TECHNICAL REPORT

ISO/TR 3242

First edition
2022-10

Blockchain and distributed ledger technologies – Use cases

Reference number
ISO/TR 3242:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides a selection of use cases to illustrate a spectrum of applications of distributed ledger technologies including the blockchain (hereafter referred to as DLT). The use cases reflect various international domains, business and industry sectors and processes.

The use cases help to identify actual and potential applications of the technology in the given context, along with relevant requirements, options, benefits, and risk mitigation strategies.

The framework of this document enables this approach by providing a perspective of use cases that goes beyond the traditional vertical sectors or DLT attributes. This document provides assessment across five different categories to provide technology, market and social perspectives. The visualisation of user flows and architecture enables a broader perspective of the role of a DLT as part of on-ledger and off ledger ecosystems. By assessing current DLT implementations, these use cases provide learnings that apply to governance, compliance, interoperability, cross-border regulations, and scalability.

The open innovation approach to use cases can contribute to accelerating the implementation of these new technologies and help reduce the instance of duplication or repeated solution development. This bridge of new information and existing standards can also inform innovators and SMEs to adopt a standards-based approach to build the future of DLT, especially where new decentralised business models apply for example in areas such as financial technology (fintech) and the energy sector.

This document is arranged in three sections for easy reference and comparison.

Clauses 4, 5, and 6 describe the approach, process and criteria of use case selection and study. This provides a guide to the template structure and five key categories that draw out the impact of DLT attributes across transversal (related technologies), horizontal (attributes), vertical (sector specific), United Nations Sustainable development goals (SDGs) and status (from pilot to implementation stages). The use cases each have a set of visualizations that provide further detail of DLT activity as well as the relationship to the user and technology ecosystem. The diagrams include data flow models, a reference architecture from a single node view, and behavioural UML. As such, the template and diagrams provide a detailed insight into the individual use case.

Clause 7 provides commentary on the trends identified in the use case. This provides analysis of categories and DLT types in the use cases. Examples include the clusters of DLT the adoption of hybrid or new DLT and the use of open source[1].

Clauses 8, 9, 10, and 11 provide the detailed use cases reflecting the digital marketplace, arranging them in the template format for easy comparison. The combination of categories and commentary in this document is designed to help readers reference the relevant classification to their sector as well as discover transferable attributes from other categories that can be applied to their DLT requirements.

The work on this document started with identifying the key themes which have the most DLT activity and inviting use cases in these sectors. This resulted in a first set of sector clusters including Fintech, Supply Chains, Data Provenance and Energy.

Blockchain and distributed ledger technologies – Use cases

1 Scope

This document lists use cases that summarise common capabilities and usage patterns for attributes of distributed ledger technologies including the blockchain in order to help standards and technology development. This document includes use cases reflecting a range of industry sectors, processes and specific applications.

This document can inform decision-makers considering or involved in applying these new technologies, including business, academia, government, technical and standards bodies.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22739, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
hybrid
both a private (e.g. consortium) blockchain for internal business use and a public blockchain to publish information of public interest (e.g. certification attainment)

4 Use case processes

The use case collection methodology was broad-ranging. A global call for use case contributions was made. Use case authors submitted use cases to a use case repository and from that collection, the set of use cases contained in this document was selected.

A blockchain/DLT use case template was created to ensure conformance and facilitate comparison across use case application domains and contexts. The use case template applied here includes descriptive text and visualisation formats and applies a System View representation of the Blockchain and DLT Reference Architecture specified in ISO 23257[3].

Given the application domain of blockchain and DLT use cases, where business and enterprise aspects including tokenisation and autonomous governance can be facilitated on-chain, it is considered important that use case descriptions elaborate both business and technical information.

In this way the document provides a comparative analysis of 22 international use cases to better communicate:

— transferable blockchain attributes across vertical and horizontal domains

- infrastructures that support emerging decentralised business models
- detailed views of on-chain and off-chain DLT data flows

Figure 1 outlines this use case preparation workflow.

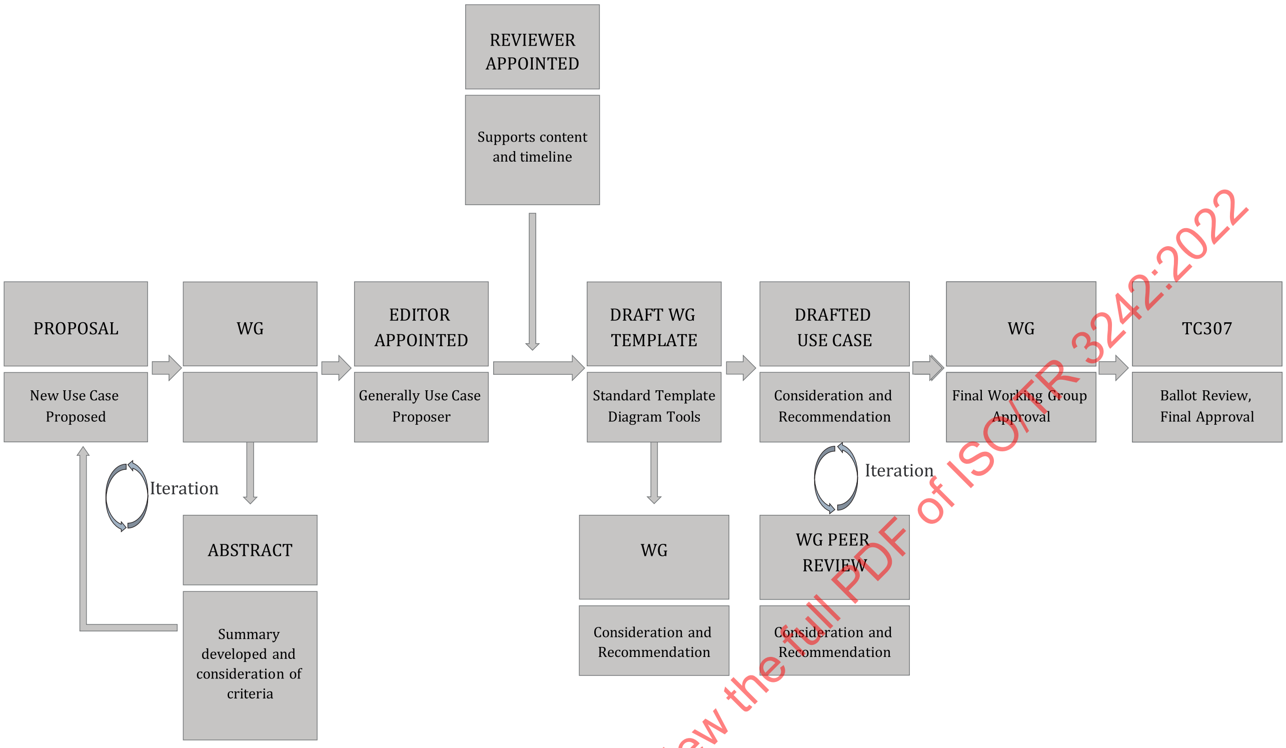

REVIEWER APPOINTED
Supports content and timeline
PROPOSAL
New Use Case Proposed
WG
EDITOR APPOINTED
Generally Use Case Proposer
DRAFT WG TEMPLATE
Standard Template Diagram Tools
DRAFTED USE CASE
Consideration and Recommendation
WG
Final Working Group Approval
TC307
Ballot Review, Final Approval
Iteration
ABSTRACT
Summary developed and consideration of criteria
WG
Consideration and Recommendation
Iteration
WG PEER REVIEW
Consideration and Recommendation

Figure 1 — Use case process and review flow

5 Template development

5.1 General

To provide a standard criterion for analysis, a comprehensive template was created that draws together attributes of each use case in a way that enables comparison and review. The template includes five sections that explore the distinct roles of blockchain/DLT in each use case:

- Title
- Categories
- Summary
- User Requirements
  - Functional Requirements
  - Visualizations
    - Reference Architecture
    - Data Flow Model
    - Behavioural UML
- Force Field Analysis[4]

5.2 Functional Requirements

The use case functions are visualised through a series of diagrams that include user models, data flows and system architecture.

There is also reference to smart contracts, security, identity and privacy management, open-source software and non-functional requirements.

5.3 System architecture

This is a Lab Project which analyses the system architecture to identify stakeholder interaction and data flows using a reference architecture described in Figure 2 that describes a DLT network application from the perspective of Node A connected to a blockchain network. This architecture derives from the modular Reference Architecture System View described in ISO 23257[3] and has been applied to all the use cases in this document. Common kinds of interfaces including external interfaces and intersystem interfaces are included as well as the APIs including both user and admin ones.

The functional components of the system architecture are grouped and outlined as follows:

- **DLT Nodes**
- **Application systems:** for administration and for users, providing end-user capabilities and capabilities for administration and management of the DLT system respectively. Use case authors specify the functional models for both systems to illustrate the services enabled by the solution.
- **Non-DLT systems:** off-chain code, the DLT oracles, the non-DLT applications and off-ledger data are presented and specified based on the actual use case situation.
- **Other DLT systems:** include the separate DLT systems that interoperate with the DLT system.
- **Multi-layer functions:** one or more of the multi-layer function components could be included as per use case actual situation, such as development, the management and operations, security and governance and compliance.

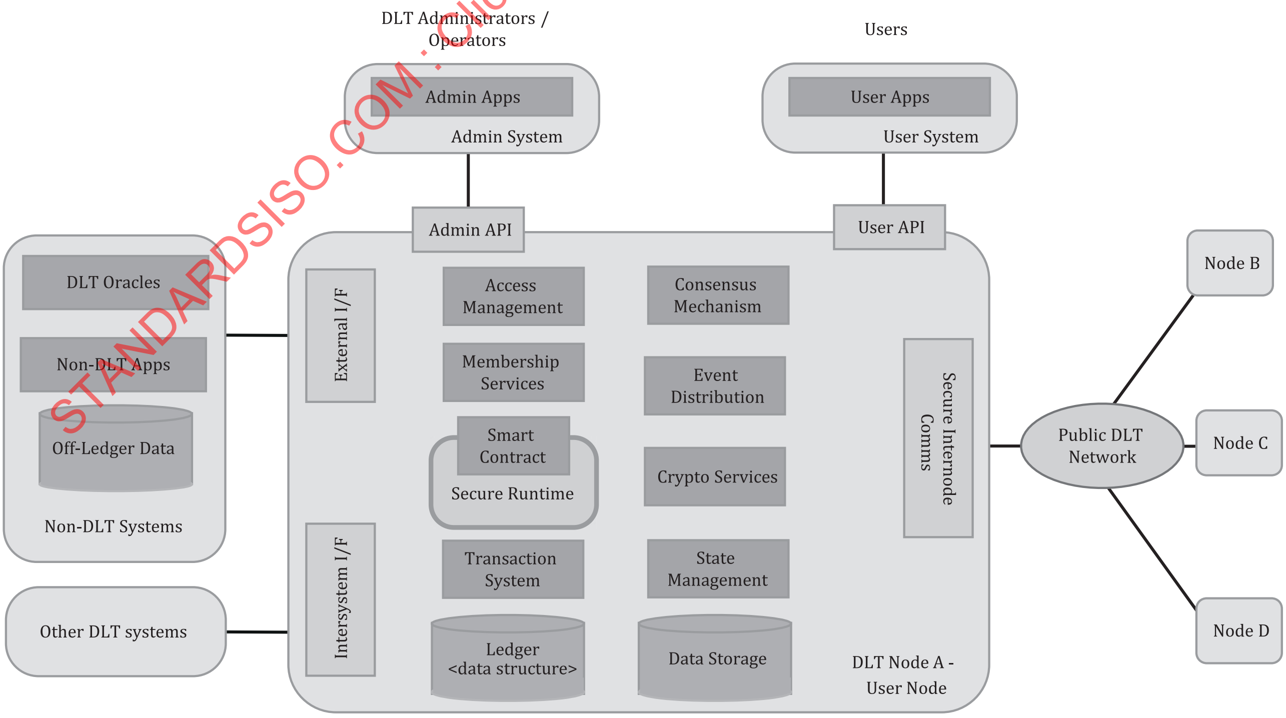


Figure 2 — Reference Architecture System View (ISO 23257 [3])

5.4 Data Flows

DLT Stakeholder roles:

The purpose of the DLT data flow diagram is to identify which data flows are triggered by the data-related operations of stakeholders, between system components that belong to or are associated with them.

DLT data can usefully be classified according to its source as shown in Figures 3 and 4. The sources identified here align with the six DLT roles (ISO 23257[3]) identified as DLT administrators, users, providers, developers, governors and auditors. Among these, administrators, users and providers are the most relevant roles to use case definition. Stakeholders achieve their aims by means of role-based interactions with the DLT system.

NOTE The treatment of off-ledger data is similar to that of other information technology systems. However, a ledger is immutable, which makes identifying transparency and privacy objectives important.

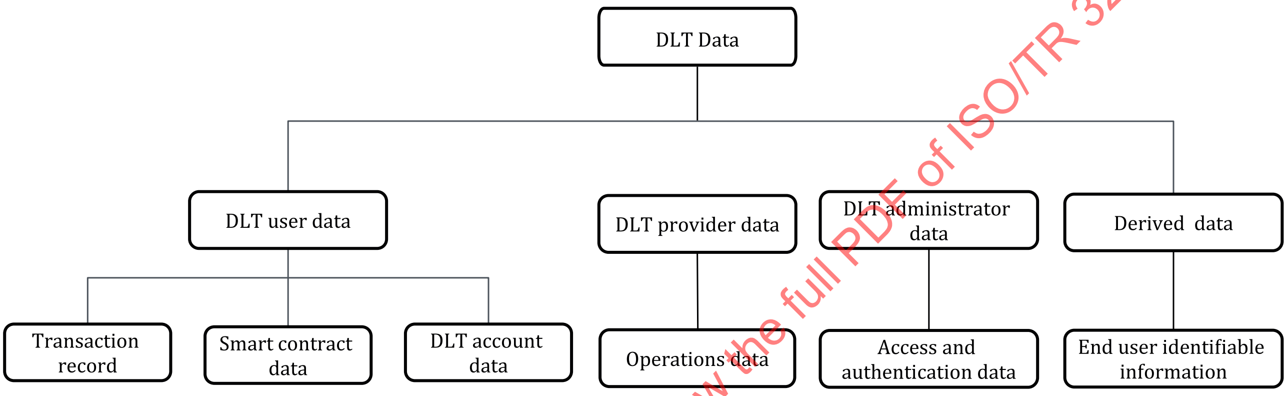


Figure 3 — Data categories from the data source perspective

System data flows:

The purpose of this data flow analysis diagram is to demonstrate a system-wide data flow, and identify which data flows are triggered by the data-related operations of which stakeholders.

a) Specify the role of each stakeholder in facilitating the data flow.

b) Identify the type of data flow (See categories A to D and Z below)

c) Identify the data location: on- or off-ledger.

There are five fundamental DLT data flows. (See Figure 4) Categories A to D are important for understanding a use case.

A: between 2 separate DLT systems when they interoperate.

B: between a DLT system and non-DLT systems connected to it.

C: between administration applications and a DLT system.

D: between user applications and a DLT system.

Z: within and between the nodes of the DLT system.

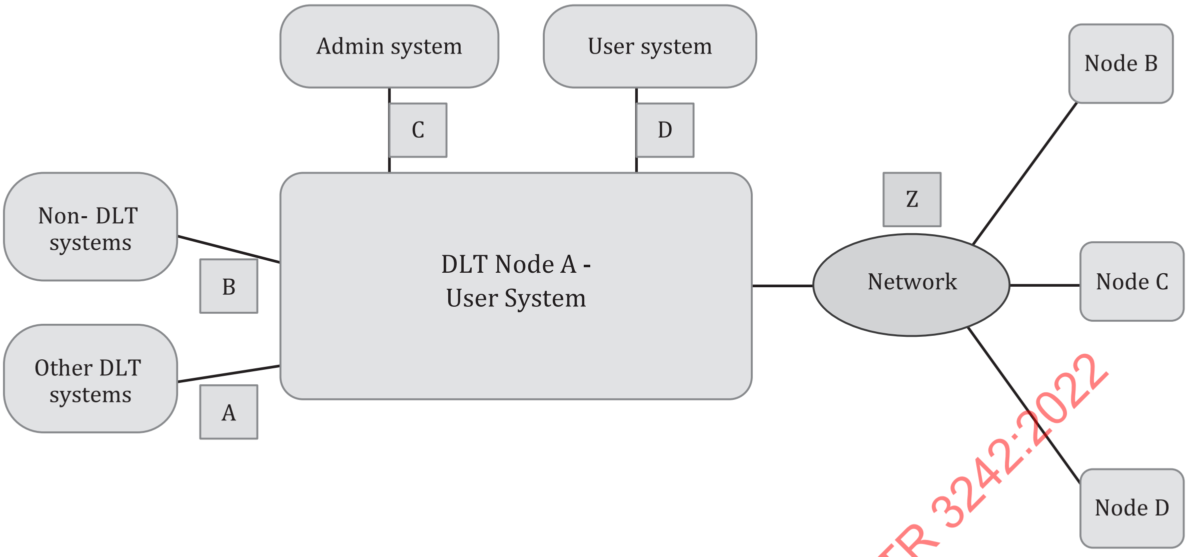


Figure 4 — DLT Data Flow diagram

5.5 Use Case Models

The purpose of a Universal Modelling Language (UML) behavioural model is to illustrate user and system interactions, as shown in Figures 5 and 6, and to provide greater detail about user aims and actions in the system and how these are achieved.

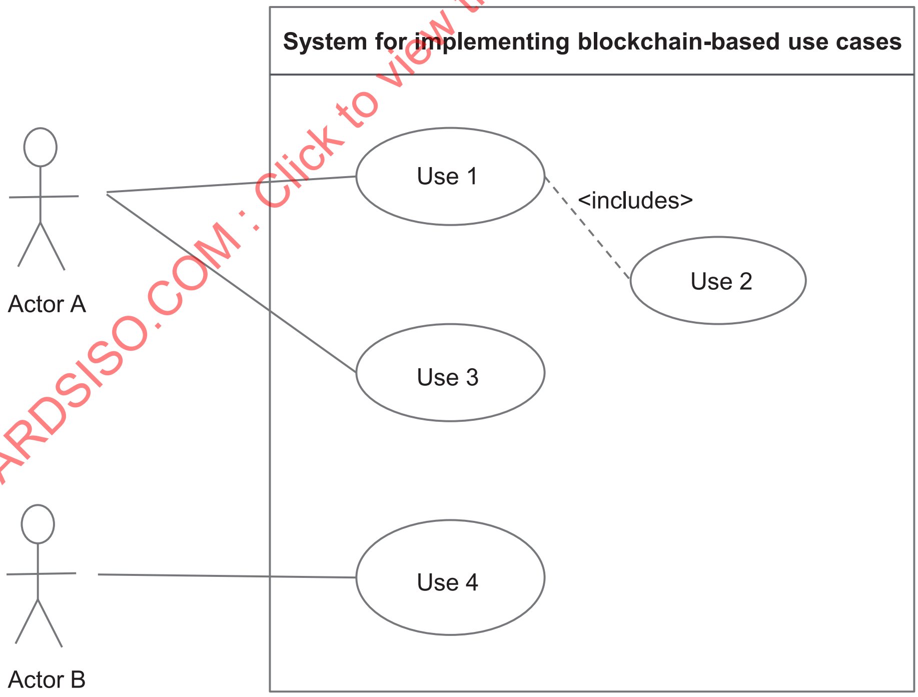


Figure 5 — Simple use case diagram

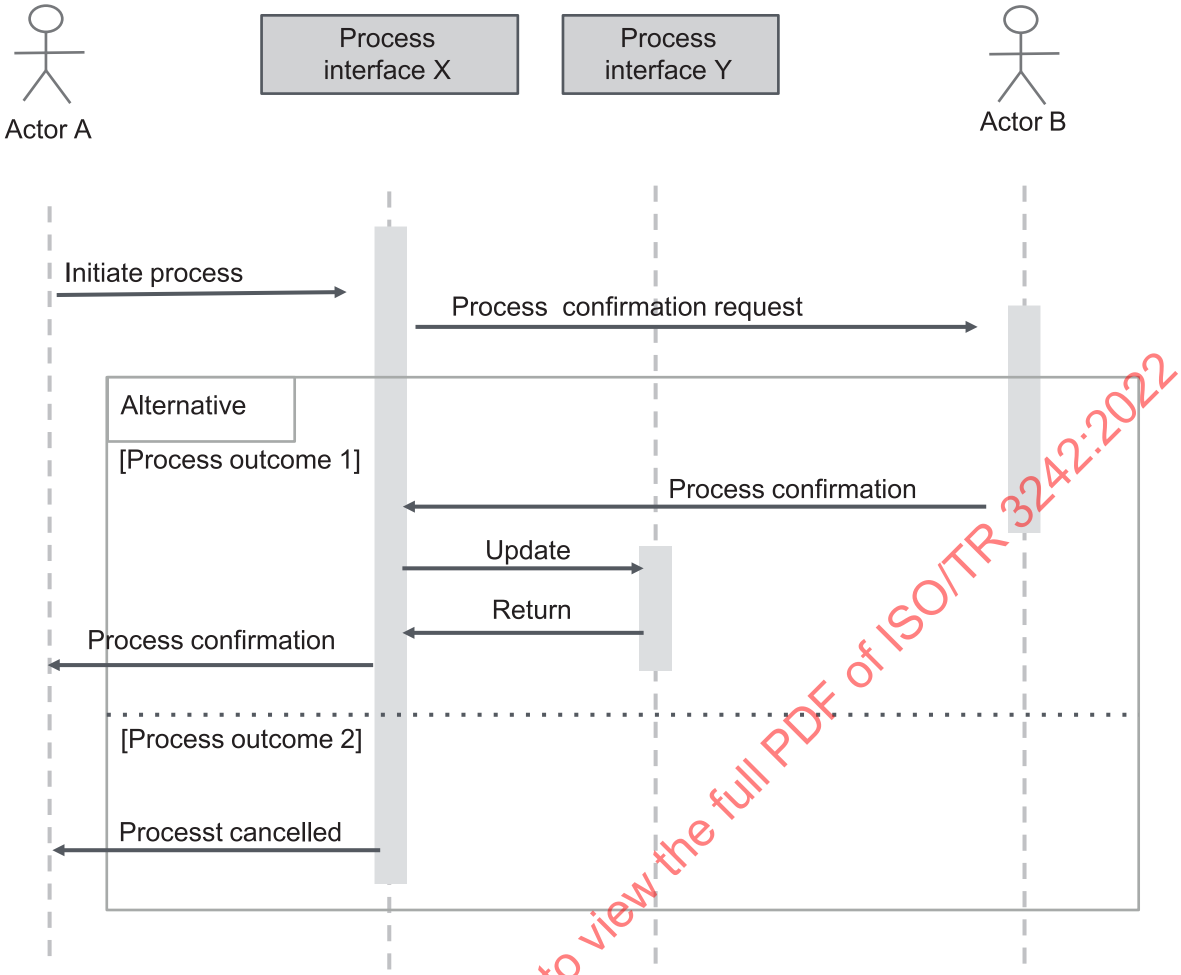


Figure 6 — Example sequence diagram

5.6 Categories

To provide a standard criterion for analysis, a comprehensive template methodology was created that includes five categories of applications. These categories are selected so that this document can usefully be referenced and incorporated into other research, analysis and standardization. These are:

— Transversal (related technologies).

— Horizontal (attributes).

— Vertical (sector specific).

— United Nations Sustainable development goals (SDGs).

— Status (classified across a spectrum of technical development phases).

