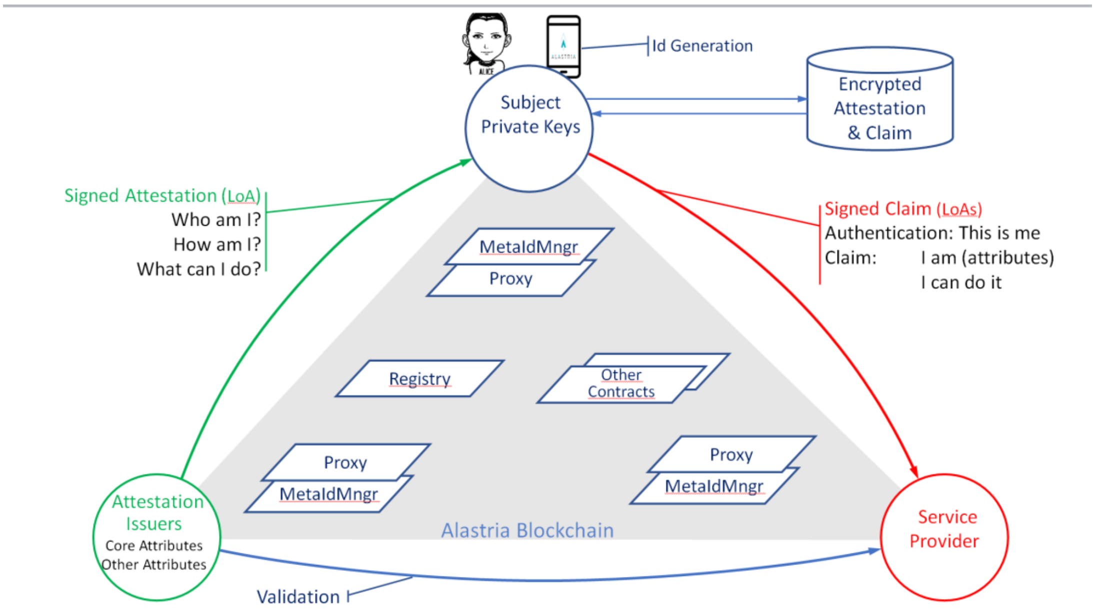
8

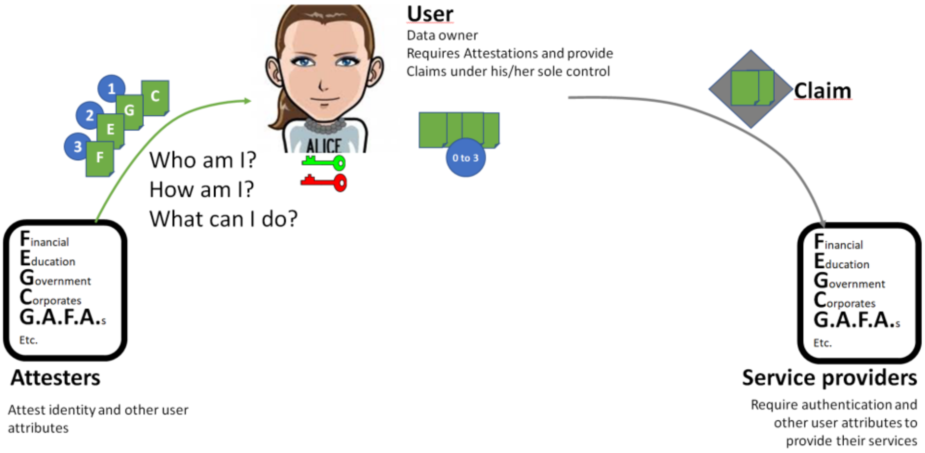
Section 2: Current process

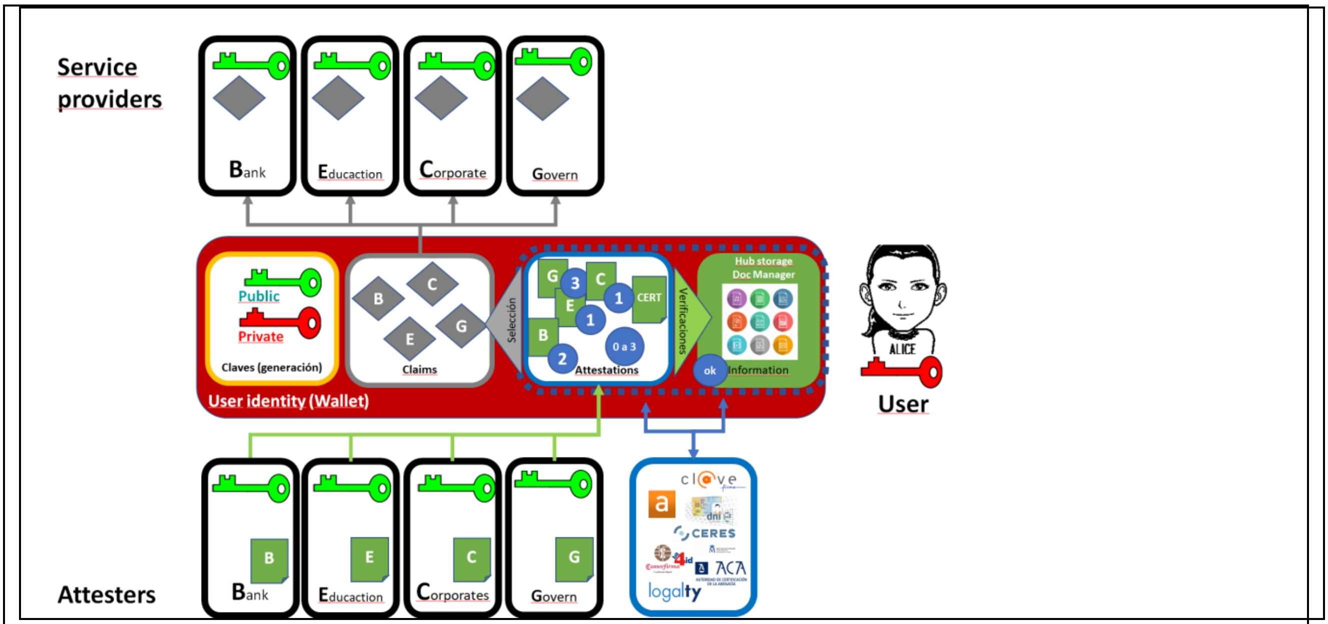
Current Solutions
There are a number of private consortiums and federated ones, but ALASTRIA is moderating the decentralization to a middle point between public and private permissioned infrastructure with all relevant participants for a country or jurisdiction like Public Notary, Corporate Registration 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-verse.