This document includes commentary of the use cases and insights into these categories in Clause 7. An example of the use case template is in Annex A.

5.7 Category: Transversal

The transversal category considers related technologies and is derived from the EU Information and Communications Technology (ICT) Standardisation Rolling Plan[5].

This category reflects the ‘Key enablers and security’ section of the EU ICT Rolling Plan which includes:

a) Cloud computing.

b) Public sector information and open data.

c) Internet of Things.

d) Cybersecurity / network and information security.

e) Electronic identification, trust services, e-signatures.

f) e-Privacy.

g) e-Infrastructures for research.

h) Accessibility of ICT products and services.

i) Artificial Intelligence.

j) 5G.

k) Broadband infrastructure mapping

5.8 Category: Horizontal

The horizontal category reflects cross-sector applications and attributes from a market-based, business analysis approach and uses terms commonly used in the current DLT ecosystem.

This category derives from consideration of ISO/TS 23258[6] leading to insights in taxonomic and ontological descriptions. Both are deemed valid approaches and by referencing both approaches it is understood that valuable insights into the DLT ecosystem as a whole are gained.

a) Identity Management
   - Rights and Identity Management, Identification.

b) Data Provenance
   - Disintermediation in Production, Actions Traceability

c) Governance
   - Collaboration, Decision Making, Structuration

d) Cryptocurrency and asset exchange
   - Electronic Payment, Cryptocurrency and Token Exchange

e) Process Optimisation
   - Intellectual Property Protection, Certification.

f) Automation
   - Contract Management, Automation.

This document includes commentary and insights into these categories in Clause 7.

5.9 Category: Vertical

The purpose of the vertical classification in the use case template is to facilitate discovery and research of economic activity by end-users of this document. For this reason, the UN ISIC economic activity classification system is chosen whereby:

“ISIC is a basic tool for studying economic phenomena, fostering international comparability of data, providing guidance for the development of national classifications and for promoting the development of sound national statistical systems.”[7].

An example of a use case classification of ISIC vertical categorisation[8] is provided below:

- Use case Title, ISIC classification: International Waste Transportation Management, E-3821
- Section: E Water supply; sewerage, waste management and remediation activities
- Division: 38 Waste collection, treatment and disposal activities; materials recovery
- Group: 382 Waste treatment and disposal
- Class: 3821 Treatment and disposal of non-hazardous waste.

5.10 Category: sustainable development goals

The sustainable development goals (SDG) category supports the ISO initiative to support the attainment of United Nations SDG goals[9].

The SDGs[10] are listed as:

- GOAL 1: No Poverty
- GOAL 2: Zero Hunger
- GOAL 3: Good Health and Well-being
- GOAL 4: Quality Education
- GOAL 5: Gender Equality
- GOAL 6: Clean Water and Sanitation
- GOAL 7: Affordable and Clean Energy
- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 10: Reduced Inequality
- GOAL 11: Sustainable Cities and Communities
- GOAL 12: Responsible Consumption and Production
- GOAL 13: Climate Action
- GOAL 14: Life below Water
- GOAL 15: Life on Land
- GOAL 16: Peace and Justice Strong Institutions
- GOAL 17: Partnerships to achieve the Goal

5.11 Category: status of use case

The ‘Status’ category reflects the stages of a use case, from initial concept to integration, and adoption within a community. In this way, use cases reflect the changing objectives from hypothesis to pilot, implementation and learnings phases of a typical technology development process. The Status categories in this document are:

a) a “thought experiment”.

b) approved but not implemented.

c) in development or pre-production.

d) in trial or pilot.

e) in production/live implementation.

f) a completed trial or pilot.

g) a failed trial/pilot/implementation.

h) an integration with current systems.

i) something else (please describe).

5.12 Category: Other use case classifications

The use case template features other classifications including smart contracts, security, identity and privacy management, open-source software and non-functional requirements.

Use cases also provide force field analysis of legal, risk, relevant existing standards and other information including consideration of the role of open source software.

Open Source[1]

The use cases reflect their use of Open Source software as well as “open” and “private” DLT implementation. This enables infrastructure developers to monitor the current community activity and assess options for their own software choices. This also informs implementation partners of current common usage patterns, which can assist governance and risk management strategies by demonstrating which open source trends are adopted in the market.

The Template includes two perspectives of open source adoption:

Open Source scenarios:

a) Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.

b) Reference implementation (to show that a specification is implementable).

c) Required part of a standardization deliverable.

d) Complementary to a standardization deliverable.

e) Test suites, unit tests, etc. for functionality tests.

f) Other.

Open Source engagement:

a) Although the engagement wasn't successful it is important to continue.

b) Has evaluated/studied how to make meaningful use of Open Source Software.

c) Engagements showed that Open Source Software is not the right tool to solve the relevant needs.

d) Open Source Software is critical for a successful adoption.

e) The engagement was successful but there is uncertainty on how to continue.

f) It was easy to collaborate with Open Source Software communities

g) It was difficult to collaborate with Open Source Software communities.

h) Open Source Software is critical for validation of implementations.

i) Other (specify) .

This document includes insights from use cases preference for open source.

6 Use case list and abstracts

6.1 Data Provenance

Data Accountability (European Commission)

Short description:

Smart contracts can be used for data accountability and provenance tracking (e.g. privacy preferences), and to allow data controllers and processors to verify if they have the rights to use this data (e.g. redistribution).

Keywords: Data provenance, accountability tracking.

Abstract:

Users (data subjects) in current systems are unaware of how their data is used by data controllers and processors. In case of data misuse, for example when receiving an undesired e-mail message, they have no mechanisms to verify that their privacy preferences were respected.

A public DLT can be adopted to enable a solution where users declare, using smart contracts, how their data is used (privacy preferences), and to allow data controllers and processors to verify if they have the rights to use that data. In this use case, smart contracts store hashes of the data exchanged by the user with data controllers and processors as well as the rule-based privacy preferences.

These rules are in a blockchain executable format that governs how the data exchanged can be used by these entities. Hashes are resilient against dictionary attacks and allow data subjects to request proofs during audits or whenever there is a reason to believe data is being misused by data controllers or processors.

Property Records Management (India)

Short description:

Applying blockchain for provenance of property ownership and tracking of the property records, using the blockchain-based Property Record Management System (PRMS). This use case highlights how time-sequenced and tamper-evident storage of property details and transactions helped in overcoming the shortcomings of the existing system.

Keywords: Property Management, DLT

Abstract:

The blockchain based PRMS stores property registration transaction details in the blockchain in time sequenced fashion. Seller details can be verified from the blockchain before generating the checkslip which is one of the most important activities in the workflow of registration application. It would help the buyer and the authorities to get an affirmation of the ownership of the property. This solution would help to curb issues related to double selling, registrations based on fake documents and it would also be resistant towards internal attacks. This use case also helps to give a reliable encumbrance search of the property details without manual intervention.

As multiple departments are involved in the property document registration, blockchain based Property Record Management System helps to maintain a shared ledger providing the single source of truth for the property details and thus building a trust across known and untrusted entities with the distributed, tamper evident and append only database enabling verification of transactions.

Sub-Registrar Office (SRO), Revenue and Survey and Settlement Departments are potential stake holders of the system. Additionally, other departments can benefit from this system to obtain tamper evident data from a blockchain ledger.

Student records management system (India)

Short description:

In this use case, the Student Records Management System (SRMS) is using a blockchain to provide a new way of securing and storing student record data and certificates on a blockchain platform, ensuring immutability of records. The objective is to prevent fraud and hacking of student information and develop confidence for all stakeholders for the long term.

Keywords: Certificates fraud, diploma, transcript, degree, education, credential, data sharing

Abstract:

The SRMS provides immutable storage for student academic certificates using a blockchain. This use case solves 2 problems:

a) the problem of student academic records being fraudulently updated in the computer system to benefit someone by malicious players. Any non-blockchain software system is vulnerable to data tampering by malicious system administrators and /or hackers.

b) inconveniences and overheads in data sharing among education institutions, among government departments etc.

The actors are:

a) student,

b) certificate issuing institute & its staff (SSC board)

c) verifier (organizations, institutions interested in authenticity of the certificate where the student has submitted the certificate as supporting document)

Blockchain makes the data immutable (tamper-proof) with its techniques of cumulative hashing and decentralization. Being a DLT it facilitates sharing data among legitimate stakeholders by each of them hosting a node. This use case is being supported by the Indian regional Government of Telangana.

Education Certificate Provenance (Singapore)

Short description:

Provenance of education certificates in Singapore through an open-sourced platform leveraging a public blockchain for notarising education certificates, designed with the intention to reduce education fraud. The platform and framework by OpenCerts provides the ability to verify data provenance from a given certificate, without the need to query the issuing organisation. Data privacy is enforced by only publishing the cryptographic hash on the blockchain. Additionally, privacy controls are made available to the certificate holder to selectively disclose contents of their certificate.

Keywords:

Open Attestation, Ethereum, Education Fraud, IHL: Institute of Higher Learning

Abstract:

Typically, a graduate who presents a certificate is subjected to scrutiny by the receiving party, for example, a prospective employer, who wishes to verify the legitimacy of the certificate contents. Traditionally, the request for verification is submitted to the issuing organisation, e.g. an Institute of Higher Learning (IHL). This requires time and effort to retrieve and verify the certificate from the IHL's system.

Leveraging the Ethereum public blockchain, the OpenCerts platform provides an innovative approach to decentralize the verification of certificates and provided an opportunity to improve.

a) Speed of verification

b) Selective disclosure of information within a certificate

c) Revocation of a certificate post-issuance

d) Costs savings

Content timestamp verification (Netherlands)

Short description:

Online Content Management Systems (CMS) such as Wordpress can apply blockchain to protect copyright of content, proof of the existence at different moments in time and give website visitors the tools to see and verify how content has changed over time and when it was last updated. This results in a more trustworthy internet for all the stakeholders of the published content. The WordPress plugin can be used to manually or automatically sign content to several different blockchains.

Keywords:

WordPress, Timestamp, Blockchain, Usability, Content, Web, Website, Article, Graphics, Authenticity, Integrity, Fraud, Plagiarism, Revisionism, Copyright, Protection, Proof, Verify, Proof of Existence, Infringement

Abstract:

How do consumers know whether the information presented by websites can be trusted, and how can content creators claim ownership over their content? Trust in the internet is declining and website visitors are actively changing their behaviour as a result.[13] This use case addresses the problem of copyright violation, where creative content can be stolen or copied where content creators often don't have proof of ownership.

Content Timestamp Verification contributes to a more trustworthy Internet by offering a tool that a website can use to timestamp content on the blockchain. These content creators obtain indisputable proof of existence at different moments in time to protect their copyright without expensive third parties.

Website visitors can verify when content was last updated and compare different revisions to see how the content has changed over time. By adding the hash (fingerprint) of the content to the blockchain, website visitors can verify what was communicated at what moment in time and when the content was last updated. Similarly, search engines and social media platforms can verify these blockchain timestamps as they are standardized.

Examples of sectors that could benefit from such a solution include:

- Banks are required by law to maintain an archive of what was communicated at which time
- Healthcare providers publish information that matters in decision making

Thus it is possible to hold those providers accountable and citizens need to trust the information published by governments, but cannot verify whether this trust is verified.

The distributed character of blockchain technology takes away the need for website visitors to trust content creators. They can verify it themselves. The history of content is traceable and both the content and transactions are immutable. The 'Wordproof' Timestamp verification is a simple, accessible plugin for the WordPress web-publishing platform to assert creative rights, verify authenticity and make content more transparent.

Self-Sovereign Identity (Cyprus)

Short description:

Self-Sovereign Identity (SSI)[14] is a blockchain-enabled decentralized, distributed identity and data management platform that allows data producers to manage their identity and other personal data.

Keywords:

Cloud computing, public sector information and open data, Electronic identification, trust services, e-signatures, e-Privacy, self-sovereign identity, personal data management, transparency & compliance in data sharing

Abstract:

This use case is a blockchain-enabled decentralized, distributed identity and data management platform that aims to disrupt the international data market, by offering a highly scalable marketplace app service, empowering users to control and capitalize on their data.

Access Control systems such as the Kraud platform in Cyprus is designed to grant control to persons (natural or legal) over their digital identity attributes and personal information in a digital era, where honesty, integrity, transparency, and trustworthiness are paramount.

Enabled through blockchain technology, the purpose is to bring together data providers (natural or legal persons owning data), data consumers (natural or legal persons processing data) and service providers into a common marketplace/network, where data subjects/users can control, share and consume data in a secure, transparent and rewarding manner while guaranteeing control, accountability, and auditability for all stakeholders in the data ecosystem.

In particular, this use case aims to:

- Develop a global network platform where data subjects (including natural and legal persons) can create a cryptographic identity wallet, enabling them to store, manage, verify and validate their own identity data, as well as share and allow processing of such data in a transparent and rewarding manner from data-requesting organizations.
- Provide data analytics and data insight tools to both data producers and consumers, to support decision on data already held by producers (identity data, social media or search engine activities, bank account transactions, electronic health records, insurance records, driving records, personality & psychometric data, etc.).
- Ensure that data within the network are verified and validated through identity verification procedures, by, for instance, governmental and other certified, external validation mechanisms, currently available for identification and verification of data subjects' identity.
- Provide Data Ownership and Control of every processing activity performed within the Kraud Network, ensuring compliance with European and Domestic Data Protection Regulations and Laws (e.g. GDPR[15] & e-Privacy in EU, CCPA in USA, etc.).
- Disrupt the EU and international data economy and market, by offering a highly scalable Marketplace App service supporting millions of users, and various functionalities applicable to different data types made available by data subjects, and useful to primary and secondary data consumers.

6.2 Fintech use cases

Accounts receivable financing system (China)

Short description:

There are three components of the solution, including:

a) APOC for core enterprise;

b) APOS for upstream suppliers and downstream partners;

c) APOB for the bank.

The Blockchain-based platform and smart contracts can collect transactions information in a more secured, efficient and cost-effective way which will facilitate the loan to the enterprise more efficiently as well. The whole process could be automated via a blockchain solution with the following procedures:

a) The core enterprise makes a smart contract and APOC receives the payment information.

b) APOC uploads the information to the blockchain. Then smart contracts automatically enforce obligations, and write the results to the blockchain.

c) The upstream suppliers confirm the contract and apply for their loan from the bank in APOS.

d) The bank checks the information on blockchain and processes the application.

e) After the upstream suppliers finish the production and delivery, they confirm the delivery and ask for payment, all these are uploaded to the blockchain through the platform.

f) The core enterprise confirms the accounts receivable and pays for the contract later.

g) The bank checks the information from the blockchain.

All the events of the loan are uploaded to the blockchain and are validated on the blockchain.

All the parties will be alerted if there are any abnormal transactions.

Keywords: Blockchain, FISCO-BCOS, smart contract, Supply-Chain Finance, core enterprise, upstream supplier, downstream partner

Abstract:

The supply-chain finance includes core enterprise, upstream suppliers, downstream partners and financial institutions such as banks. Small and middle sized partners find difficultly to get bank loans due to a shortage of fixed assets or insufficient credit rating, etc. The banks spend great efforts to review accounts receivable or other collateral that support partner’s loan applications The primary challenges are:

a) Low efficiency: there are many institutions to establish a mutual trust mechanism in the traditional way with banks and with each other, which involves manual processing with high labour costs and low efficiency.

b) High cost: banks have to collect more information to identify if the transaction in the supply chain is true or not. There are high costs for information collection and staff management.

c) High risk: the authenticity of the transaction between enterprise and their partners can be doubtful, and the risk of loan losses is very high.

As the core technology of trusted value networks, blockchain can utilise asymmetric cryptographic algorithms, consensus mechanisms, decentralization, permanency and immutability, to solve the problems mentioned above.

Built on FISCO-BCOS technology, China Digital's Account Receivable Financing System applies blockchain to record the transaction process between core enterprises, upstream suppliers and downstream partners. It records contracts, delivery, etc., which provides sufficient evidence for banks to make credit management for upstream suppliers and downstream partners of core enterprises.

Interbank loan reconciliation and settlement (China)

Short description:

By enabling reconciliation with a distributed ledger, blockchain technology can streamline and reduce the settlement period to T+0 days from the industry average of T+1 to T+2 days. This use case provides Interbank Loan Reconciliation and Settlement based on DLT, which is a live implementation in China.

Keywords:

Reconciliation, DLT, Bank, Efficiency

Abstract:

Today, the traditional reconciliation process between different banks often takes as long as T+1 or T+2 days. This long reconciliation time both creates inefficiencies and can lead to information asymmetry.

By enabling reconciliation with a distributed ledger, blockchain technology can streamline and reduce the settlement period to T+0 days from the industry average of T+1 to T+2 days.

The platform is a pioneering blockchain application for a "distributed business scenario", wherein a high level of interbank operational efficiency, process automation and system reliability are required to ensure cost efficiency and business continuity.

Title: Organized CHIT funds (India)

Short description:

Facilitate reliable access to financial services via ROSCA operations targeting financially excluded citizens. Empower ROSCA operations across the state by decentralizing regulatory activities and making the network of innovative financial offerings more transparent and thus trustworthy for participants.

Keywords:

ROSCAs,[16] Chit Funds,[17] Financial Inclusion, Regulators, Subscribers, Banks, Auditors, Financial Institutions, NBFC, Insurance companies, Brokers, Blockchain, Smart Contracts, DLT, DLTs, Fintech

Abstract:

Access to financial services in India is dependent on many parameters, especially for those with little access to formal institutions such as Banks and NBFCs. This use case focuses on catalysing financial inclusion in India through Organized Chit Funds. Rotating Savings and Credit Associations (ROSCA) / Chit funds are key instruments of financial inclusion in India. They offer simple access to finance for millions of people across India. Many low budget investors are however susceptible to misinformation and fraud.

It is estimated that between 1,2 to 1,4 lakh[1)] crores[2)] of public money is lost to various of ROSCAs / Chit Funds schemes. A total of 350 scams have been reported across 17 states, and 15 crore (approximately 150 million) families, primarily low-budget investors, have been impacted[18].

While Chit funds help people save money for their future needs, regulatory failures can cause millions of people to lose their life-time savings, all the while maintaining continued expectations of high returns.

1) A lakh is a unit in the Indian numbering system equal to one hundred thousand.

2) A crore or koti denotes ten million and is equal to 100 lakh in the Indian numbering system (10 to the power 12).

The aim of this use case is to make investments in ROSCAs / Chit Funds more accessible, credible, reliable and rewarding to subscribers. It will have a significant impact for the financial safety net of low budget investors and ROSCA subscribers. It will directly impact a range of economic, social, livelihood and financial implications of the subscribers.

Title: Transparent securitisation (Italy)

Short description:

Accessible and transparent securitisation via a fully digital and legally binding process based on decentralised technologies and compliant digital identities.

Keywords:

Actor types: Administrator, Users, Providers, Developers, Auditors, Governors

System characteristics: accessible, transparent, cost-effective.

Industry sector: DeFi

Hashtags: #financial_inclusion #trust #digital_transformation #seamless_securitisation

Abstract:

The private debt market is poised for massive digital transformation: it is poorly accessible, opaque, illiquid, and inefficient. There is a need to optimise end-to-end digital securitisation processes, from assets origination to issuance and exchange of asset-backed securities.

The platform involves all the main actors of securitisation, namely Portfolio (PTF) Agents, Suppliers, Servicers, Special Purpose Vehicles (SPVs), Representatives of Noteholders, Investors. It also leverages several external systems: a Registration Authority for Know Your Customer service (KYC), an Anti- Money Laundering service (AML), a Signature flows service provider, a Certification Authority (CA), a Cloud service provider, a Data preservation service, a Custodian of digital securities, and, for notarisation and tokenisation, the Algorand blockchain, a permissionless Pure-Proof-of-Stake blockchain particularly suited for the DeFi industry. This offers several gains shared across the economic system:

- democratic access to capital markets: new and effective financing channel to SMEs and new investment opportunities to investors through fractional ownership and improved supply-demand match;
- democratic information: data related to the performance of the assets backing the securities are handled as a common good, rendered transparent and accessible to everyone preserving privacy and data and financial sovereignty;
- democratic transfer: investors have full control of their assets thanks to a seamless user experience that, together with disintermediation, provides easy and efficient ownership transfer.

Stonize's ultimate goal is to democratise finance and serve the real economy by leveraging its compliance and trusted platform. To this aim, the decentralised approach stimulates participation and network effect of investors and savers, who share information in a privacy-safe ecosystem.

Indeed, citizens are able to co-invest with professional investors, increasing trust in the platform. Leveraging these factors and stimulating the evolution of the regulatory framework of blockchain/tokenisation to foster local economies, the aim is to foster growth across the European Union (EU).

Title: Pension process optimisation (China)

Short description:

Utilizing blockchain technology to optimize pension business processes, including investment transaction, payment and custody.

Keywords:

Blockchain, Consensus Algorithm, Smart Contract, Pension, Hyperchain, Occupational Pension, Client, Trustee, Account Manager, Custodian, Investment Manager.

Abstract:

The pension sector includes occupational pensions, enterprise annuities, and pension insurance. The business processes of pension involves five roles: client, trustee, account manager, custodian and investment manager. The traditional business process faces some challenges:

— Low efficiency. There are many roles and institutions across different industries involved, including insurance, bank, and funds. Establishing a mutual trust mechanism in the traditional way, involves manual processing with high labour costs and low efficiency.

— Long business period. Normally, one business period takes one month to process. Therefore, long business periods result in high communication costs.

— Lack of security mechanism. Most of the data transfer through email and fax without strong data encryption. It is easy to obtain the data and decipher the content.

— Low capital utilization efficiency. The current low business efficiency impacts the net value of the annuity portfolio and the monthly purchase and redemption operations, resulting in a reduction in the waiting time for trustee funds.

— High cost. The existing business model of pensions is limited to the "consensus" among the institutions. The difference in trust has caused an increase in connecting costs.

As the core technology of trusted value networks, blockchain utilises asymmetric cryptographic algorithms, consensus mechanisms, decentralization, permanency and immutability, to solve the problems mentioned above, bringing new opportunities for the development and innovation of pension business.

Blockchain enables a group of parties to maintain a safe, permanent, and tamper-proof digital ledger of transactions, which can evolve over time without a central authority. The application of the blockchain technology allows the institutions to optimize the pension business process, enhance the development of automating pension business, as well as increasing capital utilization, and improving the customer experience.

Title: Decentralized charity platform (the Republic of Korea)

Short description:

This decentralized donation platform was selected by the Ministry of Science and ICT in 2019 as a national project which created an open ecosystem where the general public can easily access donations through micro donations. The entire donation process is not controlled by a specific institution or manager, but provides an infrastructure that can be operated autonomously and reliably by smart contracts.

Keywords:

Decentralization, Micro-donation, Trust, Platform, Donation campaign, Token(Crypto), Economics, Dapp.

Abstract:

The decentralized donation platform based on blockchain, started as a pilot project in April 2019, led by a non-profit organization in the Republic of Korea, and has included more than 3,000 donations, 350 donation campaigns, and more than 150 thousand dollars in donations.

The credibility and transparency of donation organizations have been severely impaired since 2017 as “Donation Phobia” appeared in the Republic of Korea. Despite the economic growth, the percentage of donations continues to fall. With the indifference of donations and a continuous decrease in donation activities, the transparency and credibility of fund management by donor organizations are the most important issue.

The key questions are how to activate a stagnant donation culture and how to ensure the reliability of the donation platform.