Section 2: Current process

Process scheme (as-is) and ROLES / DATA FLOW







Data and information (as-is)		
Data	**Type**	**Description**
1	*Adhesion*	Normal standard document for being a member of Alastria See https://alastria.io/en/become-a-member/

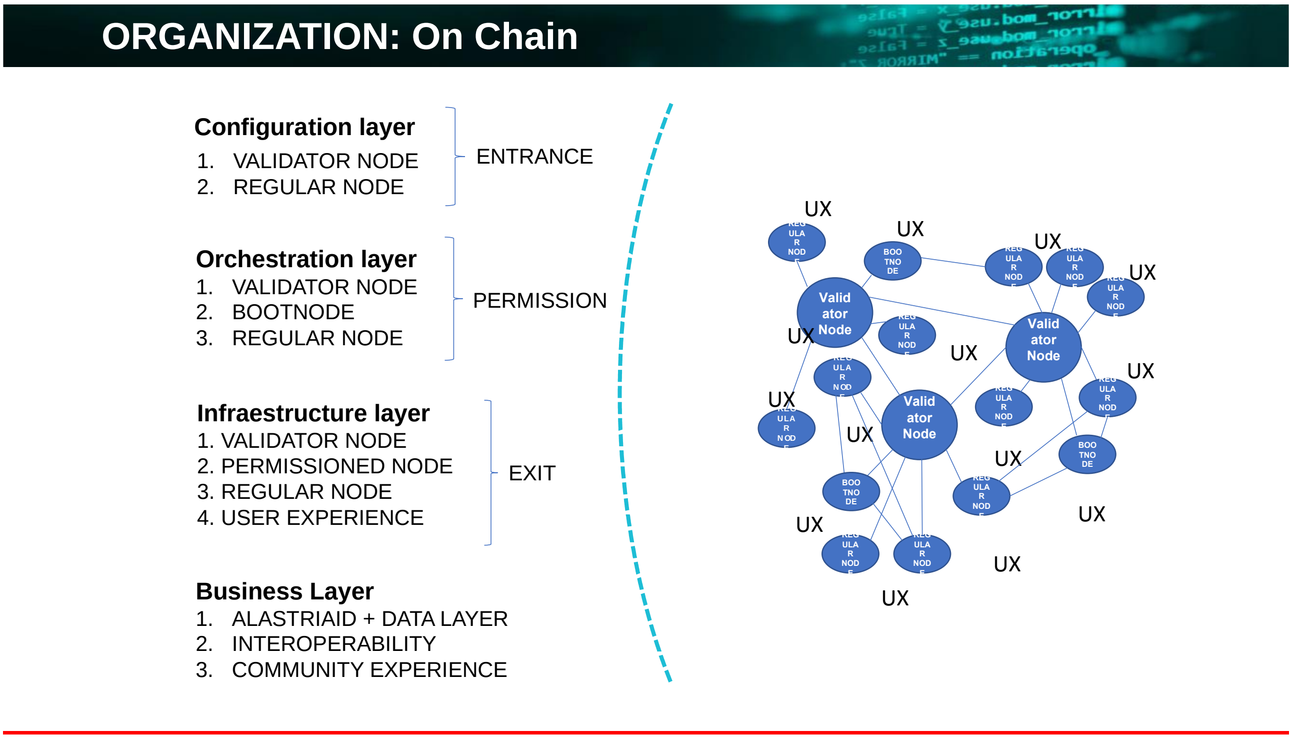
Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Commissions*	Deploy different areas of the infrastructure, technological area, resilience area, trust framework area, standards, sustainability area, risk and cybersecurity processing.
2	*Committees*	Coordination and Implementation 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.

Process scheme (to-be)



ORGANIZATION: On Chain

Configuration layer
1. VALIDATOR NODE
2. REGULAR NODE

ENTRANCE

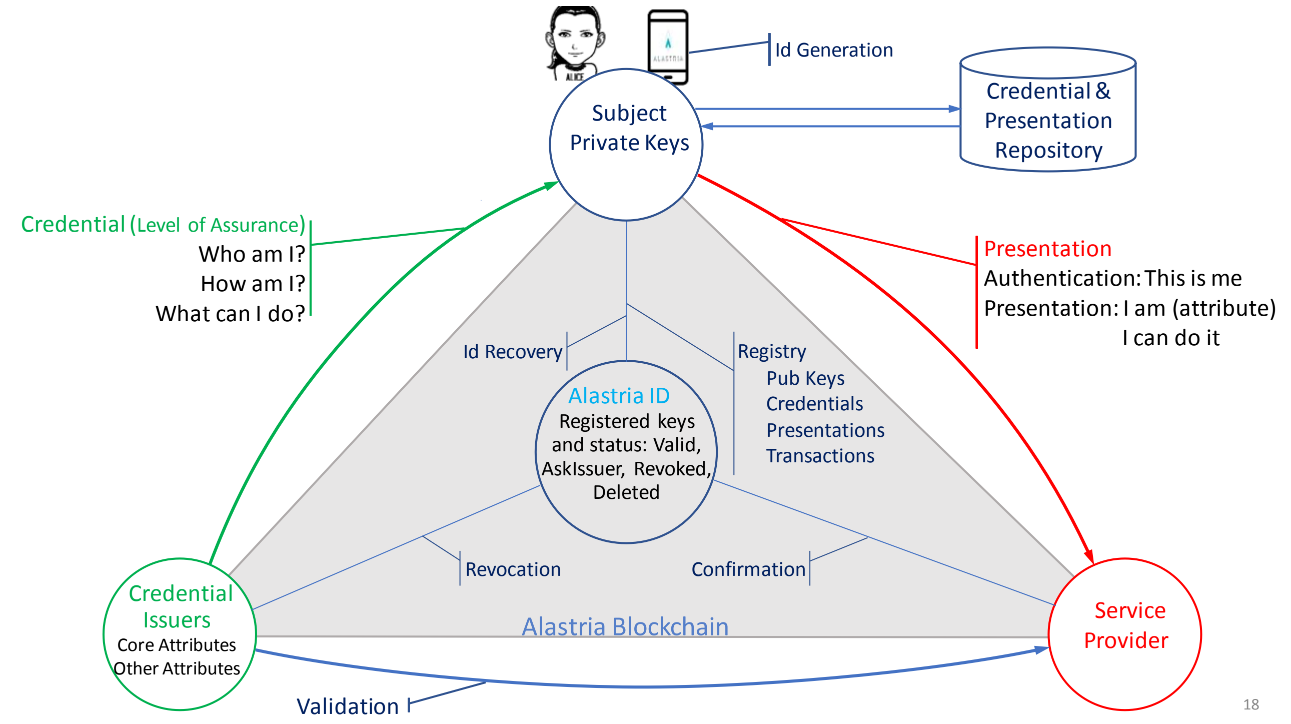
Orchestration layer
1. VALIDATOR NODE
2. BOOTNODE
3. REGULAR NODE

PERMISSION

Infraestructure layer
1. VALIDATOR NODE
2. PERMISSIONED NODE
3. REGULAR NODE
4. USER EXPERIENCE

EXIT

Business Layer
1. ALASTRIAID + DATA LAYER
2. INTEROPERABILITY
3. COMMUNITY EXPERIENCE



Id Generation

Subject
Private Keys

Credential &
Presentation
Repository

Credential (Level of Assurance)
Who am I?
How am I?
What can I do?

Presentation
Authentication: This is me
Presentation: I am (attribute)
I can do it

Id Recovery

Registry
Pub Keys
Credentials
Presentations
Transactions

Alastria ID
Registered keys
and status: Valid,
AskIssuer, Revoked,
Deleted

Revocation

Confirmation

Credential
Issuers
Core Attributes
Other Attributes

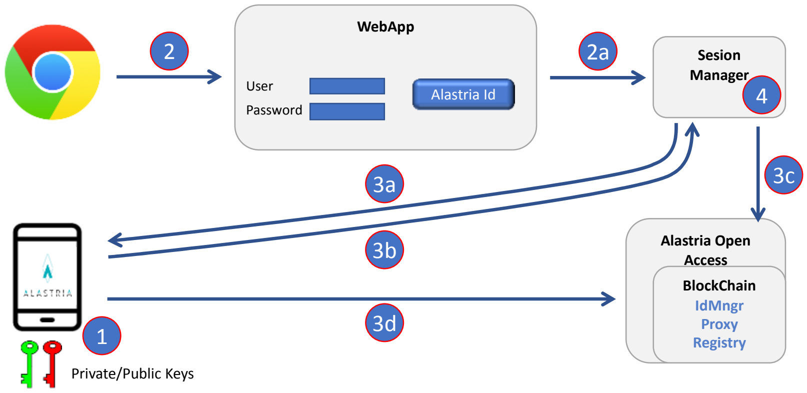
Alastria Blockchain

Service
Provider

Validation

18

AlastriaId Generation



2

WebApp

User

Password

Alastria Id

2a

Sesion
Manager

4

3a

3b

3c

3d

Alastria Open
Access

BlockChain
IdMngr
Proxy
Registry

1

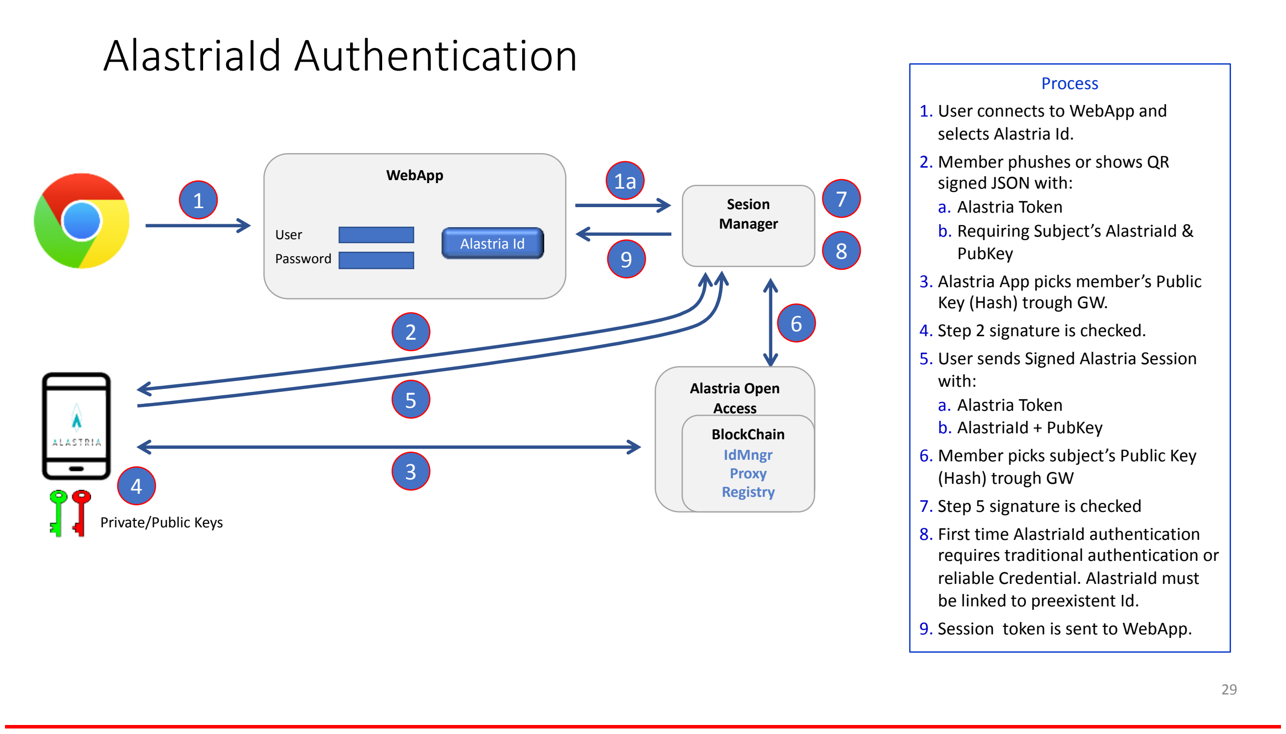
Private/Public Keys

Process

1. Private/Public Key generation on Subject's device
2. Authentication by the current member WebApp.
3. Alastria Id set-up
   a. Members Pushes or shows QR
      i. JSON Alastria Token (AT)
      ii. Requiring KPub
   b. Subject sends signed AT and waits SetUpAlastriaId Event
   c. Member calls setUpAlastriaId
      From: Member
      To: MetaIdentityManager.
      Function: SetUpId (PubKey)
      Returns: AlastriaId
   d. At SetUpAlastriaId Event
      Subject calls CreateAlastriaId
      From: Subject
      To: MetaIdentityManager.
      Function: CreateId (PubKey)
      Returns: AlastriaId
4. At CreatedIdentity Event
   Member links AlstriaId to Subject preexistent Id on its systems.