To resolve these problems, the blockchain is used as a base technology to achieve three tasks:

— Revitalization of micro donation ecosystem

In addition to the existing donation organizations, various donation campaigns participated, including individuals, consumer groups, start-ups, and open source projects. This Use Case includes an open donation network that can be accessed in a variety of ways, including donation portals, standalone services, and donation buttons. It has been linked to various digital transaction platform such as bank accounts, points, and cards so that anyone can easily participate in donations, and are able to provide an ecommerce service to purchase donated products.

— Establishment of autonomous donation system (based on a smart contract)

To autonomously operate the campaign by donor participants, the token economy-based game theory algorithm (Token Curated Registry) was applied. It is designed to autonomously screen high-quality campaigns by introducing a curation system that allows participants to directly evaluate and reject poor campaigns for each campaign.

— Build a platform with reliability/efficiency

For the smart contract-based blockchain network to have a stable operation, this use case secured platform stability and traffic performance based on the POA consensus algorithm and sidechain. In addition, in order to securely link donation tokens and fiat currencies, transaction details are recorded on the blockchain through each participant's wallet, and the movement of assets through a validator is verified.

6.3 Supply Chain cases

Title: International Trade Transparency (Singapore)

Short description:

Working with various agencies and industry partners both locally and overseas, “TradeTrust” focuses on the exchange of digital trade documentation. It is an interoperability framework that aims to facilitate participation of DLT-based business in the same way that it does non-DLT business. Interoperability is achieved at the business application layer rather than network layer.

Keywords:

Cross-border Trade, Title-Transfer document, Trade Finance, Fraud prevention, MLETR, Fintech

Abstract:

In today's world of international trade, conventional digitalisation efforts have given rise to increasingly fragmented digital ecosystems consisting of siloed groups of user communities. This Singapore use case seeks to develop an interoperability framework ‘TradeTrust’ which works within this reality by enabling various enterprise and platform systems to effectively interoperate and accelerate digital innovation in global trade.

Working with various agencies and industry partners both locally and overseas, “TradeTrust” focuses on the exchange of digital trade documentation. This will enable a more seamless and efficient flow of goods between digitally inter-connected trading partners. This framework aims to reduce inefficiencies and complexities of cross-border trade arising from the current usage of paper-based documentation, such as Bills of Lading. This lowers operating costs for businesses and the risk of fraud while accelerating the digitalisation of cross-border trade processes thereby facilitating more efficient trade.

Title: Maritime Bills of Lading (Israel)

Short description:

A blockchain-based digital Bill of Lading extends the digital service that the International Port Community Systems Association (IPCSA) provides to the maritime trade today. This blockchain solution brings transparency and speed to the maritime trade.

Keywords:

Port Community Systems, Supply Chain, Maritime trade, Bill of Lading

Abstract:

Port Community System (PCS) operators are constantly seeking to promote a more secure and efficient maritime trade process as well as a better service to the members of the community.

One of the most important documents in the maritime trade process is the Bill of Lading (BoL), which is still a physical document. A BoL is a negotiable document issued by a carrier (or his agent) to acknowledge receipt of cargo for shipment. BoL is one of three crucial documents used in international trade to ensure that exporters receive payment and importers receive the merchandise.

The IPCSA Blockchain based Digital BoL service will allow all those business process players to issue, approve and endorse the BoL.

Title: Franchised Pharma Management (China)

Short description:

Use of blockchain technology can guarantee the authenticity of the drugs and pharmaceutical equipment, and ensure the healthcare and safety of the people.

Keywords:

Drugs and Pharmaceutical Equipment traceability system, healthcare, hospital, medical institution, government, logistics, customs, blockchain, IOT, GIS, Data authenticity

Abstract:

This DLT use case establishes a traceability and supervision system for a pharmaceutical supply-chain management system. The blockchain-based system is created to effectively monitor franchised drugs and pharma equipment using real-time traceability, tracking inquiry and supervision throughout the product lifecycle. Important lifecycle processes include: application, approval, purchase, storage, transportation, receiving and monitoring adverse reactions.

This solution responds to public sector need and was sponsored by Bo'ao Special District Committee, Hainan Province, China, with the participation from State Food and Drug Administration, Customs, Provincial Food and Drug Administration, Provincial Sanitary Planning Commission, Provincial Government and Medical institutions. Data incorporated includes drugs and pharmaceutical equipment data, commercial use and approval data incorporated as on-chain data, to lend structure and depth to on-chain provenance tracking.

This solution uses Internet of Things (IOT) equipment to replace manual input. On-chain data will flow to all nodes on the blockchain in near real-time. The supervision system deployed at each node queries traceability data across the nodes simultaneously to monitor and resolve any issues detected. Use of blockchain technology can provide assurance of the authenticity of drugs and pharmaceutical equipment and enhance the healthcare and safety of the people.

Title: Anti-counterfeit Pharma (India)

Short description:

The platform created by Realmeds in India aims to provide end authenticity and integrity assurance for pharma supply chain actors throughout the product life-cycle and accessible to end-user patients and caregivers.

Keywords:

Pharma traceability, product authenticity, anti-counterfeit, healthcare, hospital, medical institution, government, logistics, blockchain, IOT, GIS

Abstract:

WHO[21] and other renowned organisations[22] have noted the global size of substandard of falsified medical products. FICCI reports that nearly 15 % to 20 % of medicines sold in India are fake[23].

As per studies, this costs the pharma industry more in revenue. This puts a very large population at risk leading to deaths or ineffective treatment of their disease. This is in spite of the fact that the pharma industry has had track and trace systems for many years.

Blockchain offers attributes for traceability and counterfeit solutions for pharma drugs where on one side it protects the life of over a million people every year and on the other side provides better brand protection to manufacturers.

The platform created by Realmeds in India aims to provide end-to-end track & traceability with elaborate anti-counterfeiting checks to ensure that medicines are authentic and are safety compliant throughout the whole product lifecycle. The platform can also be used at the point of administering and at POS in-store or online.

Title: IGP Traceability (Italy)

Short description:

This use case represents a strategic solution in the IGP Red Oranges supply chain management through a smart traceability solution based on the blockchain technology.

The solution provided by the Red Orange Upgrading Green Economy (ROUGE) provides the certified and unchangeable history of the product. ROUGE supports the fight against fraud and forgery and it guarantees transparency of transactions, security and resilience within the supply chain.

Keywords:

Food Supply Chain, Agriculture produced food fraud, Made in Italy Protection, Italian Manufacturing Protection, Food companies, Food Service and Retail, Governments, Consumers, Farmers, Logistics Transparency, Traceability, Security, Resilience, Customs, Export, Italian Sounding, IOT, GIS, Precision Farming.

Abstract:

The traceability of agriculture produced food products to defend and support ‘Made in Italy’ manufacturing responds to a growing demand for information and consumer confidence. The Red Orange Upgrading Green Economy (ROUGE) is the new ally process to protect Sicilian citrus fruit farming.

ROUGE makes it possible to guarantee fruit of excellence thanks to a technological label that tells the origin, identity and characteristics of the product. ROUGE was conceived by AlmavivA with the Consorzio IGP Arancia Rossa with a vision to offer product and consumer protection services to member companies[12].

ROUGE aims to offer efficient supply chain management across the entire value chain, between the activities of producers, retailers and logistics operators. Within the supply chain, the companies involved will generate information flows able to affect the productivity by providing essential indicators in the strategic choices of adoption by domestic and foreign markets.

Some main advantages are: eliminating fraud and forgery, simplification of bureaucratic requirements, reduction of data imputation errors, improvement of control operations, transparency and traceability of transactions, security and resilience.

Title: Universal Farm Compliance (Ireland)

Short description:

Universal Farm Compliance offers the farming sector secure, real-time farm compliance reporting and mobile farm data collection on the fly.

Keywords:

Farm management, farm compliance, mobile data management, mobile edge computing, decentralised data, digital identity management, process transparency, food value chain, public sector reform, single digital marketplace

Abstract:

Farm compliance processes, as in many other public sector processes, are ripe for digital transformation: data integrity checking, anti-fraud practices and deadline driven interactions dominate the farmer/public body relationship.

For farmers, 'digital-first' raises problems of intermittent or sparse internet access, divergent technical skill levels and conflict around data ownership and privacy.

This use case offers offline-first mobile and edge computing solutions; low- friction interaction design, intelligent data entry points and decentralised data governance to effect appropriate KYC, access permissions and a novel farmer- first data ownership model that affords access to new revenue streams to farmers using the system.

The EU is making strides to facilitate public sector reform to enhance cohesion across the single digital marketplace. This use case exemplifies difficulties that exist in distributed governance contexts and applies decentralised approaches to resolving them.

With the added difficulty of applying digital solutions where connectivity can be limited the use case addresses concerns about access and performance for real- time farm management systems in the wild.

Title: International Waste Management System (Netherlands)

Short description:

To reduce the supervision costs related to European waste transportation, the Ministry wanted to combine blockchain technology with existing IT-systems. This way the inspection authorities can automate a significant portion of their tasks. This frees up knowledge and expertise for other important tasks that cannot be performed without human assistance (yet).

Keywords:

Government; Supply; Chain; IoT; Waste; Transportation; Contract; Atomization; and Regulator.

Abstract:

This use cases addresses 3 key business challenges to the cross-border waste management process, with a blockchain solution applied with the Dutch and Belgium Governments, Inspection services and waste disposal companies:

— Numerous stakeholders: Currently, multiple different government bodies supervise and authorize the export, import, and transportation of company waste throughout the European Union.

- EU regulation: The EU supervises various aspects of these processes such as granting permits, notifying involved parties of waste transports, and scheduling random sample checks.
- Manual handling: Execution of steps in the process happens on paper forms in multiple languages. Even the fax machine was still used to update the OVAM (Public Waste Agency of Flanders) in Belgium.

This use cases provides a solution through:

- Automated permit check: By implementing LTO Network into the system to issue and verify the permits, approval of the transportation request is automatic. Sharing data happens directly with the waste processor and authorities in case of cross-border transportation.
- Data re-use: The transportation companies can use their smartphones to show their transportation documentation to the authorities in case of a random check. The inspectorate can derive the data directly from the LTO Network blockchain.
- Connecting systems: By digitizing the protocol that already existed on paper into a 'Live Contract' parties were able to connect their existing systems to LTO Network to communicate, share data and notifications real-time.

This use case helps solve the problem to automate business processes and trust issues between waste disposal companies and Governments. The key stakeholders are the Dutch and Belgium governments, inspection service and waste disposal companies. This use case uses Blockchain to share data in a secure way, making sure everyone involved looks at a single point of truth. It avoids unnecessary e-mail, paper and saves time on waste management processes.

6.4 Smart Energy use cases

Title: Cooperative Energy Trading (Ireland)

Short description:

This use case enables both individual consumers and their broader communities generating their own electricity to trade electricity back to the Network Provider based on a cooperative model using blockchain to record transactions.

The project will demonstrate trading excess electrical energy generated by prosumers, wind and solar farms. The ability to document transactions using blockchain can help get support from relevant stakeholders and enable large scale trading.

Keywords:

Energy, Trading, Stablecoin, Cooperative, Ireland, PV, Solar, Wind, Photovoltaic, Electricity, Battery Storage, Disruptive Technologies Innovation Fund, DTIF, Project 2040, IERC, International Energy Research Centre, Tyndall National Institute[2], CENTS

Abstract:

The energy sector and more specifically the electricity market is at a point for significant transformation from the traditional model of the last several decades. Distributed generation is emerging as a key enabler to this change of the electricity market where new technologies including blockchain along with the myriad renewable energy options are making a significant difference towards the goals of decarbonisation.

With the predicted population growth in Ireland, there will be an increased demand for energy such that even the most forward-looking integrated electricity market could struggle to cope.

This use case addresses how the combination of renewable energy generation and blockchain can provide a key solution of this consumer-focused next generation electricity system in Ireland.

To support a range of these Irish government initiatives and making the electricity sector more flexible than ever before, the CENTS (Cooperative Energy Trading System) project is proposing to empower both individual consumers and their broader communities for their own electricity generation. It will provide a blockchain based platform for electricity trading between different communities which could be one of the key disrupters of the Irish Electricity market. This project aims to set the benchmark for other electricity markets across the world.

Title: Energy Trading (India)

Short description:

Transactive grid solutions that enable distributed energy generation and consumption among prosumers and integration of localized energy actors with centralized grid in a seamless manner.

Keywords:

2P Energy Trading, Demand Response, Flexibility Aggregator, Distribution Service Operator, Vehicle to Grid, Energy Sector, Smart Grids.

Abstract:

This use case based in India addresses how blockchain solutions can contribute to the global electricity systems as they move towards the 3D's of Decarbonized, Decentralized and Digitized forms of energy.

Currently, the power sector customers and service providers are both struggling with a unique set of problems. The customers are concerned about access to energy, cost of energy, grid reliability, poor quality of services and lack of transparency. The grid operators face challenges of high energy losses, lower capacity utilization, grid congestion, inefficient grid operations, vulnerability to grid hacking and inability to integrate increasing renewable energy into the grid. Sufficient tools are not always available to enable the grid operators to engage directly with customers.

The use case proposes an integrated energy platform with service to multiple levels of stakeholders from home owner level, community level, distribution utility level and the system operator level.

It includes two use cases to demonstrate 1) the peer to peer energy trading between prosumers in an energy community, and 2) how a utility company can engage with end consumers in real time through a Demand Response or Flexibility event.

This use case is creating transactive energy grids applications for energy exchange and grid management. Key stakeholders include the energy ecosystem (Power Utility, Renewable energy producers, power trading companies and customers) to build and demonstrate our solution through successful POCs at multiple levels.

Blockchain addresses the issues of trust, transparency, improves process efficiency in creating contracts, high transaction costs, and instant reconciliation of records among multiple untrusted parties in real time.

Title: Renewable Energy Microgrids (Spain)

Short description:

A P2P internal market of energy between energy prosumers managed and governed with blockchain technology linked to tokenised incentives to promote sustainable behaviour.

Keywords:

Prosumption, renewable energy, micro-grid, energy operator, P2P transactions, smart contracts, reward token.

Abstract:

This use case addresses a peer to peer internal market of energy between energy prosumers managed and governed with blockchain technology linked to tokenised incentives to promote sustainable behaviour.

The proposal is for a government-led blockchain project in Catalonia, Spain, to create a circular economy of local solar communities to transact energy through self-management of renewable energy prosumer micro-grids.

A government-led blockchain project for local solar communities to transact energy has extensions to reward sustainable behaviour and energy- conscious choices. These extensions would allow for the inclusion of citizens who do not have solar panels and therefore are not part of a solar community. This strategy of having the core use case (solar communities) extended towards complimentary strategies to reach out to the wider citizenship without exclusion is a key element for uptake and adoption of government-led blockchain projects, and to deliver on sustainability goals.

Prosumer micro-grids can benefit from disintermediation if the grid is operated independently and isolated from the commercial network. Blockchain technology is used for self-management and self-governance of the micro-grid, through the contracting of the service and invoicing of energy. By using Proof of Authority (PoA) algorithms, this use of the blockchain optimises processes to reduce service costs and adds transparency to the management of this shared resource.

7 Use case overview and insights by category

7.1 General

This document provides insights, trends and observations relevant to those designing and implementing solutions. By reviewing these insights, users will be able to search this document for the relevant classification to their sector and discover transferable skills to their blockchain requirements.

The use case categories are:

- Transversal (related technologies), Figure 7.
- Horizontal (attributes), Figure 8.
- Vertical (sector specific), Figure 9.
- Status (classified across a spectrum of technical development phases) Figure 10.
- United Nations sustainable development goals (SDGs), Figure 11.

Use cases in the same business sector can share their different perspectives, which provides insights into regional variances in approach to global challenges, from supply chains to climate change, based on their local markets and regulations.

The multiple categories allow for use cases in different vertical sectors, to discover transferable Horizontal attributes or Transversal related technologies.

In addition, an unexpected and useful outcome of the use case collaborative approach is the benefits of the ‘network effect’ and ‘peer review’ processes, which led to collaboration of different problem spaces and unexpected reuse of systems in other contexts; such as the cross-borders supply chain examples or solutions for specific SDG goals.

Analysis on each category is covered in more detail below.

7.2 Insights - transversal categories

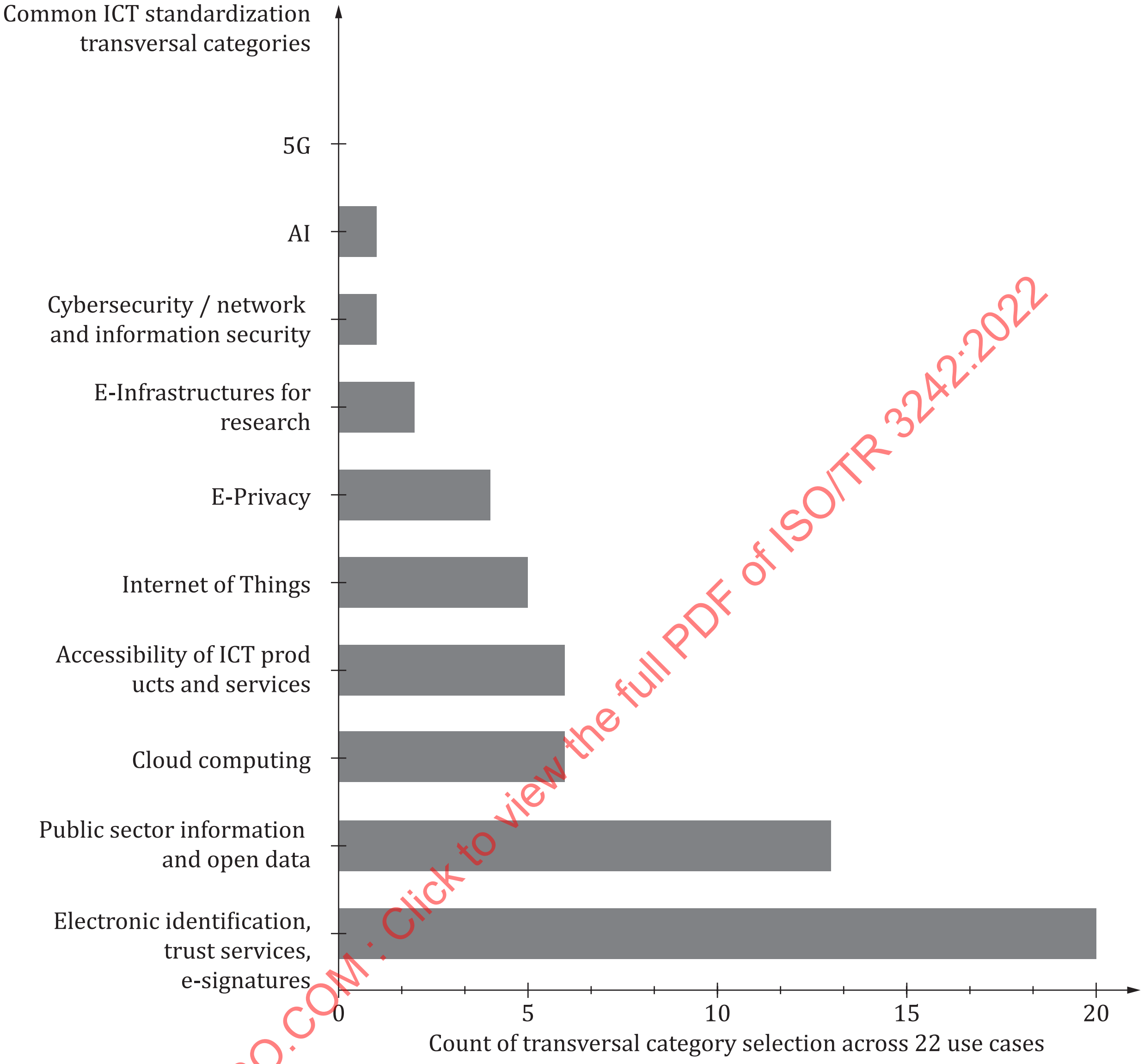


Figure 7 — Transversal category overview

Analysis of these use case categories illustrates the importance of electronic identification, trust services and e-signatures. This category is present in every one of our use cases, and points to the case for implementation via a unified, global infrastructure that would enable interoperability, foster efficiency and promote cooperation between different nations and regulatory regimes.

The role of public sector and open data programs is the second highest category, recognising the involvement of government programs in both leading and supporting blockchain ecosystems. Examples include:

— ‘International Trade Transparency’ is derived for an open-source blockchain infrastructure for certification developed by the Singapore Government for local and international businesses to build on.

— ‘Renewable Energy Prosumer Micro-Grids’ is a blockchain component of a Catalonian Government initiative based on tokenisation of a larger ecosystem of energy-efficient smart cities.

— ‘Property Records Management’ and ‘Student Records Management‘ use cases are supported on a regional government level with a dedicated blockchain district in Telangana, Hyderabad, India.

7.3 Insights - horizontal categories

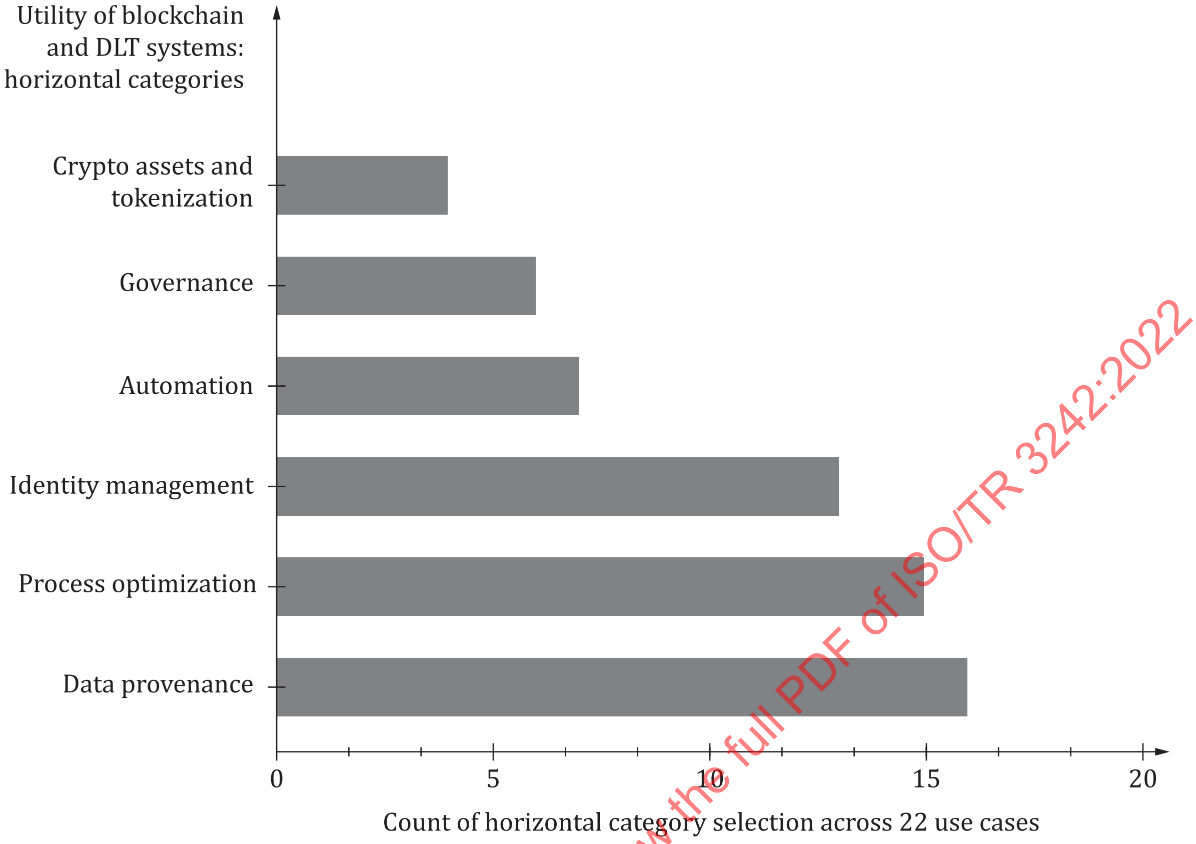


Figure 8 — Horizontal category overview

In the horizontal category, it is no surprise that Data Provenance, Identity Management and Process Optimisation are the most prominent blockchain attributes.

The Data Provenance category includes how supply chain use cases are being addressed from regional perspectives to tackle global challenges of trade efficiencies and counterfeit risks.

- 'Maritime Bill of Lading' (Israel) includes an international commercial model, whereas Singapore 'International Trade Transparency' provides a new government-backed national model.
- 'Pharma use cases provide alternative perspectives of data provenance, where 'Anti-Counterfeit Pharma' (India) considers a product traceability for consumer and brand perspective and 'Franchised Pharma Supply Management' (China) considers efficiency across the whole product lifecycle. This area is attracting increasing attention as a result of the Covid-19 issues.
- 'IGP Traceability' (Italy) and 'Universal Farm Compliance' (Ireland) reflect the supply chain of food product identification and provenance across local and international supply chains.

The Identity category includes blockchain as it is applied to individuals and entities, objects, things and processes.

- 'Data Accountability' focuses on the management of privacy by individuals within the context of European regulations, and 'Self Sovereign Identity' is a Cyprus-based use case to monetise identity management.
- Other cases address the transfer of authenticated assets between individuals, objects and processes in 'Content Timestamp Verification', 'Student Records' and 'Property Records Management'.

The Process Optimisation category covers many use cases, where blockchain initiatives are adapting to grow and scale to serve international processes.

— 'Franchised Pharma Supply Management' (China) is scaling through consortia with other blockchain systems.

These use cases illustrate the options of interoperability of multiple blockchains and off-chain systems. In assessing the future impact of blockchain at an enterprise or global adoption, this category is an example of addressing the non-functional requirements including scalability, availability and performance.

7.4 Insights - vertical category

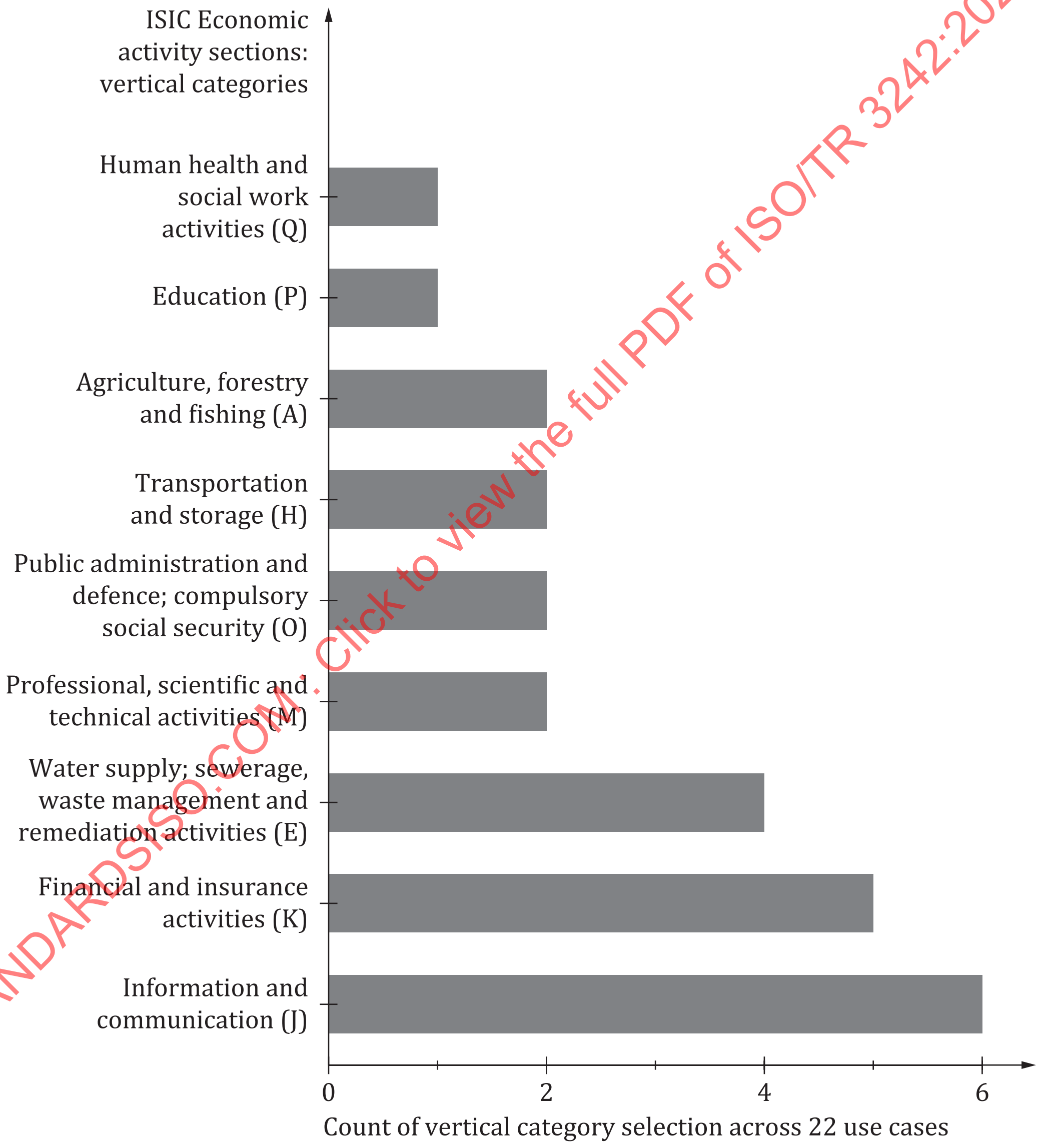


Figure 9 — Vertical category overview

There is a spread of use cases across the Vertical categories, and many use-cases illustrate transferable attributes to other economic sectors and learnings for both interoperability and governance in multiple sectors that transact across regional and international jurisdictions.

The Financial and insurance category includes a spectrum of services.

— 'Interbank Loan Reconciliation' (China) uses blockchain to streamline the settlement time.

- ‘Decentralized Charity Platform’ (the Republic of Korea) uses diverse decentralized technologies to enhance traceability and autonomous service delivery in charitable donations.
- ‘Organised CHIT Funds’ (India), and addressing solutions for people without low fixed assets or insufficient credit rating, whereas ‘Transparent Securitisation’ (Italy) and ‘Accounts Receivable’ (China) addresses the small businesses access to capital.

The Energy category use cases provide alternative perspectives of energy trading.

- ‘Renewable Energy Prosumer Grids’ (Spain) and ‘Cooperative Energy Trading’ (Ireland) focus on the consumer and community transactions, while ‘Energy Trading’ (India) focuses on utility and producer trading.
- The ‘International Waste Transportation Management System (Netherlands) describes the cross-border process between multiple stakeholders in waste, regulations and logistics.

The Information and Communication category includes use cases across a range of different types of data provenance and authentication attributes.

- ‘Content Timestamp Verification’ (Netherlands) focus is copyright protection.
- ‘Student Records’ (India) focus on education certification.
- ‘Data Accountability’ (EU) focus on EU smart contracts on privacy rights.
- ‘Pension Process Optimisation’ (China).

The Professional, Scientific and Technical Activities sector includes a use case that could fit across multiple categories. ‘Anti-counterfeit Pharma’ (India) provides information and communication on traceability to avoid fraud across the pharma supply chain.

7.5 Insights - status

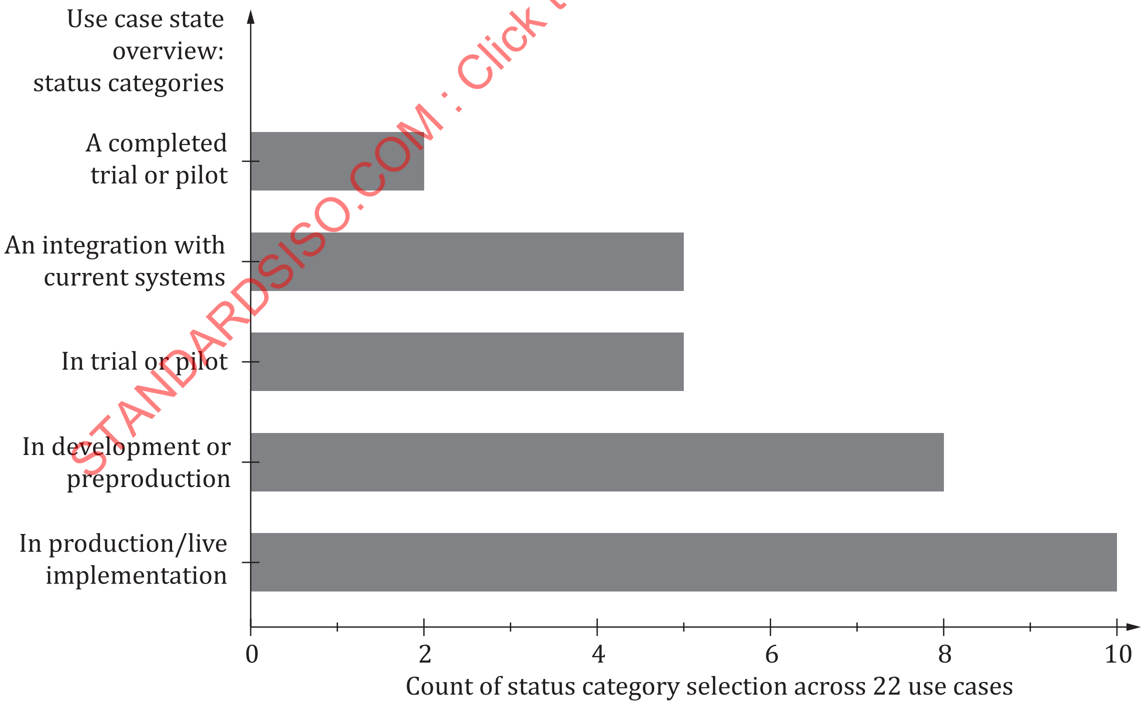


Figure 10 — Status category overview

A majority of use cases in the ‘Status’ category are in productive implementation. The Status category reflects the stages or models of a use case, from initial concept to integration, and adoption within a community. In this way, use cases reflect the changing objectives from hypothesis to implementation and learnings phases of a typical technology development process. The approach is to apply current market learnings to filter quickly into the standards development.

This document has included use cases ‘in development’ where they reflect new initiatives that will drive future blockchain requirements.

- ‘Data Accountability’(EU) reflects the new European privacy regulations, such as GDPR, that impact data traceability, on-chain and off-chain processing and storage.

The ‘implemented’ use cases provide both inspiration, feedback and learnings for blockchain users.

- ‘International Waste Management Transport’ (Netherlands) illustrates cross-border transport systems that have delivered blockchain solutions that manage permits, data re-use and real-time connected systems.
- ‘Student Records’ (India) is implemented in regional Hyderabad, yet the Use case requirements serve a global demand for trust, authenticated education processes.
- The Fintech and Smart Energy use cases in the Vertical category are demonstrating efficiencies that can apply across multiple sectors.
- ‘Decentralized Charity Platform’ (the Republic of Korea) reflects the transferable issues of identification and trust in charitable donations.
- The Pharma use cases have particular relevance due to the Covid-19 issues during the development of this document.

7.6 Sustainable development goals (SDGs)

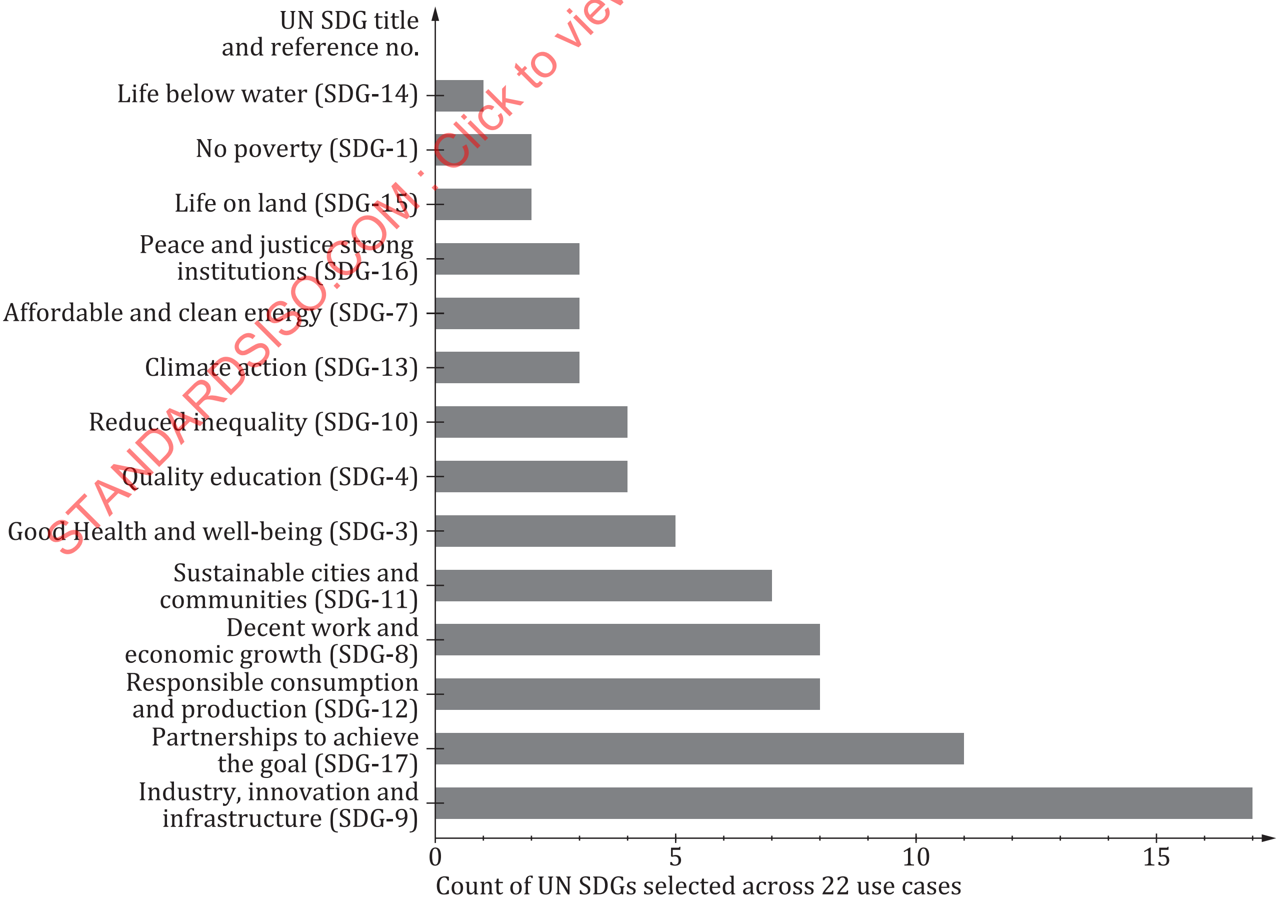


Figure 11 — Sustainable development goals category overview

Each use case provide the SDGs that are the most relevant to the business in question. In a number of use cases, the societal benefit is a core business objective, including:

- Goals – Sustainability Cities/Affordable and Clean Energy/Climate Action includes the smart energy focus with ‘Renewable Energy Prosumer Grids’ (Spain), ‘Cooperative Energy Trading’ (Ireland), ‘Energy Trading’ (India) and ‘International Waste Transportation Management System (Netherlands)
- Goals – Responsible Consumption and Production includes use cases focussed on food, ‘IGP Traceability (Italy) and ‘Universal Farm Compliance’ (Ireland), and pharma ‘Anti-Counterfeit Pharma’ (India) ‘‘Franchised Pharma Supply Management’ (China) Goal – Quality Education includes Student Records Management (India) and Education Certificate Provenance (Spain).
- Goal - Reduce Inequality includes financial inclusion focus with ‘Organised Chit Funds’ (India), ‘Transparent Securitisation’ (Italy), Decentralized Charity Platform (the Republic of Korea).

7.7 Insights - blockchain implementation types

Blockchain implementation type

Figure 12 describes the prevalence of types of blockchain implementations in this document. Public blockchains are deployed in 27 % of cases. More than 50 % of use cases described are implemented on private, permissioned blockchains and 18% on hybrid blockchains (18 %).

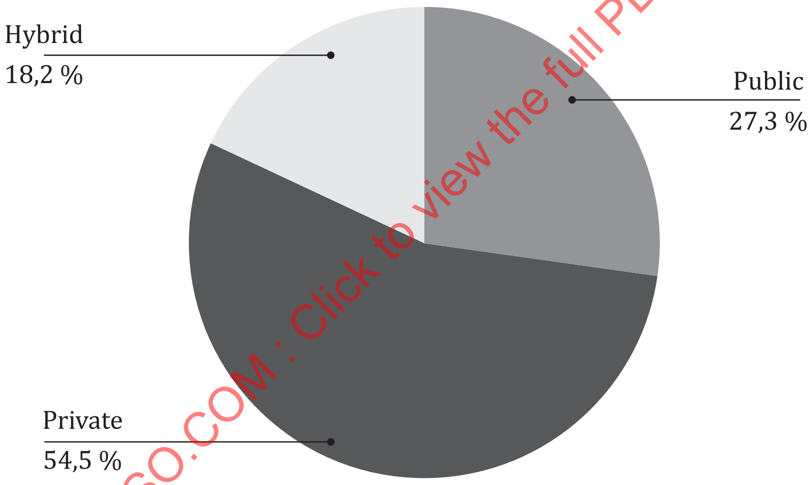


Figure 12 — Blockchain implementation type

Blockchain implementation platforms

Figure 13 shows a count the blockchain implementations referenced in this document.

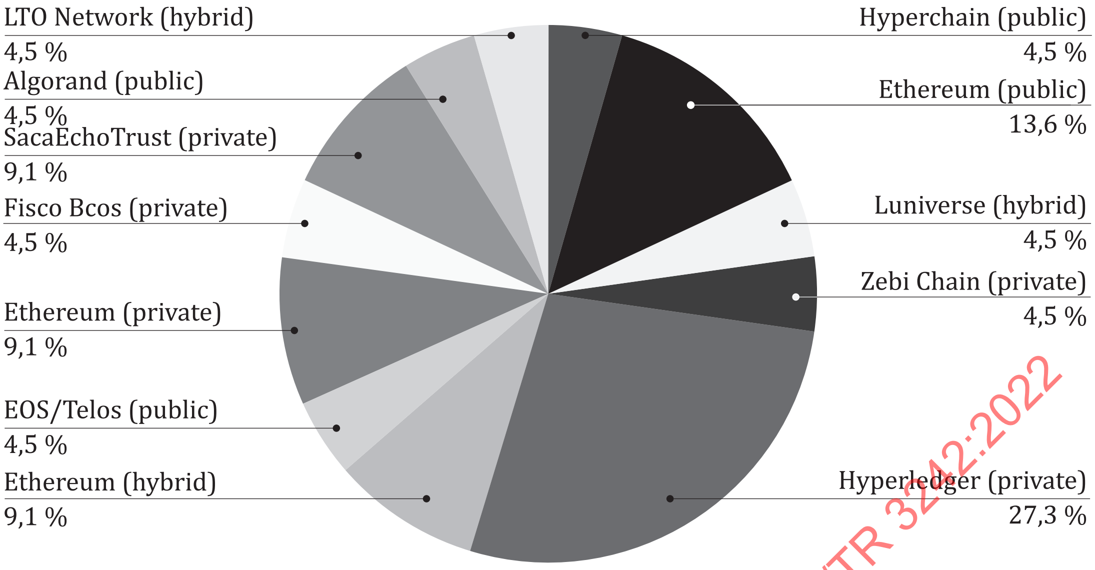


Figure 13 — Blockchain implementation platforms

By assessing the Reference Architectures diagrams, the use cases reflect new platforms including:

- Algorand: 'Transparent Securitisation' uses Algorand for its pure proof-of-stake (PPoS) protocol
- EOS/Telos: 'Content Timestamp Verification' uses EOS /Telos in smart contracts for timestamps.
- EBSI: 'Universal Farm Compliance' describes the EU Blockchain Services Infrastructure utilising a Hyperledger and Ethereum Besu client hybrid implementation.
- FISCO BCOS: 'Accounts Receivable' and 'Interbank Loan Reconciliation' use FISCO BCOS, China's open source blockchain private platform.
- LTO Network: 'Int Waste Management Transport' uses a sophisticated hybrid blockchain workflow engine from LTO Network as a means of efficiently managing regulations in different countries.
- Saca Echo Trust: a private blockchain implementation used by Neusoft Corporation, in the 'Franchised Pharma' use case.
- Luniverse: 'Decentralised Charity Platform' uses Luniverse chain service based on PoA(Proof of Authority) protocol for scalability and interoperability with other blockchain networks.
- Zebi Chain: is a private blockchain implementation utilised in the Student Records Management use case from Hyderabad Blockchain District in India.

7.8 Insights – open source

In late 2019, ISO/IEC JTC 1[26] researched experience related to standards, specifications, and open source software (OSS). ISO/IEC JTC 1 looked into how ICT standards are used in conjunction with open source. By surveying national bodies and standards organizations that incorporate open source software (OSS) into the development of standards, ISO/IEC JTC 1 sought to identify and record examples of these shared activities. Figure 14 describes the scenarios in which use case authors described their engagement with open source software.

ISO/IEC JTC 1 requested that participants provide case studies or supplemental materials with or following completion of the survey.

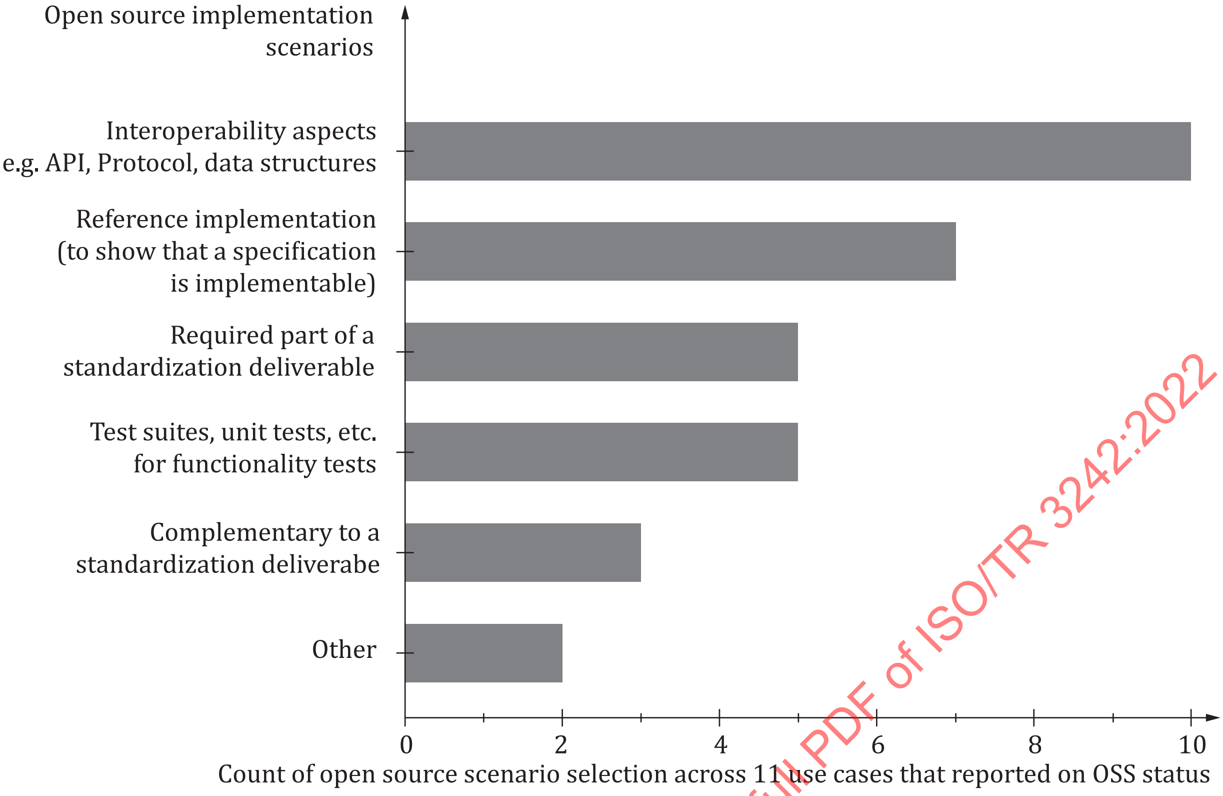


Figure 14 — Open source scenarios

Below are the summarised responses deemed most relevant to use case authors who made submissions to this document.