28

Process scheme (to-be)



AlastriaId Authentication

Process

1. User connects to WebApp and selects Alastria Id.
2. Member phushes or shows QR signed JSON with:
   a. Alastria Token
   b. Requiring Subject's AlastriaId & PubKey
3. Alastria App picks member's Public Key (Hash) trough GW.
4. Step 2 signature is checked.
5. User sends Signed Alastria Session with:
   a. Alastria Token
   b. AlastriaId + PubKey
6. Member picks subject's Public Key (Hash) trough GW
7. Step 5 signature is checked
8. First time AlastriaId authentication requires traditional authentication or reliable Credential. AlastriaId must be linked to preexistent Id.
9. Session token is sent to WebApp.

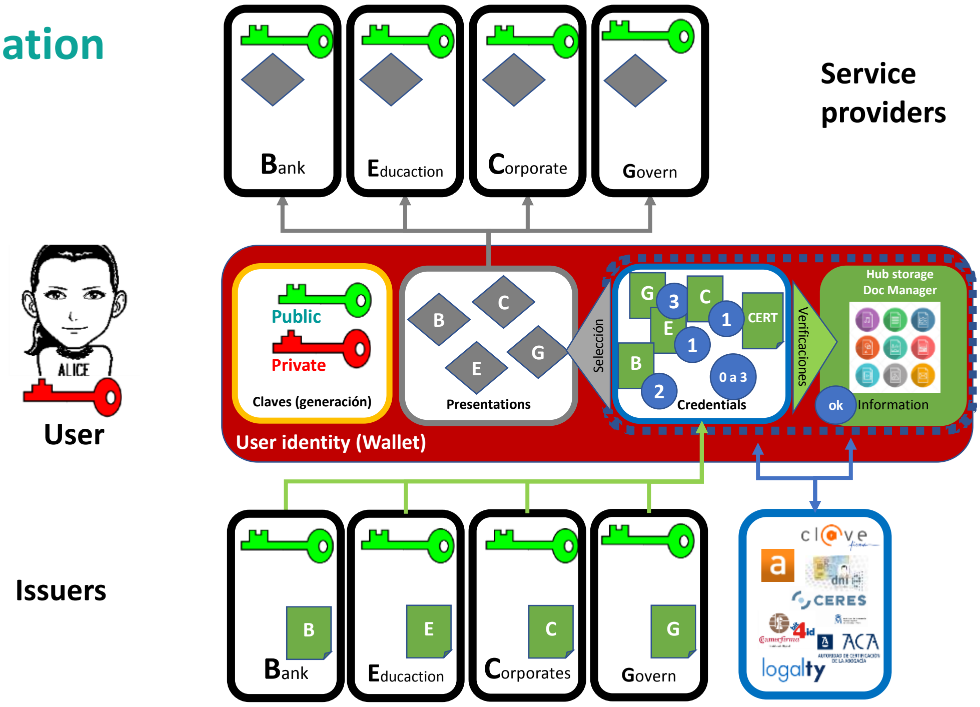
29

Participants and their roles

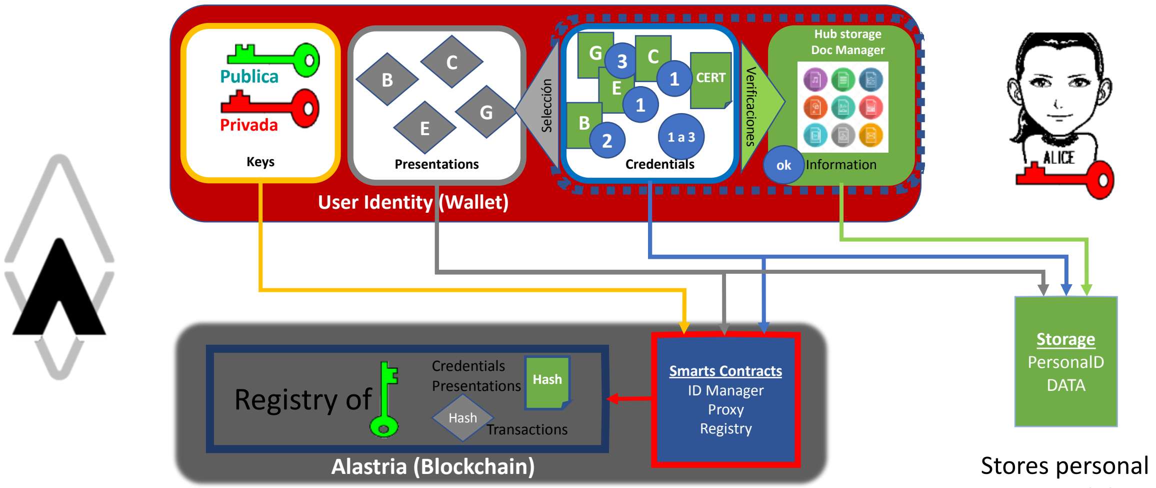
Actor	Type/Role	Description
1	*User*	ID generation
2.	*Credential Issuer*	Attributes and other events.
3.	*Service Provider*	Trust anchoring.
4.	*AlastriaID*	Registry, Recovery, Revocation, Confirmation, Deletion.