Use Case title	Open source comment
Accounts Receivable	FISCO-BCOS as the blockchain MINIO as the file storage JDK1.8 for development language Node.js for web front-end Docker as the running container
Renewable Energy Micro-grids	Fork of Ethereum network utilised to create our private network.
Transparent Securitisation	Specific parts of the code will be open-sourced (e.g. for design reasons, the smart contract handling the token issuance and transfer).

8 Use cases: Data Provenance

8.1 Data Accountability (European Union)

8.1.1 Categories

- **Transversal category:**
- 5. Electronic identification, trust services, e-signatures,
- 6. e-Privacy.
- **Horizontal category:**
- 1. Identity Management,

- 2. Data Provenance.
- **Vertical category:**
- ISIC Section, division, group and class =
- J-6311, Section J - Information and communication,
- 6311 - Data processing, hosting and related activities.
- **UN Sustainable development goals:** No.
- **Status:** 3. in development or pre-production, proof of concept implementation.

8.1.2 Summary

Long Description

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 can be enforced in all EU Member States. In light of these requirements, this use case proposes 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.

The proposed solution addresses a problem that is currently not tackled by any other framework, i.e. the need for an automated and certified tool for data subjects to verify if data controllers/processors are complying with their privacy preferences.

Although the initial trigger of this solution was the GDPR, it goes beyond this scope and it is relevant for many other use cases including, for example, regulations related to the handling of health information.

Business problem or opportunity

The solution described in this use case has the potential to improve transparency for users, increasing trust when they are required to provide personal data for processing.

Furthermore, the goal is to support regulatory compliance by data controllers and processors considering the GDPR. Finally, it also provides a systematic way for data controllers and data processors to have access to the data subject preferences.

Scope

The scope is data accountability and provenance tracking using smart contracts when personal data is given to data controllers and data processors.

The objective is to improve transparency and auditability from a data subject point of view, allowing for blockchain-based informed consent and withdrawing.

The use case applies in any context where personal data about a subject is accessed by entities playing the role of a data controller or data processor.

Objective

Improve user control and transparency with respect to the processing of their personal data.

Provide a mechanism to enable data controllers and processors to prove they have the right/consent from users to process their data.

Stakeholders

- Data Subject (human user), the owner of the data
- Data Controller, the entity accessing data in order to provide service
- Data Processor, the entity processing data on behalf of the data controller
- Service Provider, the entity responsible for building and maintaining the distributed digital
- infrastructure that provides a blockchain-based virtual machine

Predicted outcomes

A more transparent way for users to see how their data is being processed leading to increased trust and more business opportunities for data controllers/processors.

Why distributed ledger technology?

In traditional centralized ledgers data subjects have no easy way to audit and verify the following concerns

a) the set of data accessed by data controllers and processors and

b) how the provided data is being used.

8.1.3 User requirements

Functional requirements

- Data subjects create smart contracts that take into account their privacy preferences (data usage contract).
- Data controllers and processors check the data usage contracts to verify if they are allowed to use/process the data according to the activity they are about to perform.

Visualizations: Figures 15 to 19.

- **System view architecture**

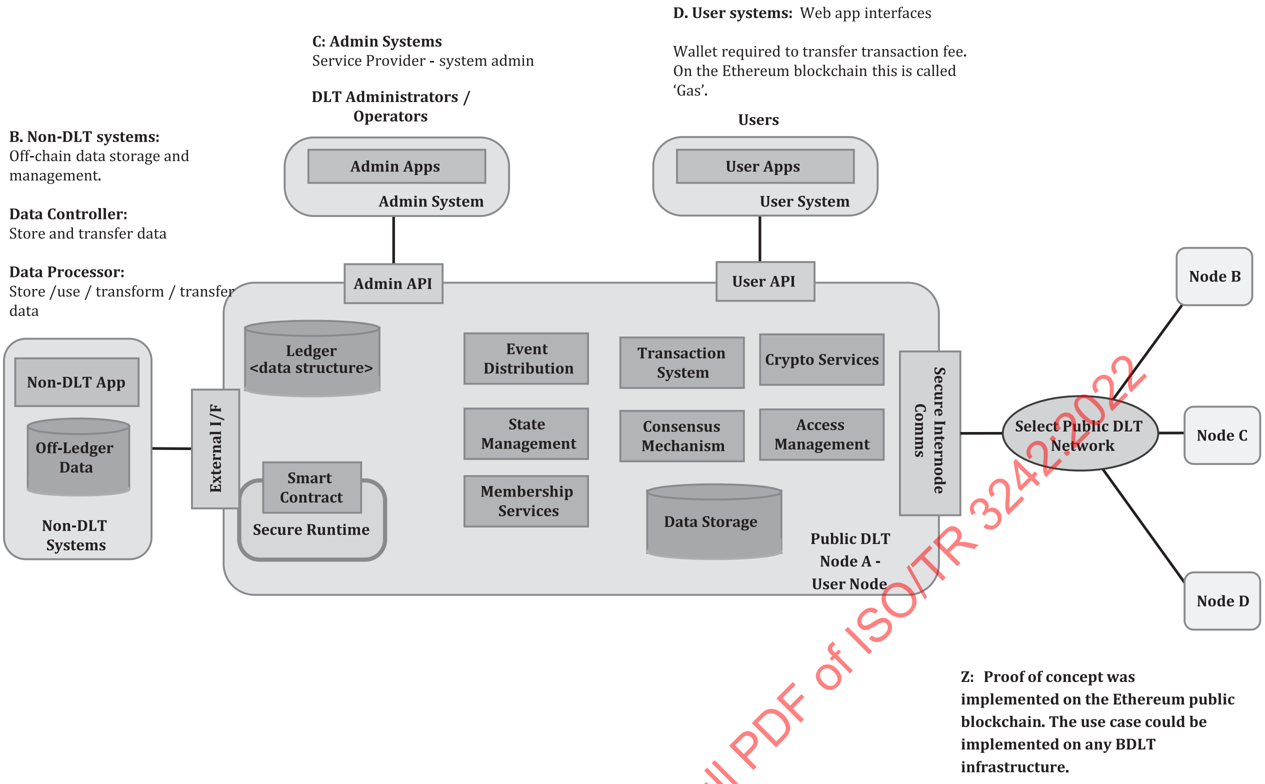

D. User systems: Web app interfaces
Wallet required to transfer transaction fee. On the Ethereum blockchain this is called 'Gas'.
Users
C: Admin Systems
Service Provider - system admin
DLT Administrators / Operators
B. Non-DLT systems:
Off-chain data storage and management.
Data Controller:
Store and transfer data
Data Processor:
Store /use / transform / transfer data
Admin Apps
Admin System
User Apps
User System
Admin API
User API
Non-DLT App
Off-Ledger Data
Non-DLT Systems
External I/F
Ledger <data structure>
Event Distribution
Transaction System
Crypto Services
State Management
Consensus Mechanism
Access Management
Smart Contract
Secure Runtime
Membership Services
Data Storage
Secure Internode Comms
Public DLT Node A - User Node
Select Public DLT Network
Node B
Node C
Node D
Z: Proof of concept was implemented on the Ethereum public blockchain. The use case could be implemented on any BDLT infrastructure.

Figure 15 — System view architecture: Data accountability (EC)

— **Data flow model**

Reference Architecture: 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 data controller or data processor, it creates a policy-based data usage contract (controller 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 allows 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
- The Blockchain-based Virtual Machine is deployed and maintained by a service provider.

Data flow analysis

Identify the data flows triggered by the data-related operations of each stakeholder:

i) Stakeholders: **Data subject (user), Data controller, Data processor and Service provider.**

ii) Type of data flow (categories A- Z) - Data type: User Data / Data flow type D - between user app and DLT system.

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

D. User systems: Web app interfaces
Data subject:
(1) subscribe
(2) create data usage contract
(3) transfer data to Controller

Data controllers + processors:
(1) view data usage contract.
(2) record data transfer to Processor

Wallet required to transfer Gas - the cost of transacting on the Ethereum blockchain

C. Admin system:
Service Provider Currently EC Joint Research Centre. In the future this may be a public authority or other provider.
(1) Build system
(2) Admin system

B. Non-DLT systems:
Off-chain data storage and management.

Data Controller:
(1) Store data
(2) transfer data

Data Processor:
(1) Store data
(2) use / transform / transfer data

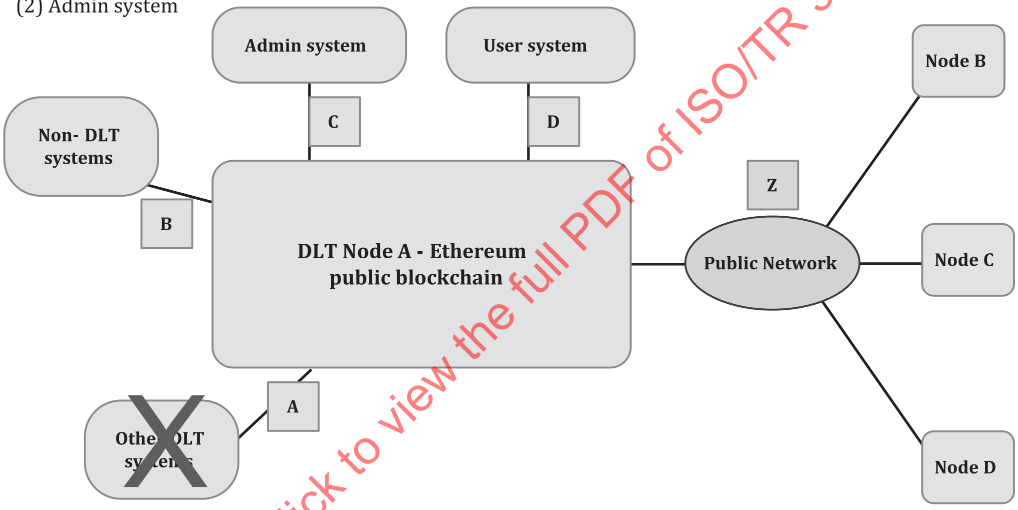


Figure 16 — Data flow analysis: Data accountability (EC)

— **Behavioural UML**

Use case diagram

The diagram below shows the information flow between the entities and contracts.

— Data Subject: Person. Creates data usage contract and provides data to the system.

— Data Controller: Organisation. Data controllers agree and check data usage contracts to verify if they are allowed to use/process the data according to the activity they are about to perform.

— Data Processor: Organisation. Data processors agree and check data usage contracts to verify if they are allowed to use/process the data according to the activity they are about to perform

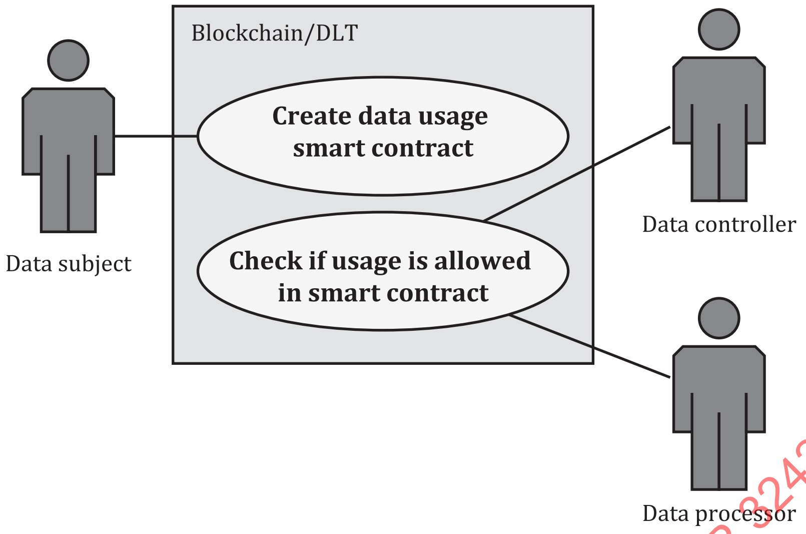

Blockchain/DLT
Create data usage smart contract
Check if usage is allowed in smart contract
Data subject
Data controller
Data processor

Figure 17 — Use case diagram: Data accountability (EC)

Use case interaction diagram

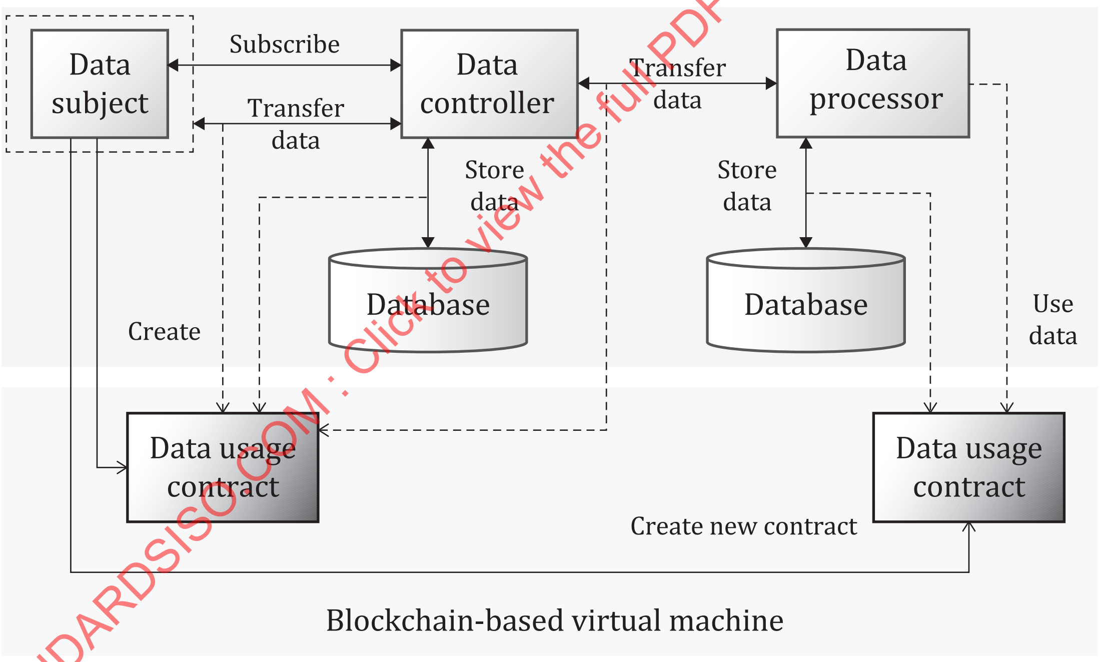


Figure 18 — Interaction diagram: Data accountability (EC)

Sequence diagram

A smart contract is defined including the list of personal data hashes accessed by data controller and processors in real-time, and the encoded usage control policy specifying the privacy preferences of the data subject stating how his/her data can be used.

The sequence diagram shows the interactions between the entities and contracts.

— The subject subscribes with the data controller, creates the custom contract for this controller regulating the use of his/her data, and transfers the data to the controller.

- For each new established contract, the subject uses a new blockchain address to prevent the ability to link the contracts established with each controller, requiring the subject to maintain a list of all addresses used and the respective nonce established with each controller or processor.
- After creating the contract, the subject transfers the data to the controller.

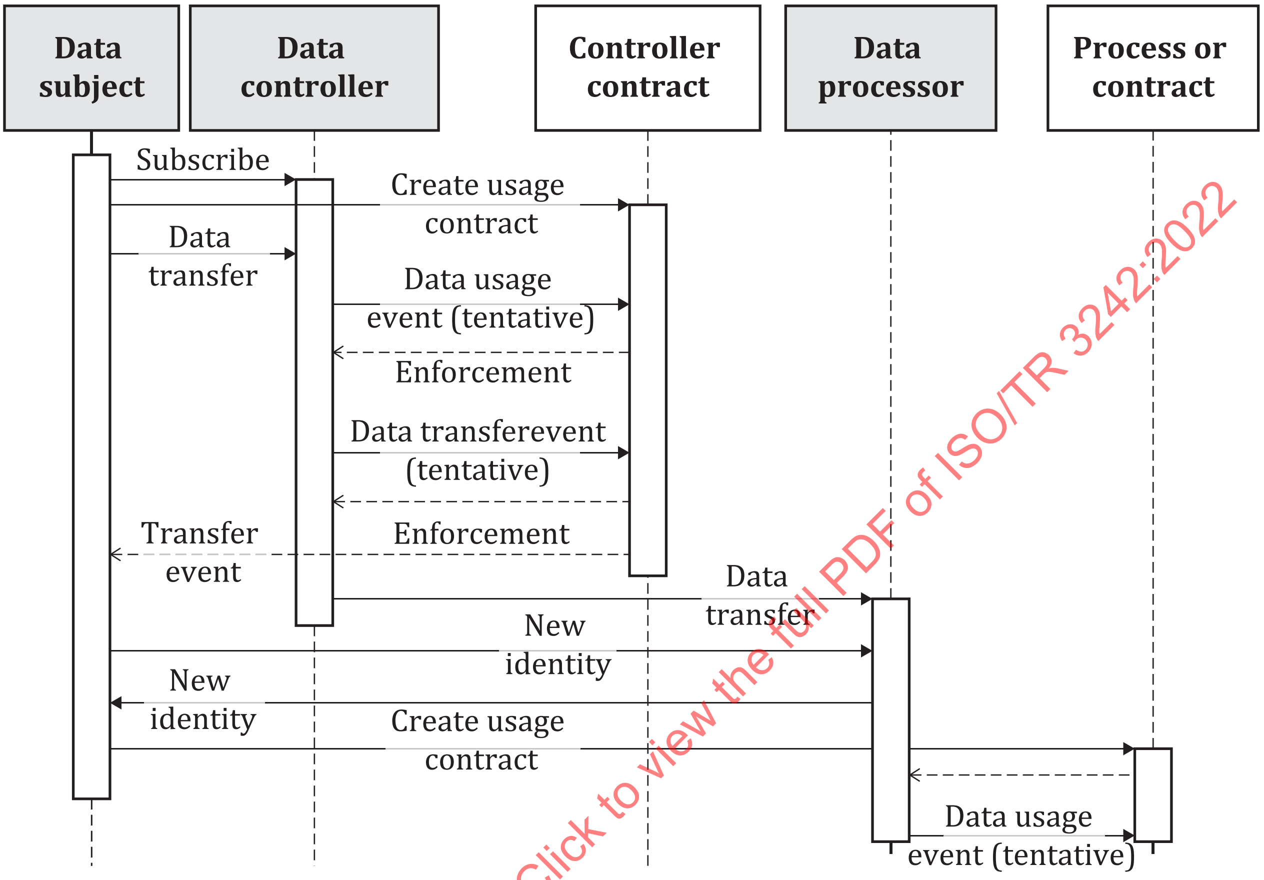


Figure 19 — Sequence diagram: Data accountability (EC)

Security, privacy and identity management

Privacy issues are very relevant since fingerprints of the personal data and the usage control policies are stored in a public blockchain.

The use case proposes a privacy-friendly way of encoding both data and policies 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 data processors and controllers can perform.

Data subjects create smart contracts using different identities, in order to prevent processors from learning and linking multiple data processing activities related to the same subject.

However, if controllers and processors collude, they could be able to learn the subject identity across processing activities.

Pre and post conditions

Pre-conditions: 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 are able to prove the data is stored and processed according to the subjects' privacy requirements.

Post conditions: 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 is encoded in a privacy friendly way.

Non-functional requirements

In public blockchain infrastructures (service provider) scalability is an issue considering the amount of data accessed, stored, and processed by many data controllers and processors.

This approach can be more viable considering only very sensitive data in lower volumes, for example, medical records.

The transaction latency is not particularly important, since the objective is to have proofs that will be checked after the data was exchanged.

Since the solution is very generic and can be applied in many different scenarios, the specific performance requirements will depend on the specific scenario.

For example, the solution could be used to record all data collected and exchanged by IoT devices with cloud services. In such high volume scenarios the solution proposed would need to be adapted to consider transfer of IoT data for particular periods without considering each specific data instance exchanged since it would become unfeasible due to the high overhead in the blockchain. In this sense, particular performance specs need to be analysed on a case-by-case basis also considering the specific blockchain technology adopted.

8.1.4 Force field analysis

Legal considerations

The use case aims notes the regional legal requirements General Data Protection Regulation (GDPR).

Risk:

Scalability is probably an issue and might need to be investigated further considering the particular scenario where the solution is deployed and applied.

From a user perspective, risk is related to the usability since privacy preferences must be encoded in a blockchain executable format. Therefore, a user-friendly interface and approach will guarantee wide user adoption.

The legal validity/binding effect of blockchain contracts can be an issue in case data subjects, processors, and controllers fall within different jurisdictions. This is not the case of the GDPR but it can be the case if the solution is applied to other scenarios involving countries with different legislations.

Other information:

A rating/score of the data processor is based on the number of abiding or violations of the data subject preferences, or from complaints from the data subject. This will lead to an increase in trustworthiness of the system for new subscribers.

Further information: European Commission Joint Research Centre[19]

8.2 Property Record Management System (PRMS) (India)

8.2.1 Categories

- **Transversal Category:**
  a) Cloud computing
  b) Public sector information and open data
  c) Cybersecurity / network and information security
  d) Electronic identification, trust services, e-signatures
- **Horizontal Category:**
  a) Identity Management
  b) Data Provenance
  c) Governance and DAOs
  d) Crypto Infrastructure
- **Vertical Category:**
  a) ISIC Section, division, group and class = O-8413
  b) Section O: Public administration and defence; compulsory social security. 841 - Administration of the State and the economic and social policy of the community
  c) 8413 - Regulation of and contribution to more efficient operation of businesses
- **UN Sustainable development goals:**
  a) GOAL 9: Industry, Innovation and Infrastructure
  b) GOAL 17: Partnerships to achieve the Goal
- **Status:**
  a) in trial or pilot
  b) an integration with current systems

8.2.2 Summary

Long description

The blockchain based Property Record Management System (PRMS) stores property registration transaction details in the blockchain in time sequenced fashion.

The registration process has two phases:

a) Pre-registration (Checkslip): check slip transaction captures and stores details namely buyer, seller and property attributes

b) Regular Document Generation: fingerprints are endorsed on the last page of the sale deed and a regular document number is assigned

The implemented PRMS system captures check slip and regular document transaction details and stores a hash in the blockchain.

The implemented PRMS system pulls the near real time checkslip transaction and regular document transaction details at regular intervals of time and stores them in the blockchain.

For high-value immovable property, accurate title (evidence of ownership) records will identify the current owner and provides a proof that the user is indeed the owner. These accurate title records provide numerous advantages such as:

a) protect owners' rights

b) resolve disputes

c) assures that the ownership is correctly transferred to a new owner after sale

d) reliable encumbrance search

Benefits of using Blockchain-based Property Record Management System are:

a) Improved transparency

b) Prevent fraud

c) Trust establishment with citizens

The PRMS is in pilot and is designed and developed by C-DAC Hyderabad and is supported by ITE&C department, NIC & Stamps and Registration departments of Telangana State Government.

Business problem or opportunity

Key business problems include double registration, producing fake documents for registration and insider attack / traditional database-related attacks are the most common frauds in the existing property registration system. This use case is an opportunity of integrating the blockchain technology with the existing property registration management system for improving the trust, security of the system and to address the above mentioned issues.

Advantages for a Property Registration application include:

— Immutability

No property record transaction can be tampered or deleted post execution on the blockchain.

Fraudulent overtaking of a property will be significantly difficult and will leave an audit trail in case an attempt is made.

— Trustworthy & transparent system

Property history and single source of truth from shared ledger ensures trustworthiness.

Users can view the relevant information ensuring privacy.

— High availability and resistant to malware attacks

Due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks.

— Reliable encumbrance search

Ease to track a property to its origin.

Scope

The scope of the application is to store the registration details, verify the title ownership and provide reliable encumbrance search from the transactions stored on blockchain.

This is implemented in India by integrating with the existing workflow and application of the Telangana State Government. It is piloted for Shamshabad district.

Though the workflow differs from state to state, it can be implemented and customised for other states.

Objective

The objectives of the developed application are to provide:

- Verification details of the owner from Blockchain ledger before checkslip is generated at the SRO
- SRO and citizens can verify the encumbrance search details from tamper evident Blockchain ledger without any manual intervention

Stakeholders

Key stakeholders include:

- SRO/Property Registrar
- Revenue Department
- Survey and Settlement Department
- Citizens
- Other departments namely municipalities, etc.

PRMS is designed and developed by C-DAC Hyderabad and is supported by Information Technology, Electronics and Communications (ITE&C) department, National Informatics Centre (NIC) & Stamps and Registration departments of Telangana State Government. This activity is funded by the Ministry of Electronics and Information Technology (MeitY), Government of India.

Domain expertise, property records data of Shamshabad district are provided by the government departments and the Blockchain-based system is implemented by the C-DAC team.

Predicted outcomes

Features of the PRMS (user perspective):

- Verification details of the owner from the Blockchain ledger before a check slip is generated at the SRO/Property Registrar to avoid double registration and fake document registration.
- SRO/Property Registrar and citizens can verify the encumbrance search details from tamper-evident Blockchain ledger. It also provides assurance since the information is retrieved from a single source of truth.

Technology perspective:

- Loosely coupled architecture for easy integration with the existing workflow. This also facilitates the addition of components and stakeholders in the future.
- Solution is designed, implemented and pilot deployed to demonstrate the applicability of Blockchain technology for property registration.
- Standard REST APIs for accessing the application (this will allow integration with any other applications, departments or stakeholders).

Why distributed ledger technology?

This use case is based on leveraging blockchain to provide trust in the ecosystem of Property Record Management System, involving multiple stakeholders, enabling transparent and tamper-evident property records that are resilient to internal attacks, fake document creation problems and double selling scenarios.

8.2.3 User requirements

Functional requirements

- SRO/Property Registrar - expects to avail the benefits of reliable encumbrance search and verifying the owner details from Blockchain based PRMS whenever there is a request for change of ownership.
- Citizen - expects to avail the benefit of reliable encumbrance search from Blockchain based PRMS.
- Existing system - captures the complete registration process and provides the identified and significant property details to the blockchain based PRMS through web services.
- Blockchain based solution provider - expects the availability of Web Services from the Data Source entity (existing system).

Smart contacts

Purpose and Role of smart contract(s) within the PRMS (India)

Type	Purpose	Smart contract
Read (R)	For querying the property details based on regular document number and year	querypropertyByRegDoc
Write (W)	For recording the details of Check-slip transaction in the Blockchain	recordCheckslip
Write(W)	For recording the regular document number details to the Blockchain	recordRegDoc
Read(R)	For fetching the encumbrance search details from the Blockchain based on the regular document number and year	getFlistoryForRegDoc
Write (W)	–	initLedger

Visualizations: Figures 20 to 24

- **Reference architecture**

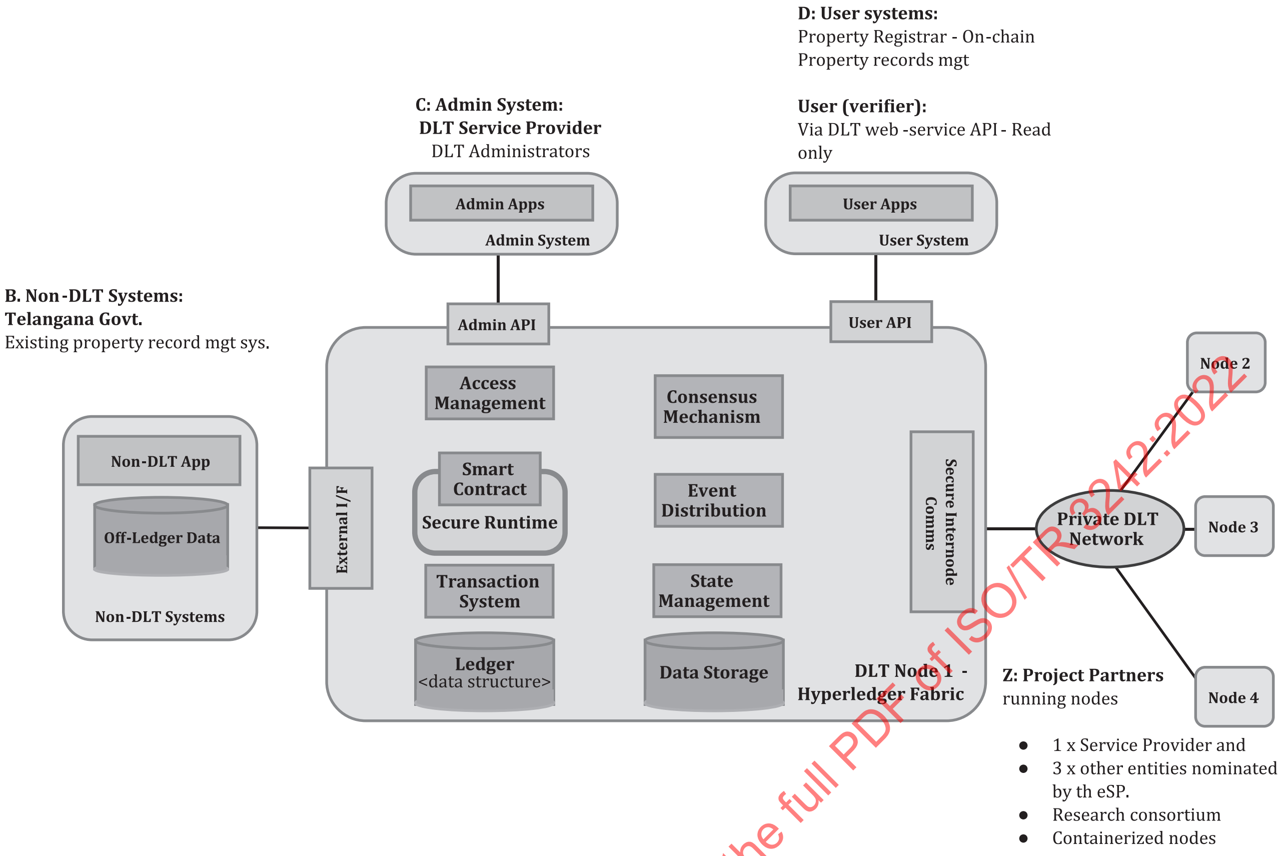
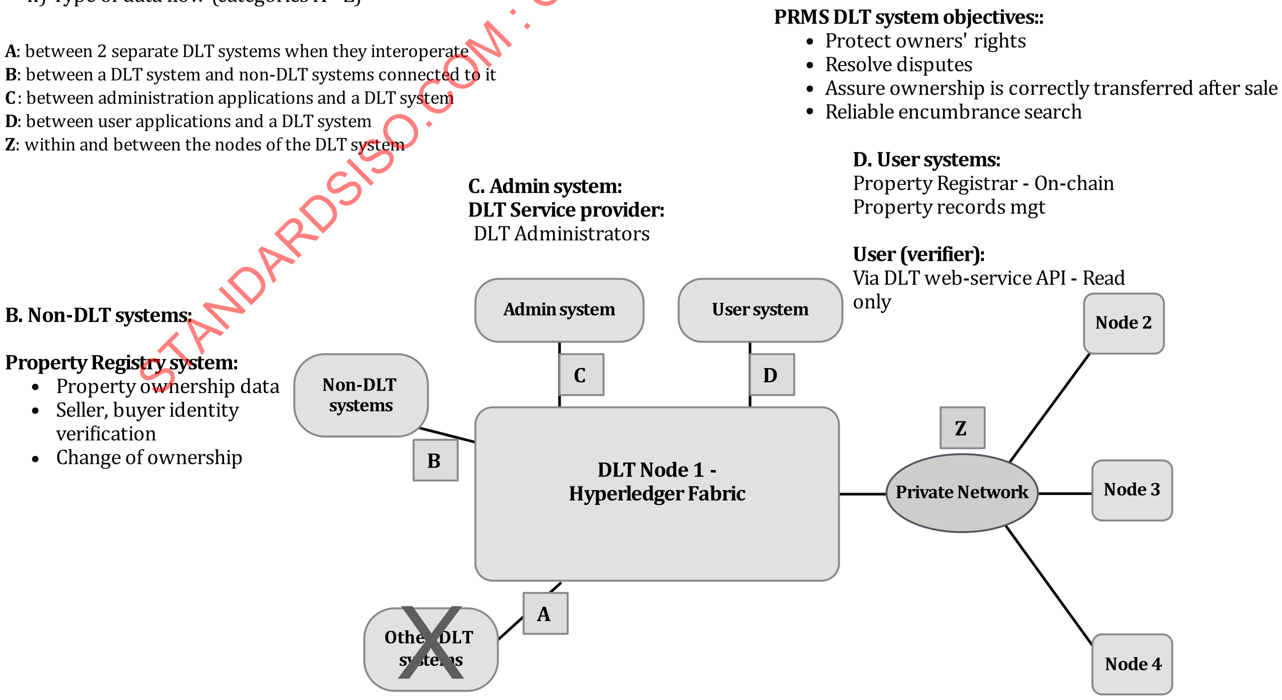


Figure 20 — System view architecture: PRMS (India)

— Data flow model

Service Provider.

ii) Type of data flow (categories A - Z)


A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

PRMS DLT system objectives::

- Protect owners' rights
- Resolve disputes
- Assure ownership is correctly transferred after sale
- Reliable encumbrance search

Figure 21 — Data flow analysis: PRMS (India)

— **Behavioural UML**

Use Case diagram

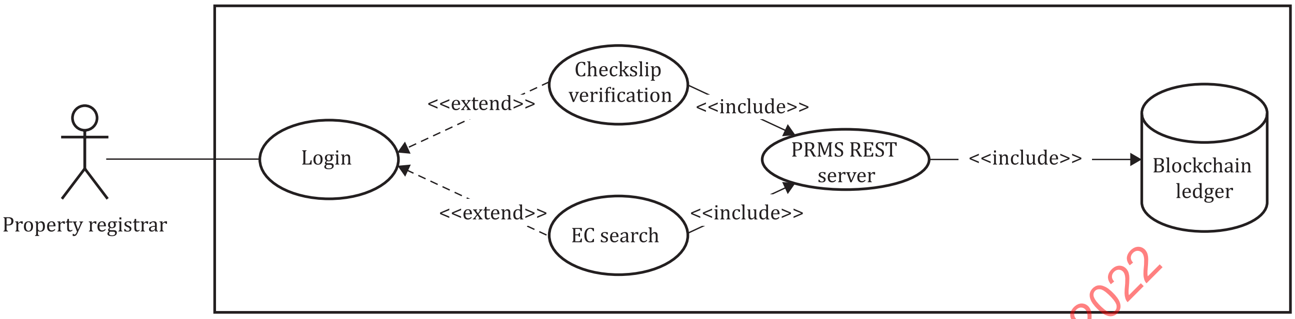


Figure 22 — Use case diagram: PRMS (India)

Interaction diagram

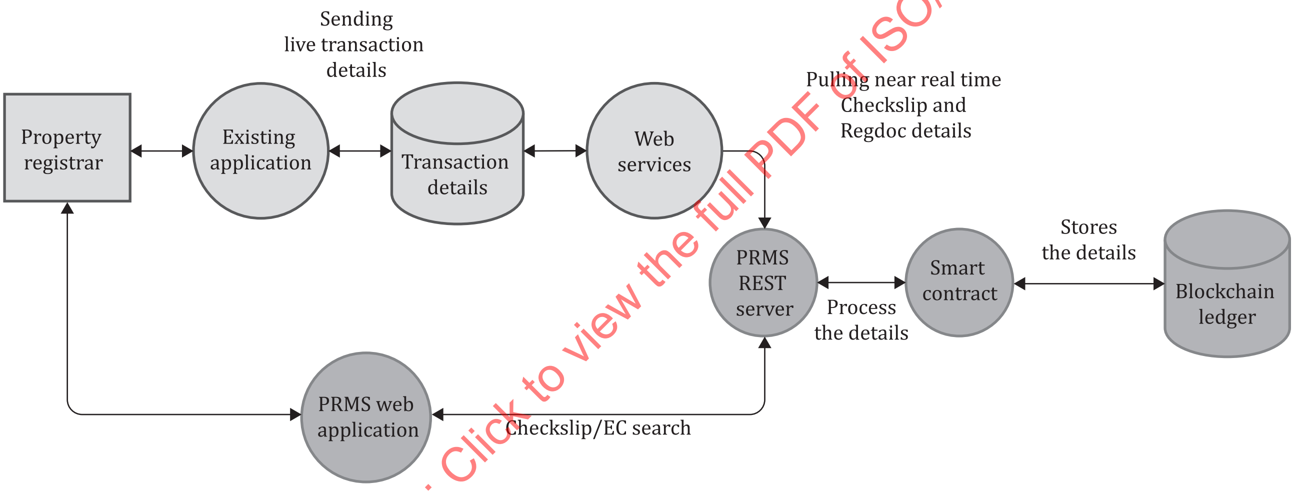
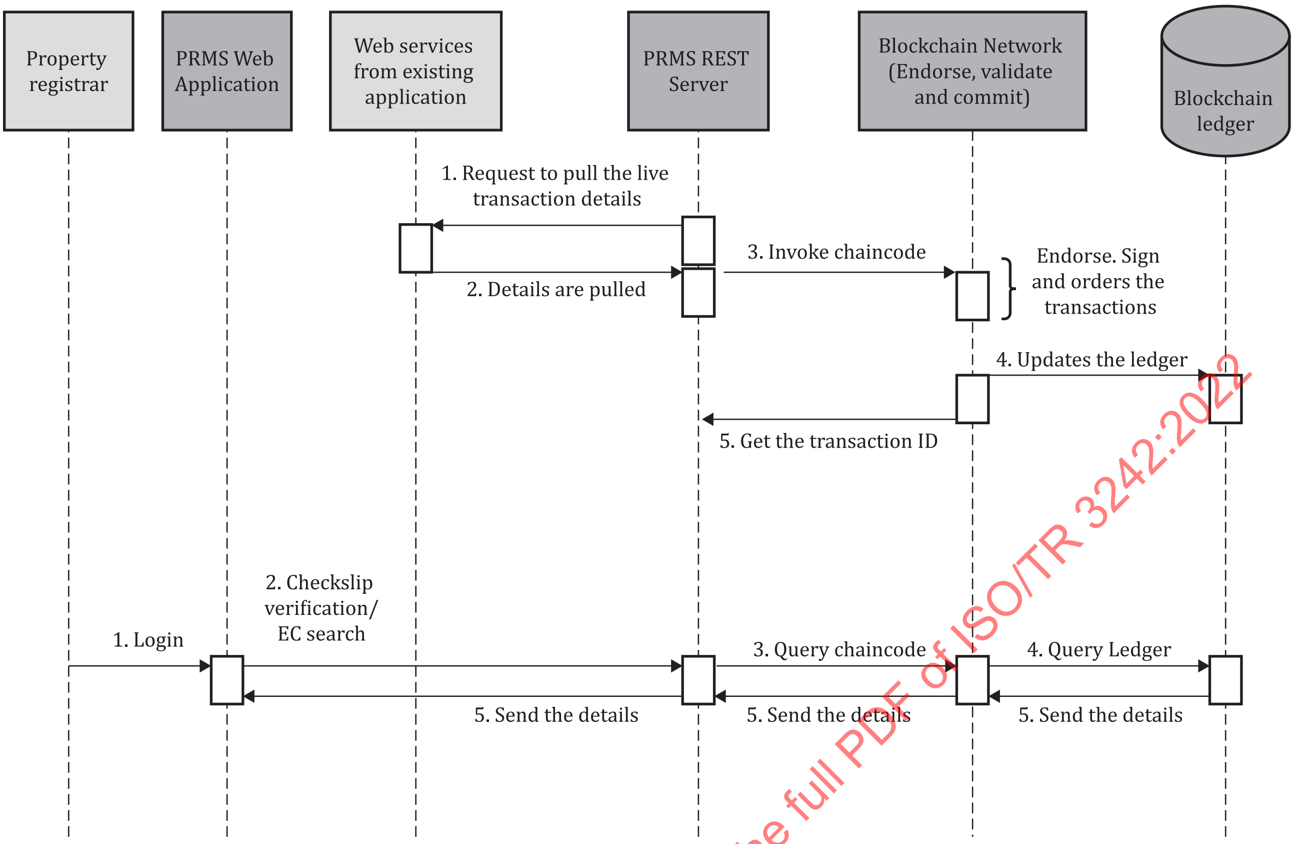


Figure 23 — Interaction diagram: PRMS (India)

Sequence diagram


Property registrar
PRMS Web Application
Web services from existing application
PRMS REST Server
Blockchain Network (Endorse, validate and commit)
Blockchain ledger
1. Request to pull the live transaction details
2. Details are pulled
3. Invoke chaincode
Endorse. Sign and orders the transactions
4. Updates the ledger
5. Get the transaction ID
1. Login
2. Checkslip verification/ EC search
3. Query chaincode
4. Query Ledger
5. Send the details
5. Send the details
5. Send the details

Key

▨ blockchain based application

□ existing application of telangana state govt.

Figure 24 — Sequence diagram: PRMS (India)

Security, privacy and identity management

— SRO's Authentication credentials are created by the PRMS and is checked every time someone accesses the system

— As the designed application is a permissioned Blockchain, privacy is applicable based on the user roles

— Authorization and authentication are enforced across the Blockchain stack, i.e. nodes, smart contract and application layer

— As it is a permissioned Blockchain, addition of nodes / users are created in a controlled environment with granular permissions

— Membership services is provided using standard public key cryptography mechanism

Pre and post conditions

— Use case assumes that integration points are available from existing application and that the system will get real time transactions from the existing application

— SRO will be enabled with the User Interface using which they can directly retrieve the details from Blockchain and verify them

Non-functional requirements

- Data from 2008 to 2018 for Shamshabad district is migrated to blockchain ledger
- Web services are used to pull the near real time transactions.
- For the Telangana State, 15,32,980 transactions have taken place in the year 2018
- It was observed that 0,15 transactions happen per sec
- Current Blockchain based system provides a throughput of approximately 10 tps for write operations and 12 tps for read operations (tps: transactions per second)

8.2.4 Force field analysis

Legal considerations

a) How to include e-stamp into the system to make it a complete ecosystem. Ref: e-Stamps service from Telangana State Government[28]

b) Currently PRMS is integrated with the existing application. If the technology is adopted to develop a solution from scratch, legal aspects are an additional consideration.

Risk:

If the solution is extended by automating the agreements and on-boarding all the stakeholders (banks, insurance agencies etc.,) it helps to prevent fraud but requires amendments to the supporting registration acts.

- Scalability is still to be tested as BCT is in its nascent stage as there are limited applications in the production.
- On boarding all the stakeholders from various departments to have a unified implementation is a big challenge.
- A unique identity is required for every property. In the present implementation it is derived based on Property details. A suitable mechanism is required considering several parameters one of which could include the latitude and longitude.

Other information:

The PRMS programme was initiated in 2017s with funding by the Ministry of Electronics and Information Technology (MeitY), Government of India. Further information:

Centre for Development of Advanced Computing[27]

Telangana State Government[28].

8.3 Student records management system (SRMS) India

8.3.1 Categories

Transversal Category

- 2. Public sector information and open data
- 5. Electronic identification, trust services, e-signatures

Horizontal Category

- 1. Identity Management
- 2. Data Provenance

Vertical Category

- ISIC Section J-6311: Information and Communication. Data processing, hosting and related activities. (p55)

UN Sustainability Goals

- List text. GOAL 4: Quality Education
- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 16: Peace and Justice Strong Institutions

Status: a completed trial or pilot

8.3.2 Summary

Long description

Academic certificates of students are used as supporting documents on several occasions by the students: for example, admission to other educational institutions, proof of date of birth, proof of credentials when joining an employer.

An academic record is a selection criterion in many places, so there is a huge motivation for malicious players to tamper with the database of the issuing system to alter the data to favour someone. Potentially, tampering with the database could lead to a student getting a falsified certificate.

Technically non-blockchain systems are vulnerable to tampering by system administrators who have the superuser password, and access to delete the audit trail logs to erase all traces of tampering.

A couple of such incidents bring disrepute to the institute and scepticism over the dependability of certificates of that institute. This impacts the other innocent alumni of the institute as well.

Using the blockchain to record the academic certificate's data immediately after their generation gives protection from such fraud. The trust in the institutes' certificates increases once its storage is blockchain.

Data sharing among departments of government, among educational institutes are also facilitated by each of them hosting a node.

Business problem or opportunity

The SSC board certificate is used as a source of truth for grade 10 scores, proof of date of birth, paternity authentication, etc. by the student. If that data is tampered with it affects several parties adversely. The data sharing speeds up several activities/approvals in government. The Indian regional Government of Telangana spotted the opportunity to fix this problem and is funding this initiative.

Scope

The potential of this solution is independent of geographic constraints and parameters. This use case was developed for the Education Sector and can be adapted to all industry sectors where immutability of documented information is expected.

Objective

The objective is to get rid of the problem of data tampering of certificate systems, which will facilitate trust in data sharing between different government departments or educational institutes.

Stakeholders

SSC Students, SSC Board, Private and Government Institutions to whom the student submits the document as a supporting document.

Predicted outcomes

Reduced fraud in education certification, increased confidence, process optimization in inter-departmental communications

Why distributed ledger technology?

- List text DLT makes the data immutable (tamper-proof) with its techniques of cumulative hashing and decentralization.
- Being a DLT, it enables data sharing (with access controls) among the different node hosting departments/educational institutions.