Data and information

Information



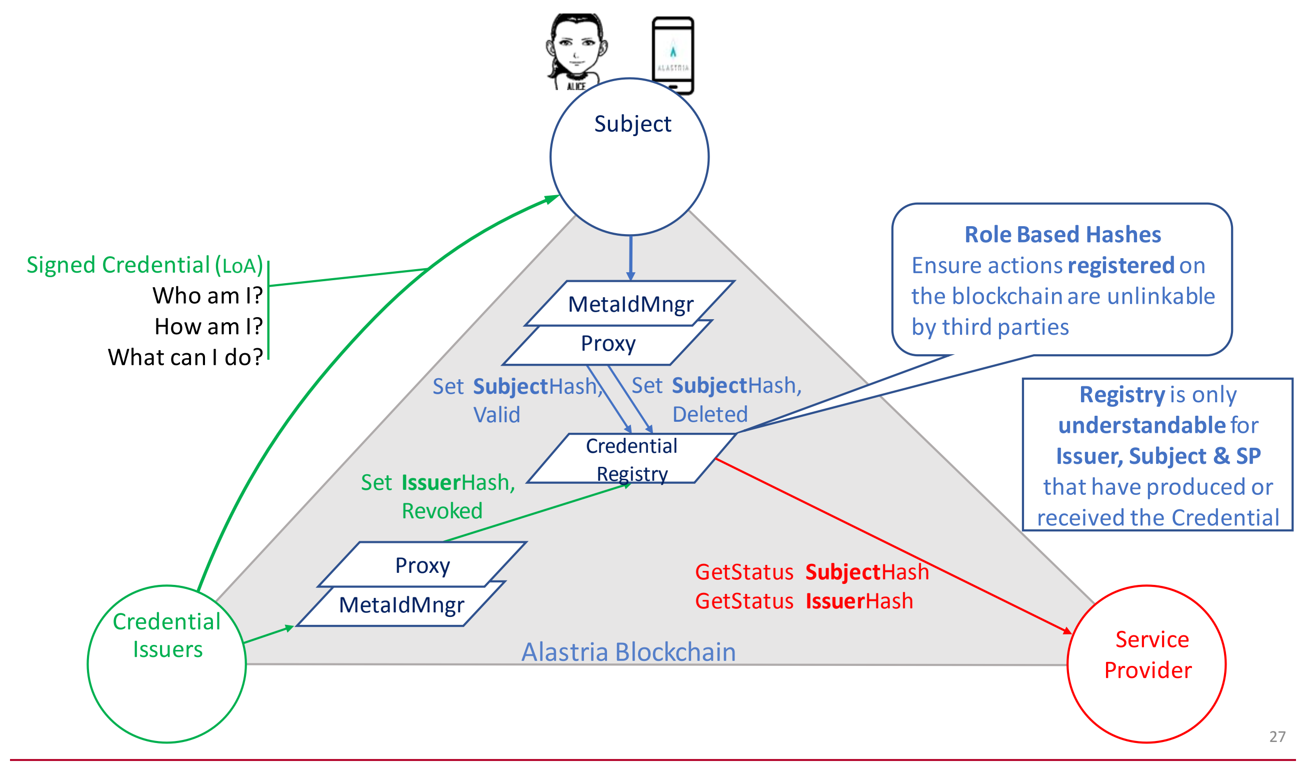
Information repositories



Stores personal encrypted data

Records evidences (hashes) never real personal data

Security and privacy



Subject

MetaIdMngr

Proxy

Set **Subject**Hash, Valid

Set **Subject**Hash, Deleted

Credential Registry

Signed Credential (LoA)
Who am I?
How am I?
What can I do?

Role Based Hashes
Ensure actions **registered** on the blockchain are unlinkable by third parties

Registry is only **understandable** for **Issuer, Subject & SP** that have produced or received the Credential

Set **Issuer**Hash, Revoked

Proxy

MetaIdMngr

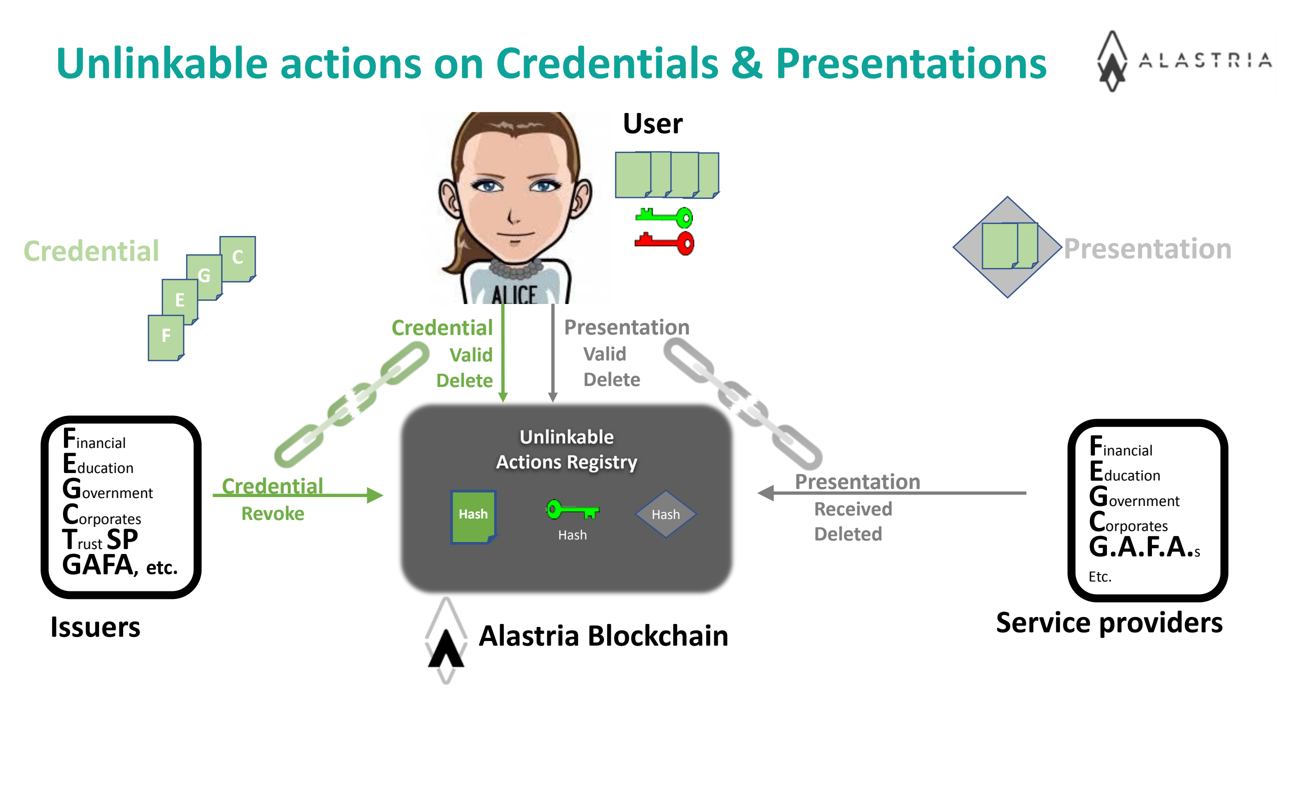
GetStatus **Subject**Hash
GetStatus **Issuer**Hash

Credential Issuers

Alastria Blockchain

Service Provider

27



Unlinkable actions on Credentials & Presentations

ALASTRIA

User

Credential

Presentation

Credential
Valid
Delete

Presentation
Valid
Delete

Financial
Education
Government
Corporates
Trust **SP**
GAFA, etc.

Credential
Revoke

Unlinkable
Actions Registry

Hash

Hash

Hash

Presentation
Received
Deleted

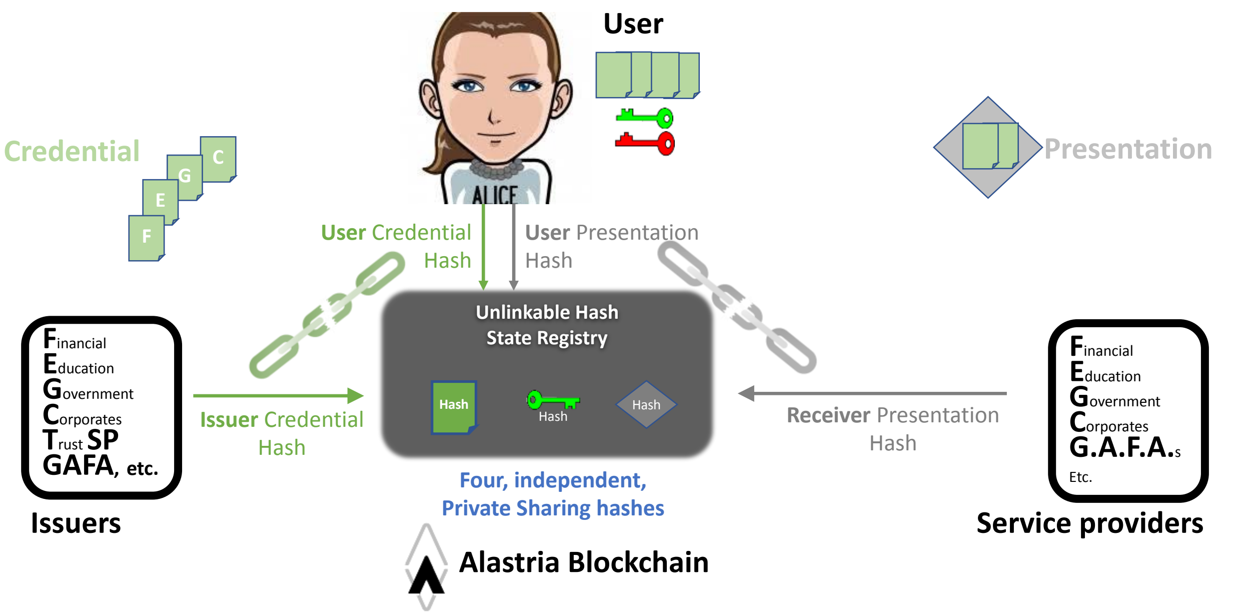
Financial
Education
Government
Corporates
G.A.F.A.s
Etc.

Issuers

Alastria Blockchain

Service providers

Privacy by design: *Private Sharing Multi hashes*



User

Credential

Presentation

User Credential Hash

User Presentation Hash

Unlinkable Hash State Registry

Financial
Education
Government
Corporates
Trust SP
GAFA, etc.

Issuers

Issuer Credential Hash

Receiver Presentation Hash

Financial
Education
Government
Corporates
G.A.F.A.s
Etc.

Service providers

Four, independent, Private Sharing hashes

Alastria Blockchain

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
Currently private users need to visit office of organization with identity documents, such as passport, driving license, social security, etc. *Each organization providing online identification for their customers have to re-implement corresponded software platform and take care about fraud data.*

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.		

Process scheme (as-is)

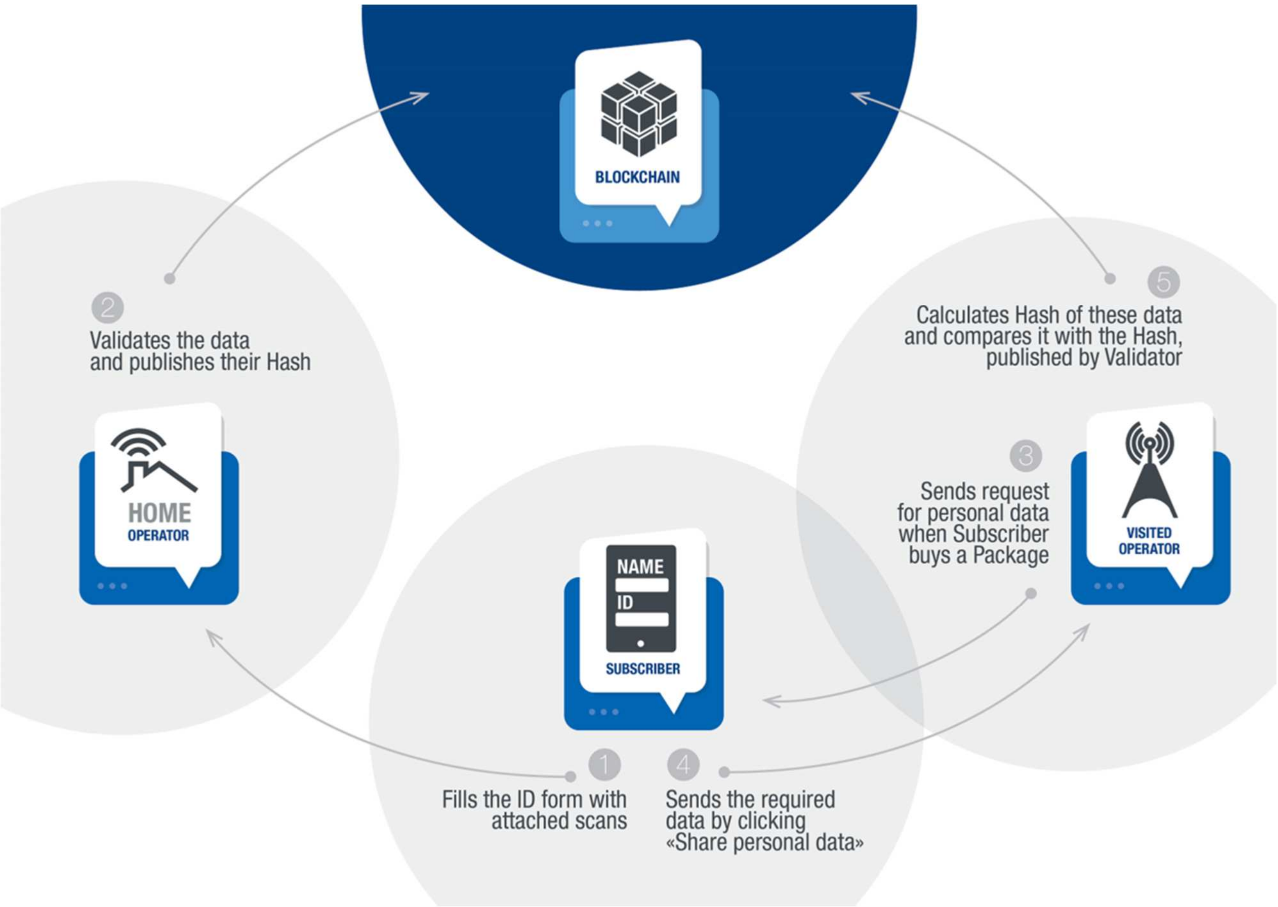
Data and information (as-is)		
Data	**Type**	**Description**
1		