8.3.3 User requirements

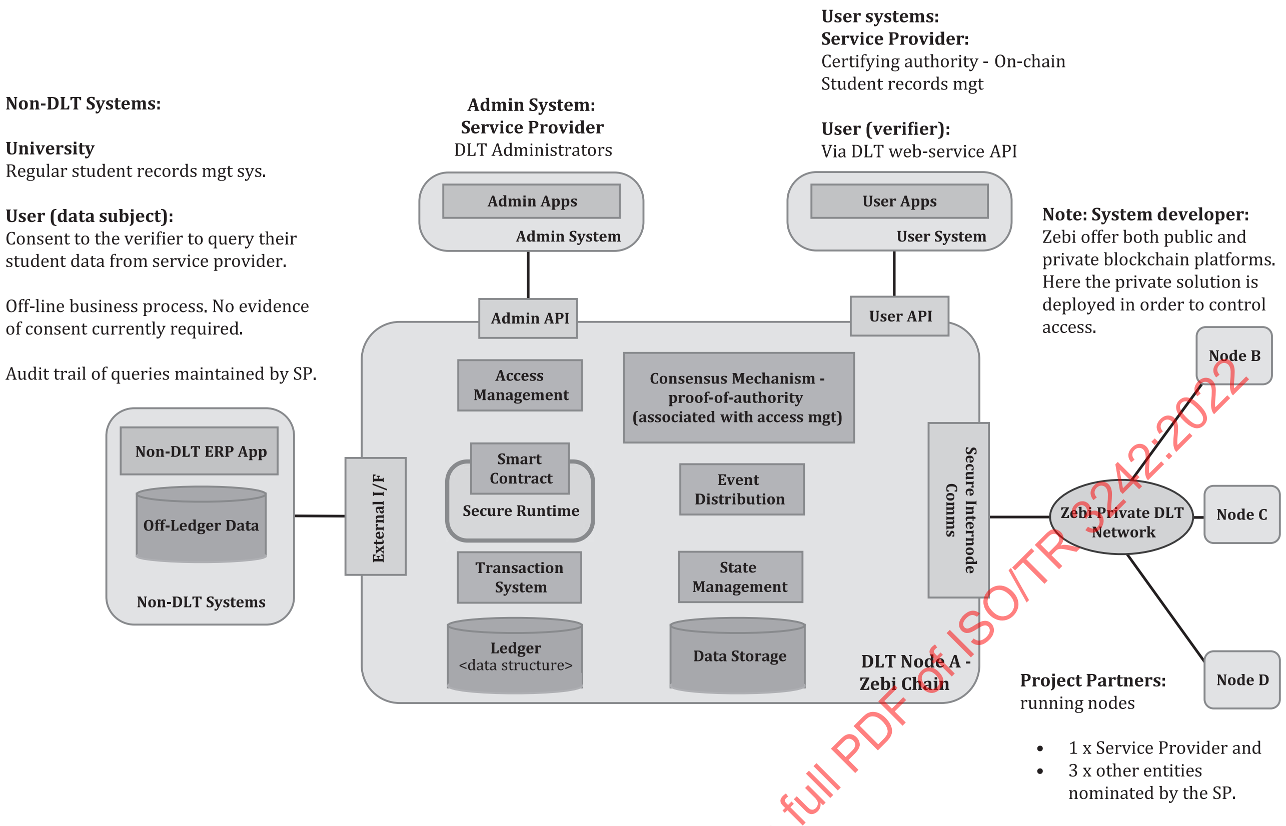
Functional requirements

- SSC student: system stores his academic certificate data and makes it immutable.
- SSC board: regular data transfer from existing non-blockchain system into this blockchain module.
- Certificate verification seeker: convenient way to verify authenticity of certificates submitted by a candidate as supporting document.
- Smart contracts to inform and alert relevant stakeholders on any form of tampering of records.

Visualizations: Figures 25 to 29

- **Reference architecture**

Telangana SSC Board Student Records and the use of blockchain



Non-DLT Systems:

University
Regular student records mgt sys.

User (data subject):
Consent to the verifier to query their student data from service provider.

Off-line business process. No evidence of consent currently required.

Audit trail of queries maintained by SP.

Admin System:
Service Provider
DLT Administrators

User systems:
Service Provider:
Certifying authority - On-chain
Student records mgt

User (verifier):
Via DLT web-service API

Note: System developer:
Zebi offer both public and private blockchain platforms. Here the private solution is deployed in order to control access.

Project Partners:
running nodes

- 1 x Service Provider and
- 3 x other entities nominated by the SP.

Figure 25 — System view architecture: SRMS (India)

— Data flow model

Telangana SSC Board Student Records and the use of blockchain

i) Stakeholders: Certifying authority (service provider), Student - data subject and consent provider, Verifier (user).

ii) Type of data flow (categories A- Z)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

Note: The content of the Student Certificate is recorded on-chain. Certification authority maintains custody of the student information in order to maintain a real world identity link. Immutability and tamper-resistance are the important blockchain features relied on here.

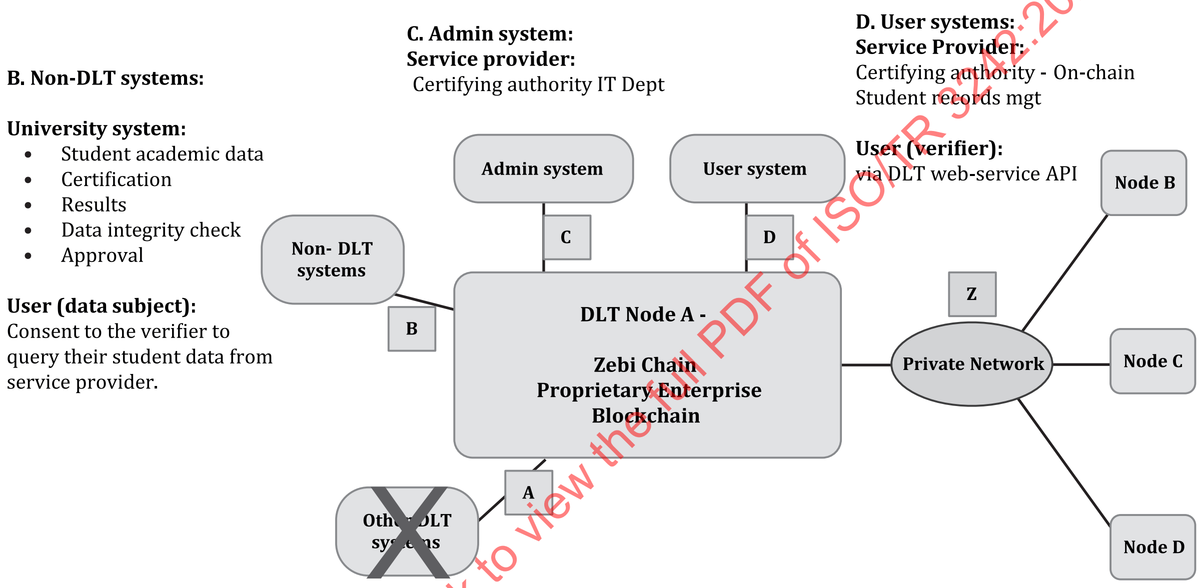


Figure 26 — Data flow analysis: SRMS (India)

— Behavioural UML

Use Case diagram

Telangana SSC Board Student Records and the use of blockchain

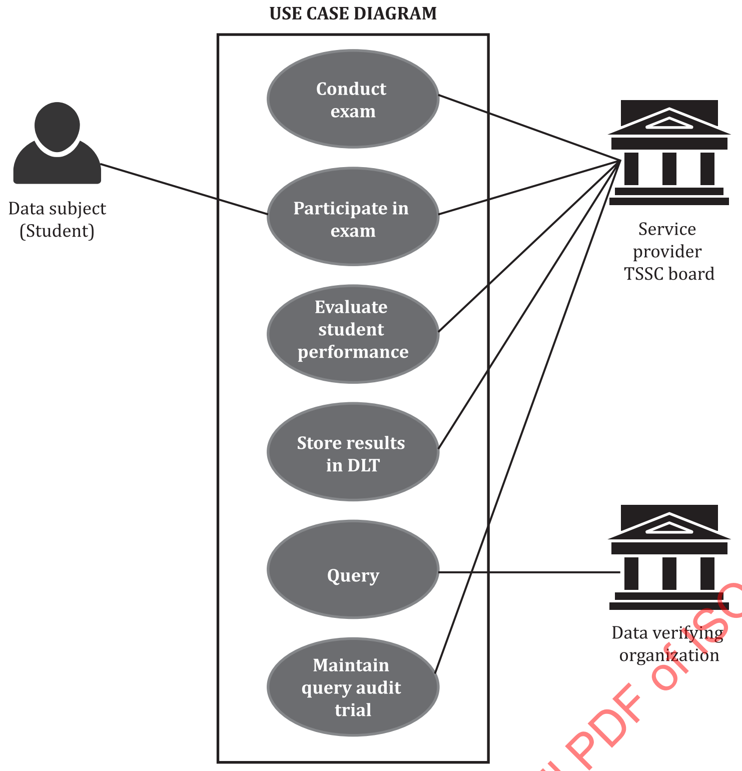

USE CASE DIAGRAM
Conduct exam
Participate in exam
Evaluate student performance
Store results in DLT
Query
Maintain query audit trial
Data subject (Student)
Service provider TSSC board
Data verifying organization

Figure 27 — Use case diagram: SRMS (India)

Sequence diagram

Telangana SSC Board Student Records and the use of blockchain

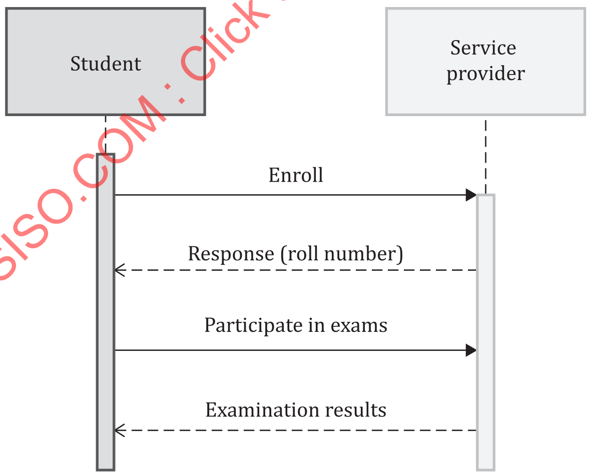


Figure 28 — Sequence diagram: SRMS (India) – Enrol student

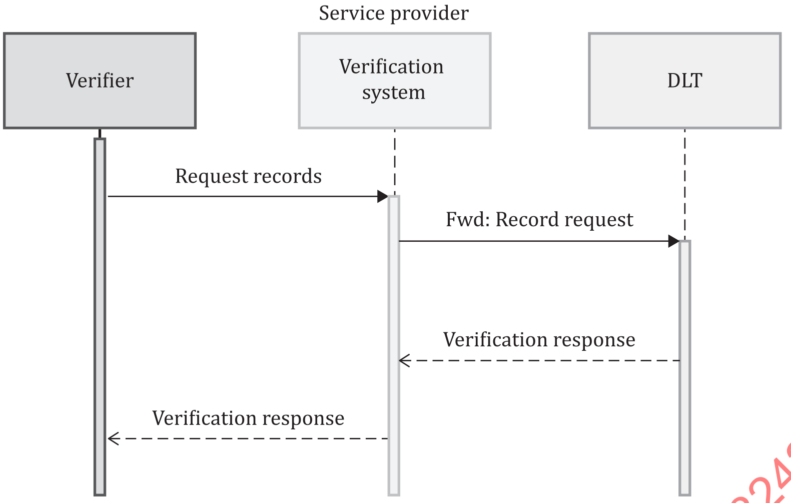


Figure 29 — Sequence diagram: SRMS (India) – Verify record

Security, privacy and identity management:

There are various security features of authentication, authorization (role-based access control), and https (TLS) mode of transfer.

This also safeguards the privacy of the student because here the verification requestor directly interacts with blockchain system for verification as opposed to traditional way of engaging a background verifier and the certificate copies passing through multiple hands.

Pre and post conditions:

Preconditions

- fully automated method of transferring historic data from existing system's RDBMS into blockchain without any human handling or the chance for tampering en-route.
- the multiple blockchain nodes to be spread across different custodians.

Post conditions

- queries on the portal of the departments retrieve and display data from blockchain storage and not from the non-blockchain RDBMS.
- the non-blockchain RDBMS storage can be totally removed to avoid data duplication.

Non-functional requirements:

- The system handles volumes of 500,000 students' certificate data per year.
- High Availability: being a DLT the new system doesn't have a single point of failure and hence resilient.
- Quick responses to queries.

8.3.4 Force field analysis

Legal considerations:

At present, there is no additional legal protection for data stored on blockchain vs data stored on non-blockchain system. Source of truth in event of inquiry is the response from the department. Of course, the department would provide the response by querying on blockchain.

Data privacy standards are followed while storing the data on blockchain as well; Sensitive fields are encrypted and stored. Fields such as Aadhaar (UID-biometric identity field) are not stored along with the other data.

With or without blockchain the department is responsible for the integrity of the data. Blockchain technology helps the department greatly in fulfilling this responsibility.

Risk:

Before and after the implementation, the data is owned by the SSC board department. With blockchain implementation they are effectively nullifying the risk of potential data tampering in that data.

However, risk of data leakage increases a bit with blockchain implementation because now there are multiple nodes (under different custodians) storing full data set; so the burden of preventing unauthorized reads of the data will increase.

This can be mitigated by encrypting the data and storing in the blockchain nodes. Data can also be fraudulently changed by bypassing the application UI layer. Data provenance and integrity remain important concerns.

Referenced standards:

SHA-256 cryptography standard.

Other information:

The implementation cycle was within a month, which is considered to be rapid.

This is a dual-system proof-of-concept approach. It is hoped that eventually the non-blockchain system would be retired.

It is the department's prerogative to decide which datastore is the system of record. But being tamper-proof, the blockchain would be a good choice for a system of record.

Further information: Zebi Data India Pvt[29].

8.4 Education certificates provenance (Singapore)

8.4.1 Categories

Transversal Category

2. Public sector information and open data

5. Electronic identification, trust services, e-signatures

8.Accessibility of ICT products and services

Horizontal Category

2. Data Provenance

5. Process Optimization

6. Automation

Vertical Category

a) ISIC Section J - Information and communication (p. 56, ISIC, Rev.4) Group 631 Data processing, hosting and related activities; web portals

b) ISIC Section P - Education (p. 59, ISIC, Rev.4)

c) 8522 Technical and vocational secondary education

d) 8530 Higher education

e) 8549 Other education n.e.c.

UN Sustainability Goals

- List text.
- GOAL 4: Quality Education
- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 16: Peace and Justice Strong Institutions
- GOAL 17: Partnerships to achieve the Goal

Status: in production/live implementation

8.4.2 Summary

Long description

Certificate Issuing organizations such as Institute of Higher Learning (IHL) organisations issue digital certificates in the OpenCerts format to graduating students. The students can then use these certificates in a job application or as a supporting document in an application for further studies.

To combat education fraud:

- Verifiers of an OpenCerts certificate will be informed if a certificate had been revoked, without having to check back with the issuing organisation. Unlike PDFs which have been signed digitally, OpenCerts certificates can be revoked post-issuance for example, if a student was found to have cheated. Previously, the holder of the certificate could still be in possession of his/her certificate, even though it had been revoked, and could still share with unsuspecting recipients.
- Traditionally, the request of verification is submitted to the issuing organisation, e.g. an Institute of Higher Learning (IHL). This requires time and effort to retrieve and verify the certificate from the IHL's system.
- Leveraging on the Ethereum public blockchain,

This use case provides an approach to decentralize the verification of certificates, and provided an opportunity to improve:

a) Speed of verification:

In comparison to a traditional request of contacting an educational institute to verify the authenticity of a given certificate, which could take days, if not weeks to be completed. OpenCerts platform provides an alternative to verify the provenance of the education certificates data in a matter of seconds.

b) Selective disclosure of information within a certificate:

The application of pre-computed cryptographic checksums enabled certificate holders can selectively share information from their certificate, without compromising the data provenance properties of the document.

c) Costs savings and possibility to redeploy IHL's resources which had been previously tasked with verification of certificates.

Business problem or opportunity

Issuance of Verifiable Credentials which could be easily communicated and verified, independent of country of issuance and country of verification.

Scope

The use case has applications internationally, mainly in the Education and Vocational training sectors. However, the technology allows for it to be applied to any type of document with structured data. OpenCerts is open-sourced, and available for any interested parties/organisations to adopt and implement.

Objective

- Quick verification of certificates on a single portal
- Reduce certificate fraud
- Empowering certificate holders to control the information to be shared

Stakeholders

- Students
- Organisations issuing certification
- Verifier of certificate
- SkillsFuture Singapore

Predicted outcomes

- Predicted outcomes:
- Quick verification of certificates on a single portal
- Reduce certificate fraud
- Empowering certificate holders to control the information to be shared

Why distributed ledger technology?

Improved service availability on blockchain

- No longer dependent on the issuing organisations' system uptime. It also lowers the barrier to entry as issuing institutes need not run their own highly available infrastructure or verification portal.

Selective disclosure of information

- Pre-computed cryptographic checksums enable certificate holders to selectively redact information from a certificate, without compromising document's data provenance properties.

Revocation of a certificate post-issuance

- Unlike PDFs which have been signed digitally, OpenCerts certificates can be revoked post-issuance, for instance, if a student was found to have cheated. Previously, the certificate holder could still be in possession of a certificate post-revocation and continue to share it with unsuspecting recipients. Verifiers of an OpenCerts certificate will be informed if a certificate had been revoked via the OpenCerts portal.

8.4.3 User requirements

Functional requirements

- Students: A shorter processing or evaluation time when certificates are submitted.
- Organisations issuing certification: Automated service to validate the authenticity of a certificate's data
- Verifier of certificate: Fast and simple verification process.

DocumentStore smart contract:

- This smart contract is deployed once per issuer. The smart contract's responsibilities are to:
  - Only allow modifications by the owner
  - Store and retrieve a list of hashes that have been issued, and when they were issued
  - Store and retrieve a list of hashes that have been revoked, and when they were revoked

Visualizations: Figures 30 to 34

- **Reference architecture**

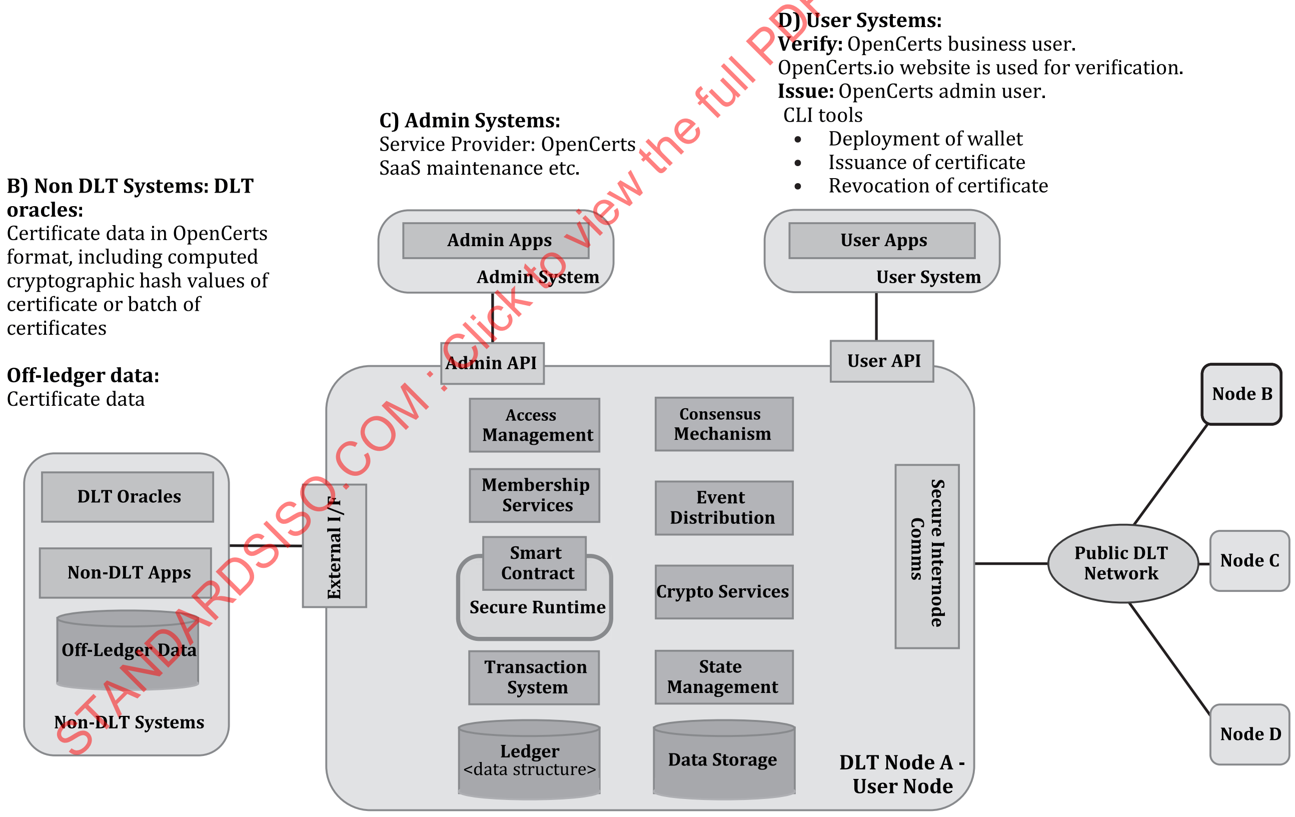


Figure 30 — System view architecture: Education Certificates Provenance (Singapore)

- **Data flow model**

Data flows triggered by the data-related operations of each stakeholder:

i) Stakeholders: **GovTech, Inst Higher Learning, Skills Future Singapore, Students, Business Community (verify)**

Type of data flow (categories A- Z)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

C) Admin Systems:
Consortium of 18 issuer organizations, comprising of IHLs, Educational and Training certificate issuing bodies. Government Technology Agency of Singapore provides the framework (APIs and CLI tools) which have been open-sourced. Each issuer organization needs their own IT personnel to support development and deployment.

D) User Systems:
Verifier of certificates eg. (prospective employers, students, or persons verifying a certificate) are able to do so on a web browser. Process of verification is free-of-charge (crypto wallet setup is not required). view at www.OpenCerts.io

Issuer Organisations: API and CLI tools to deploy smart contract, issue and revoke certificates. During issuance and revocation, cryptographic hash are published onto the public blockchain, for comparison during verification.

B) Non DLT Systems:
IHL issues certificates in OpenCert (json compatible format). The certificate(s) are cryptographically hashed, and the hash recorded the blockchain, which is then used for comparison during verification.