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.

Process scheme (to-be)
 BLOCKCHAIN 2 Validates the data and publishes their Hash HOME OPERATOR 5 Calculates Hash of these data and compares it with the Hash, published by Validator 3 Sends request for personal data when Subscriber buys a Package VISITED OPERATOR NAME ID SUBSCRIBER 1 Fills the ID form with attached scans 4 Sends the required data by clicking «Share personal data»

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Subscriber*	Subscriber of mobile service, who needs to identify himself.
2	*Home operator*	Mobile operator hosting Subscriber in his native country (or other authorized organization), which can identify Subscriber and verify identity information.
3	*Visited operator*	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	*Documents*	Scans of passport and any other documents which customer may be requested to present. 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.

Data and information		
Data	**Type**	**Description**
2.	*ID file*	A collection of documents stored in a special file at customer's smartphone.
3.	*Hash*	Digital hash of ID file transmitted via blockchain by home operator to make identification status available to other participants.

Security and privacy

1. Identity status (hash of ID file) is protected by digital signature of home operator within corresponded transaction within DLT system

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

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.

Conditions (pre- or post-)

n/a

Performance needs

Although not strictly required, fast transactions (within a few seconds) are desirable to distribute identity status among participants.

Legal considerations

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.

Risks

n/a

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:**	*Vertical/Horizontal*
Submission Date:	January 4, 2019	**Is Use Case supporting SDGs**	*Yes/no*
Use Case Title:	Decentral Identification – Using human factors and a social graph to bootstrap ID.	**Domain:**	*4-B*
Status of Case	*PoC, to be improved with use of Quorum*	**Sub-Domain**	*1*
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	**Self-sovereign ID.** Using a social bootstrapping mechanism (using a plurality of attestations) allow humans to self-initialize identification. This aids in identification of displaced people/refugees. Once ID layer is initialized; allow additional attestations for education, professional certifications, or other relevant social data points.		
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:	*Government actors, NGOs, aid organizations, health professionals, educators.*		
Stakeholders	*Displaced humans, new immigrants*		
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		

	identity. This IDs “trueness” is improved with attestations from humans within the social graph. Public/Private key’s that cannot be lost because they are tied to human factors that don’t change (Iris, heartbeat, and possibly DNA) Basic attestations (Name, Height, Weight, Eye color, Country of Origin) Immunization / Health attestations Professional attestations (education)
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
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.
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 me moved to public networks.

Section 2: Current process

Current Solutions
We are unaware of systems to do this at present.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.		
2.		

Process scheme (as-is)

Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	
2	*Payment transactions*	

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

Other Notes
Any assumptions, issues

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	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	*Users*	Humans who want to be IDd
2	*Educators*	Participants in system, who can attest to truth
3	*Aid Organizations*	Participants in system, who can attest to truth

Data and information		
Data	**Type**	**Description**
1	*Documents*	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 moble 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

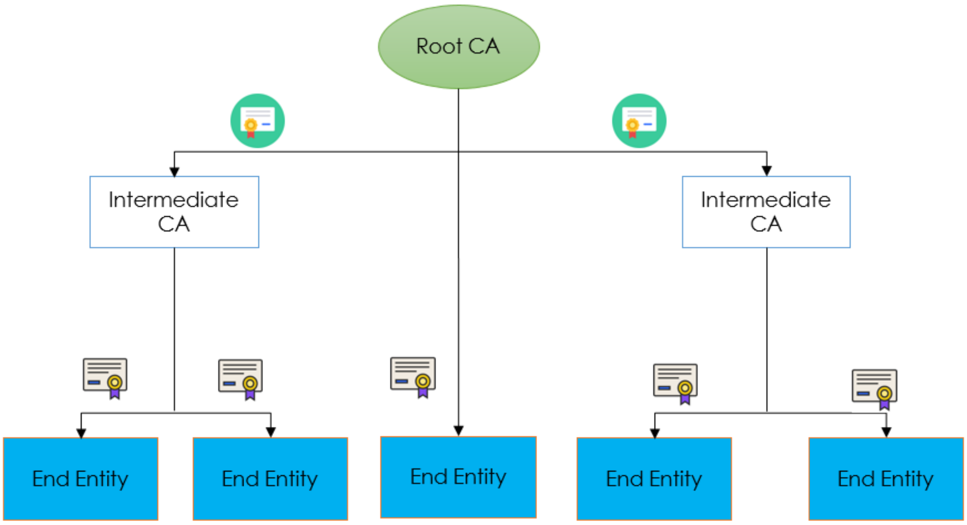
Any assumptions, issues

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**	*Yes*
		Domain:	Security Management
Status of Case	Proof of Concept	**Sub-Domain**	Public Key Infrastructure
Contact information of person submitting/ managing the use-case	*Xinpeng Wei* *Bingyang Liu*	*wexinpeng@huawei.com* *liubingyang@huawei.com*	
Proposing Organization	*Huawei*		
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	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. 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. By using DLT, a decentralized PKI system can be built without highly centralized root CA, and avoid the single point of failure problem.		
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	**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.  Root CA Intermediate CA Intermediate CA End Entity End Entity End Entity End Entity End Entity 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.

<u>Section 2 Current process</u>

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.

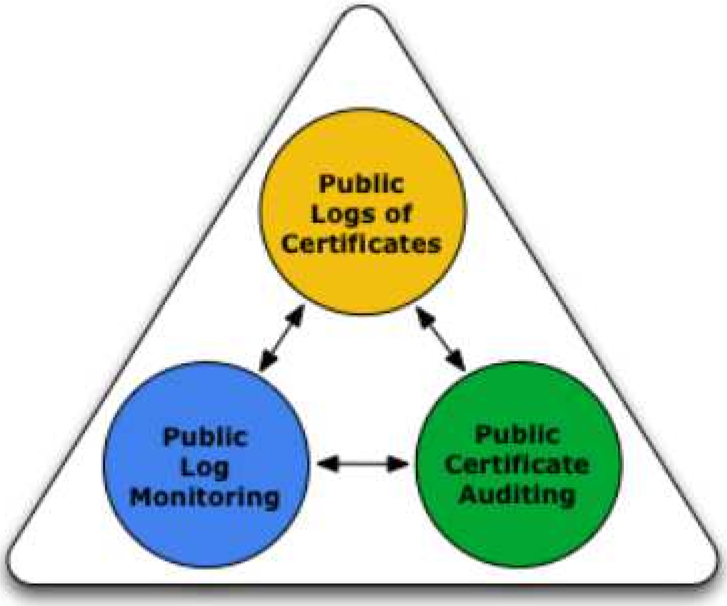
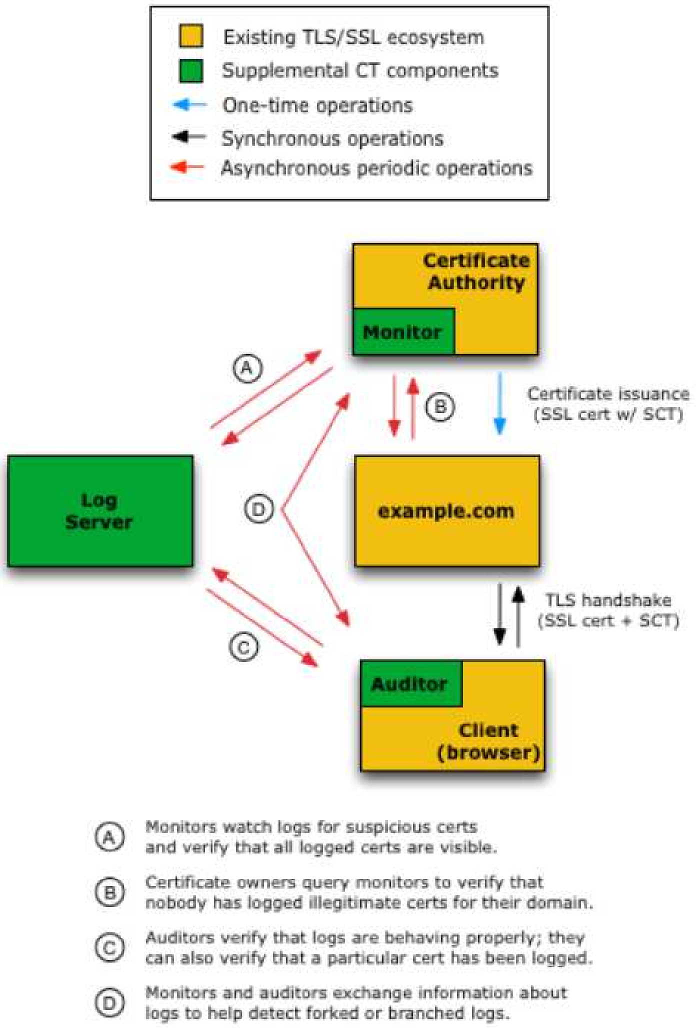


Figure 2: Basic Components of Certificate Transparency[1]

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

Process scheme (as-is)


🟧 Existing TLS/SSL ecosystem
🟩 Supplemental CT components
One-time operations
Synchronous operations
Asynchronous periodic operations
Certificate Authority
Monitor
A
B
Certificate issuance (SSL cert w/ SCT)
Log Server
D
example.com
TLS handshake (SSL cert + SCT)
C
Auditor
Client (browser)

Ⓐ Monitors watch logs for suspicious certs and verify that all logged certs are visible.

Ⓑ Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.

Ⓒ Auditors verify that logs are behaving properly; they can also verify that a particular cert has been logged.

Ⓓ Monitors and auditors exchange information about logs to help detect forked or branched logs.

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.

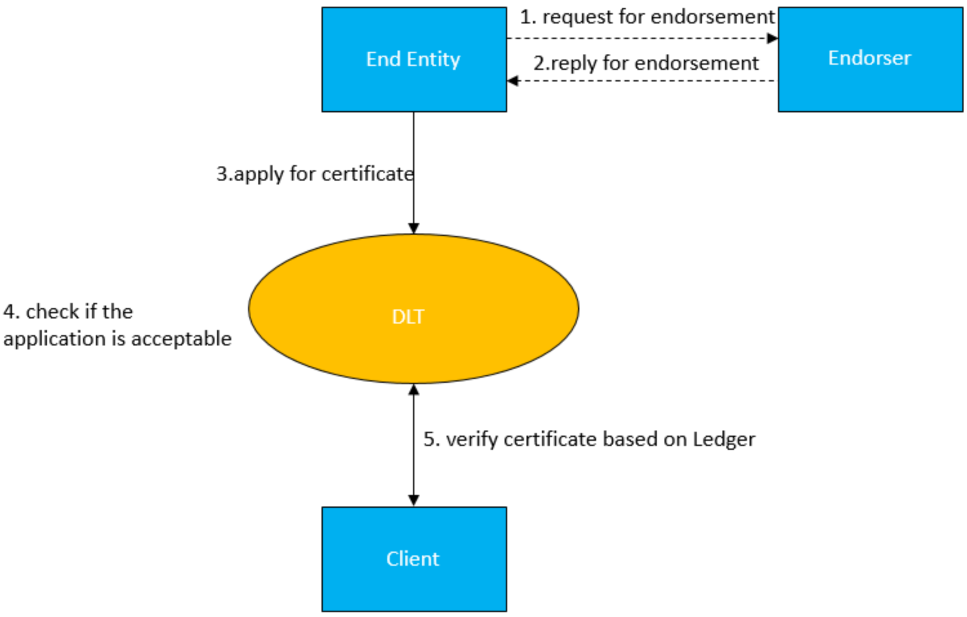

End Entity
1. request for endorsement
2.reply for endorsement
Endorser
3.apply for certificate
4. check if the application is acceptable
DLT
5. verify certificate based on Ledger
Client

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)