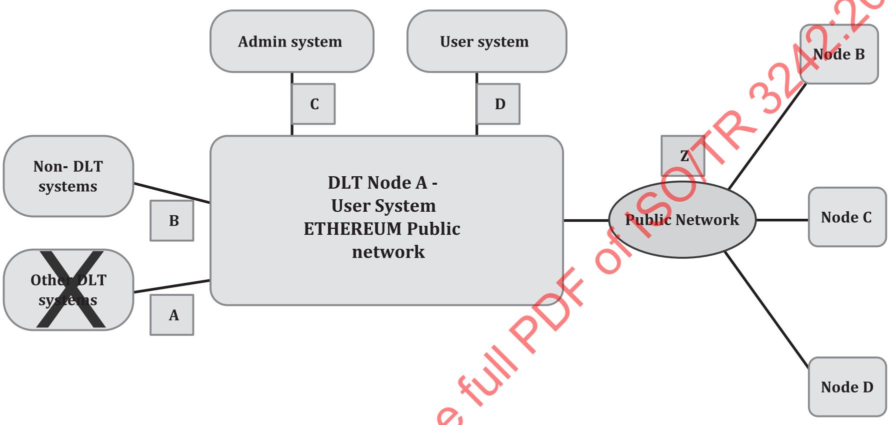


Figure 31 — Data flow analysis: Education certificates provenance (Singapore)

— **Behavioural UML**

Use Case diagram

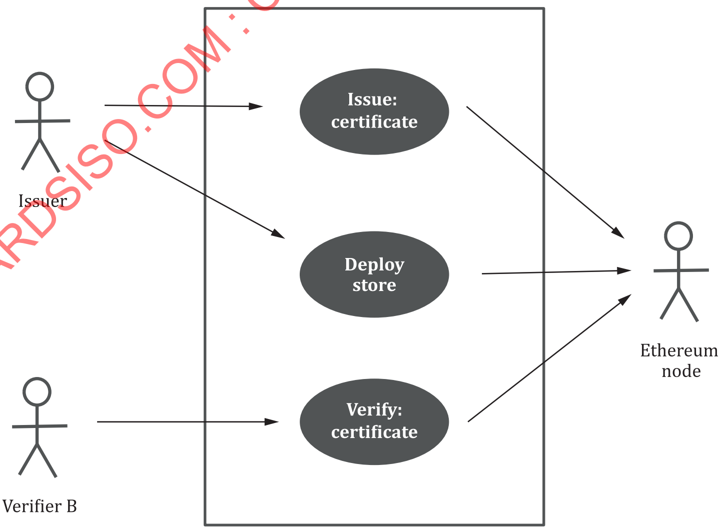


Figure 32 — Use case diagram: Education certificates provenance (Singapore)

Sequence diagram

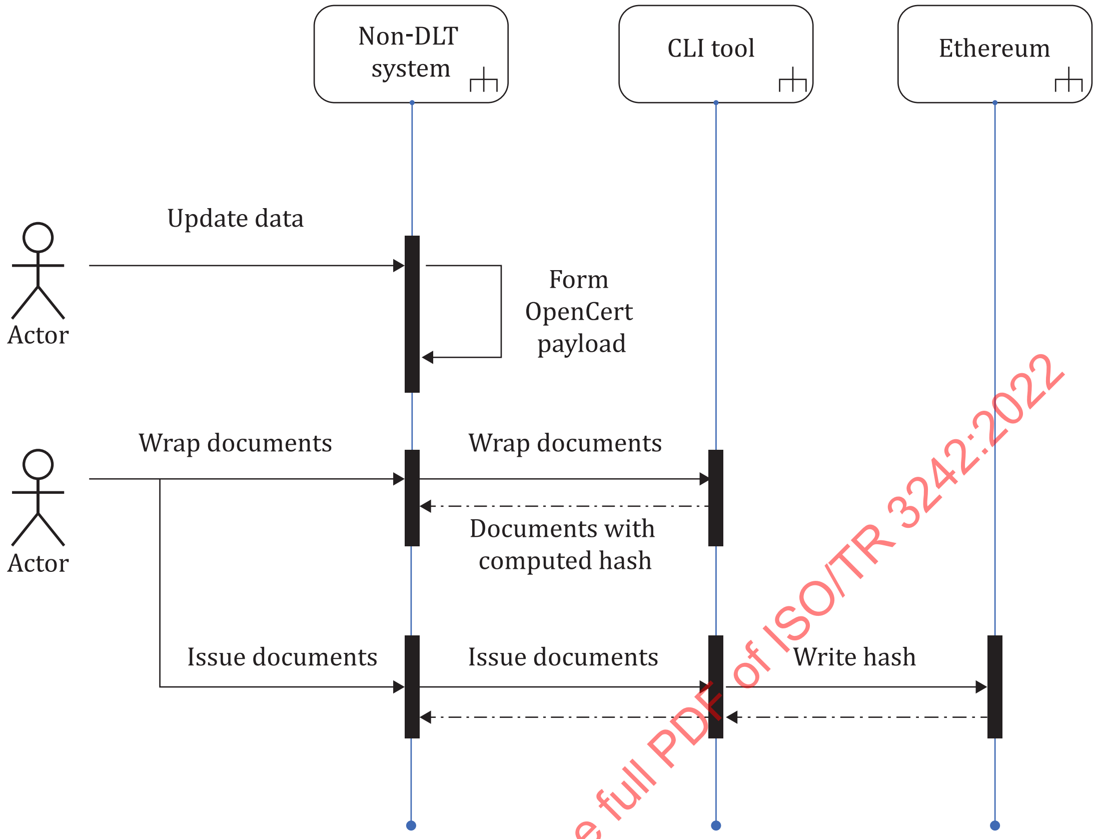


Figure 33 — Sequence diagram: Education certificates provenance (Singapore) – Register certificate

Sequence diagram

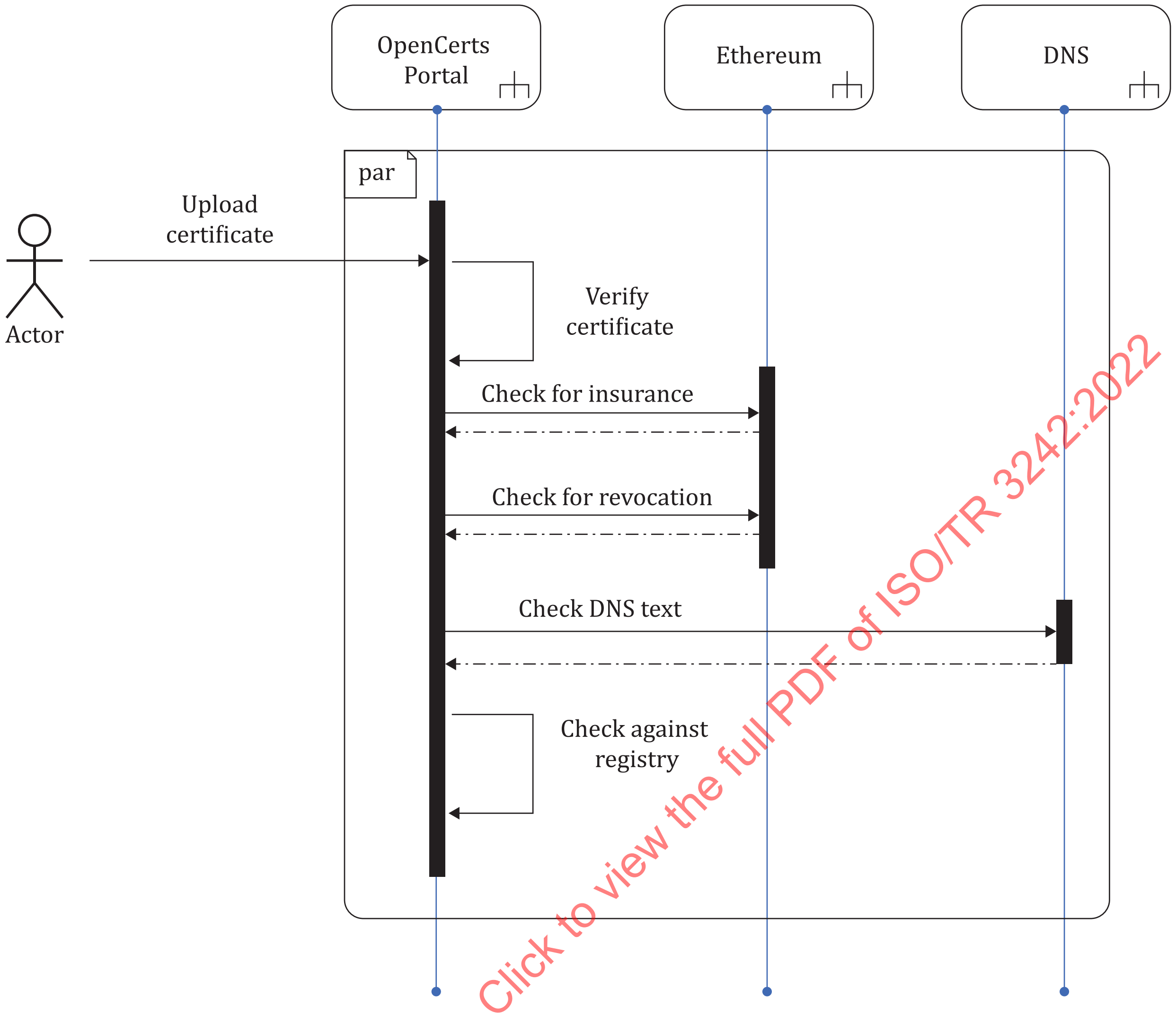


Figure 34 — Sequence diagram: Education certificates provenance (Singapore) – Verify Certificate

Security, privacy and identity management:

Certificate holder can decide with whom to share the certificate, as well as which parts of the certificate to be shared.

When the verifying party uploads the certificate to the OpenCerts.io portal for verification, the portal does not store a copy of the certificate, ensuring the certificate is held only by intended recipients of the data.

Verification does not require an interaction with the issuer's system, thus reducing the need to expose a public endpoint, which in turn reduces the potential attack surface.

Pre and post conditions:

An internet connection is required to upload the certificate onto the OpenCerts.io portal, and also for verification process which checks against Ethereum's distributed ledger.

Non-functional requirements:

The write-once, read-often nature of certificate issuance data was taken into consideration when developing OpenCerts. This was a good fit for DLT, as the performance limitations of DLT only affect writing data. OpenCerts also sidestepped the cost/slowness of storing large amounts of data on the

DLT by allowing the batching of a theoretically infinite number of documents into one issuance. This is achieved by using the Merkle tree data structure.

By making the verifying application a static website that queries the DLT directly, it simplifies the architecture greatly and makes high availability extremely easy to achieve. This can be likened to having only client-side software without a server involved. As such, the system is available for verification as long as an Ethereum node is reachable.

Since issuance is not usually real-time critical, the limitations caused by the confirmation time of the ledger is acceptable as long as it is <1 day or even more depending on the institution. Even when Ethereum was congested at the peak of CryptoKitties, the confirmation time never exceeded a day with some elevation in gas costs.

8.4.4 Force field analysis

Legal considerations:

In the current rollout of OpenCerts, there is a provision for DIDs.

However, there is a constraint that no DID resolution framework is available for integration currently. Consequently, ownership of a certificate on its own can be insufficient depending on the rigour of the verification process.

Risk:

Due to current constraints on positively identifying the purported owner of a certificate, two or more persons bearing an identical name, as listed in the certificate, can claim ownership of the OpenCert. In some instances, the issuer organisation includes a unique student identifier within the certificate, which can supplement as supporting document to mitigate the risk of identity fraud.

Open Source Software:

Scenarios

- Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.
- Reference implementation (to show that a specification is implementable)
- Required part of a standardization deliverable
- Complementary to a standardization deliverable
- Test suites, unit tests, etc. for functionality tests

Assessment of Engagement

- D. Open Source Software is critical for a successful adoption
- F. It was easy to collaborate with Open Source Software communities
- H. Open Source Software is critical for validation of implementations

Other information:

OpenCerts started off as a proof of concept when a local IHL shared its use case with the Government Technology Agency of Singapore.

Key considerations:

- Certificates aretamper-proof

- Reduce the effort required to verify certificates (the traditional verifications were taking 7 man-month effort per annum).
- Ease the certificate replacement process

The success of the proof of concept led to the formation of a consortium, comprising of 18 issuer organisations (representing IHLs, Educational and Training certificate-issuing bodies.

OpenCerts started off as a proof of concept when a local IHL shared its use case with the Government Technology Agency of Singapore.

8.5 Content timestamp verification (Netherlands)

8.5.1 Categories

Transversal Category

- 2. Public sector information and open data
- 5. Electronic identification, trust services, e-signatures
- 7. e-Infrastructures for research

Horizontal Category

- 1. Identity Management
- 2. Data Provenance
- 5. Process Optimisation
- 6. Automation

Vertical Category

- ISIC Section, J6399. Information and Communication Section. Other information service activities n.e.c. (p.56)

UN Sustainability Goals

- GOAL 4: Quality Education
- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 16: Peace and Justice Strong Institutions
- GOAL 17: Partnerships to achieve the Goals

Status:

5. in production/live implementation

8. an integration with current systems

8.5.2 Summary

Long description

Websites built with WordPress can use the Content Timestamp Verification process with WordPress plugin to timestamp content on the blockchain. Other platforms can use the Document Timestamp API by WordProof.

The input of a timestamp depends on the post type (e.g. post, page, and product) and is based on the open-source Timestamp Standard.[30] The content is bundled, hashed and added to the blockchain in a transaction. Content creators can sign the transaction with their own blockchain account or with the WordProof blockchain account.

After content has been timestamped on the blockchain, websites can show the so-called blockchain certificate pop-up at the bottom of the timestamped content with the title, date and time, hash and, optionally, revisions of the content. Website owners can also download the Blockchain Certificate as a PDF, proving the existence of the content on their website at different moments in time, helping with copyright related claims. Visitors can use the pop-up certificate to compare different versions of the content and see (and verify) how the content has changed over time. Additionally, the certificate shows when the content was last updated (and proofs that the content was not changed since that time).

Business problem or opportunity

This addresses the problem of copyright violation. Creative content can be stolen or copied where content creators often don't have proof of ownership. Content users can currently tamper with information presented on a website, such as the "last edited on" date, so changes are not transparent to visitors. WordProof offers a strong toolset which enables trust for both content creators and website visitors, leading to a more reliable and trustworthy internet.

Scope

Global reach. Every content creator and web visitor.

WordProof's timestamps are added to the structured data of websites that search engines and social media platforms can parse.

Objectives

- Assist content creators to automate the process of asserting authors rights over their creative output without needing a third party, in an integrated digital way.
- Pre-emptively aid in dispute resolution in case of a copyright infringement.
- Increase trust for website visitors by providing tools to do due diligence (for example: how did the content change over time, has the content been modified since the last timestamp, how can the website be held accountable for the information that was presented at specific moments in time).
- Search engines can verify the trustworthiness and history of the content.

Stakeholders

a) Website visitors accessing published information that directly impact their decision-making.

b) Content creators who can pre-emptively build a case for copyright infringements without expensive legal fees.

Predicted outcomes

WordProof wants to improve the trustworthiness of the internet by timestamping content on the blockchain. Content creators get the tools to fight copyright infringements, while website visitors can see the origin of content and hold content creators accountable.

Why distributed ledger technology?

Trust in the internet is declining and website visitors actively change their behaviour as a result. Websites can claim that the content was last edited at a certain time, but visitors can't verify such a claim, or can't see how content has changed over time. Even if websites would show some sort of history function, the data would still come from the website's database and thus will not be automatically trusted by the website visitors.

Current solutions all depend on a centralized database where the website controls all the data - including the history of content and the times at which the content was updated. Blockchain provides a trust framework where transactions are immutable and the network is distributed.

Where content creators don't have ways to assert ownership unless they go to a notary. Adding a hash to the blockchain, which is immutable, transparent and distributed, is a more affordable alternative

8.5.3 User requirements

Functional requirements

- A website visitor would like to verify when content was last updated to ensure that what is being read today, is the same as what was read yesterday.
- A website visitor would like to verify how content changed over time to see what changes were made.
- A content creator would like to obtain proof that their content existed on their website at certain moments in time, without the need for a notary.
- A content creator would like to be transparent about their content changes to increase the trustworthiness of their website.
- A content creator woukd like to ensure intellectual property rights because the current solution is not effective in the digital era.

Visualizations: Figures 35 to 38

- **Reference architecture**

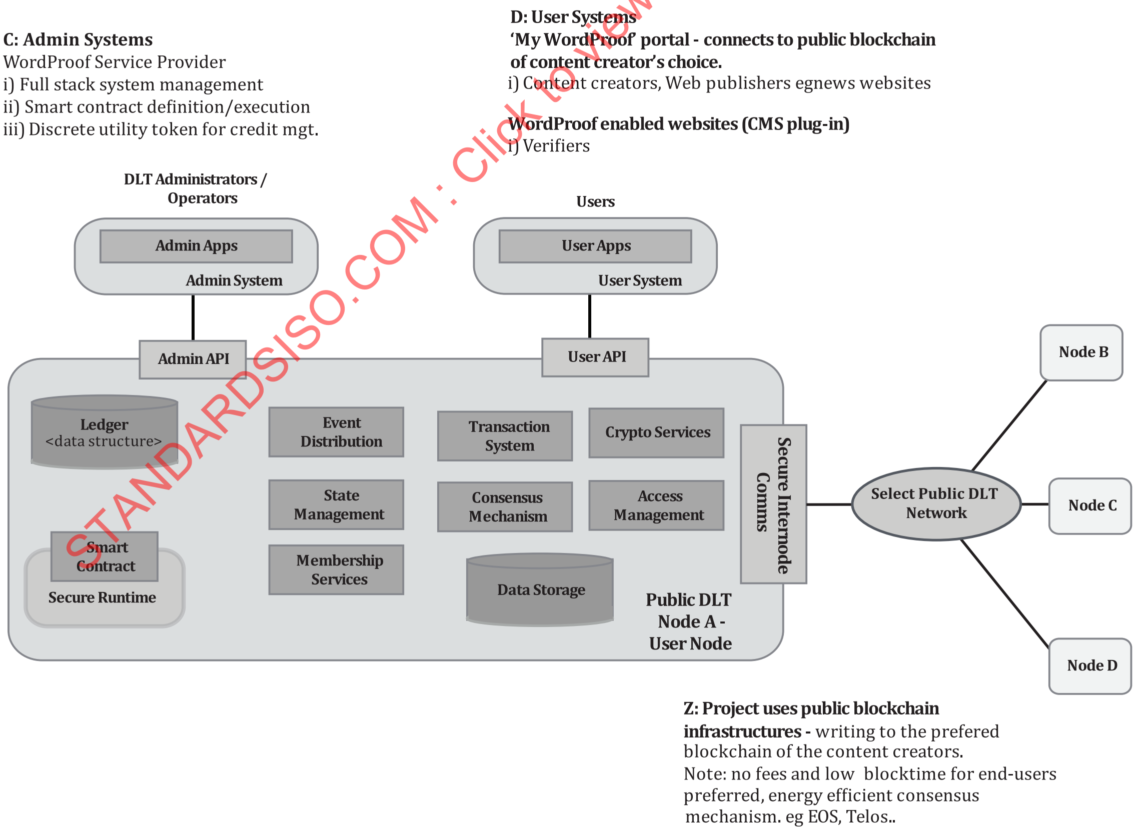

C: Admin Systems
WordProof Service Provider
i) Full stack system management
ii) Smart contract definition/execution
iii) Discrete utility token for credit mgt.
D: User Systems
'My WordProof' portal - connects to public blockchain of content creator's choice.
i) Content creators, Web publishers egnews websites
WordProof enabled websites (CMS plug-in)
i) Verifiers
DLT Administrators / Operators
Admin Apps
Admin System
Users
User Apps
User System
Admin API
User API
Ledger <data structure>
Event Distribution
Transaction System
Crypto Services
State Management
Consensus Mechanism
Access Management
Smart Contract
Secure Runtime
Membership Services
Data Storage
Public DLT Node A - User Node
Secure Internode Comms
Select Public DLT Network
Node B
Node C
Node D
Z: Project uses public blockchain infrastructures - writing to the prefered blockchain of the content creators.
Note: no fees and low blocktime for end-users preferred, energy efficient consensus mechanism. eg EOS, Telos..

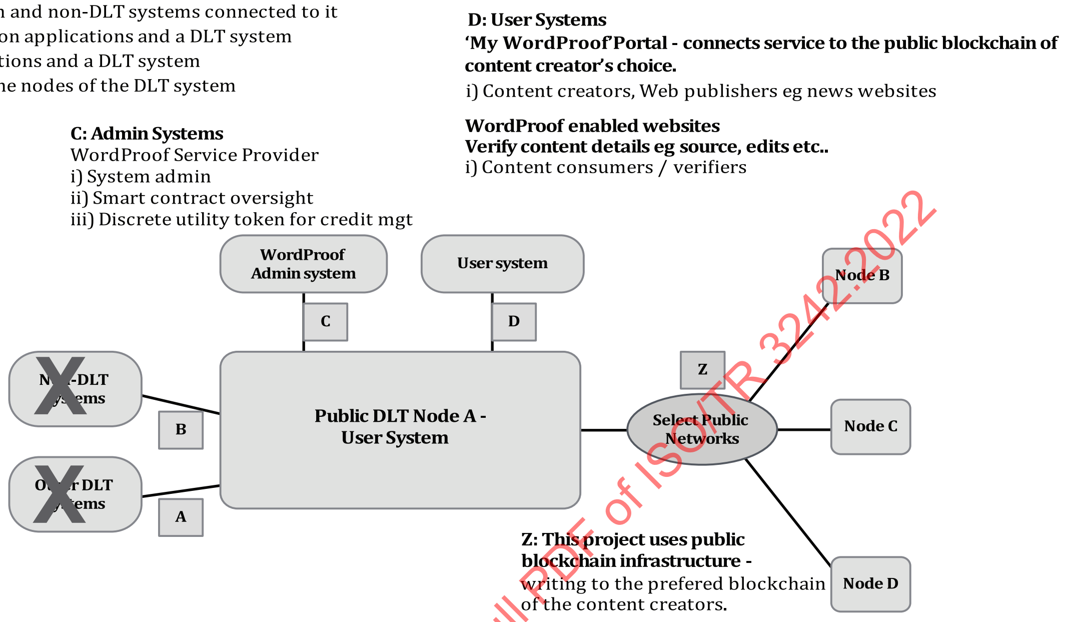
Figure 35 — System view architecture: Content timestamp verification (Netherlands)

- **Data flow model**

Data flows triggered by the data-related operations of which stakeholders.

i) Specify the role of each stakeholder in facilitating the data flow: **Content publisher, content verifier, service provider.**
ii) Identify the type of data flow (See categories A-Z below)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system



D: User Systems
'My WordProof' Portal - connects service to the public blockchain of content creator's choice.
i) Content creators, Web publishers eg news websites

WordProof enabled websites
Verify content details eg source, edits etc..
i) Content consumers / verifiers

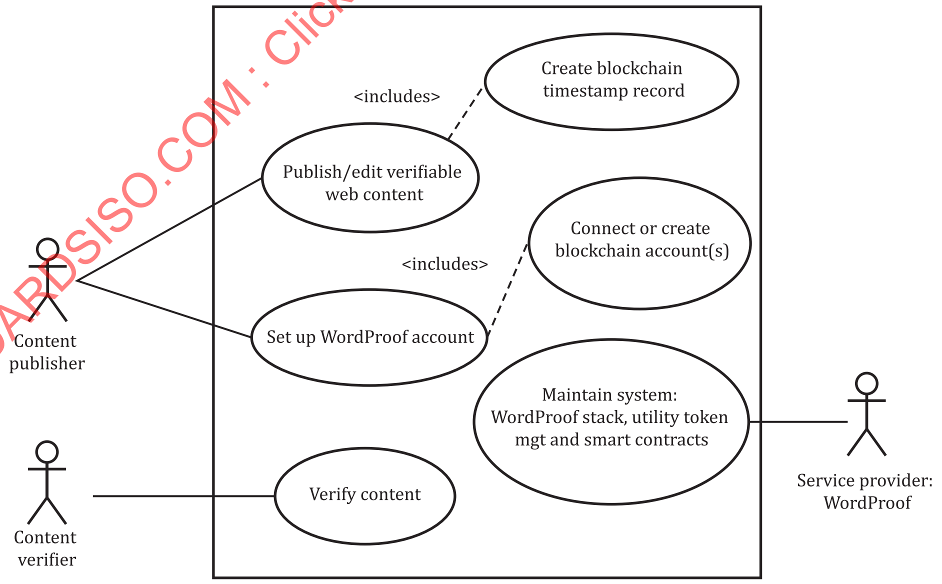
C: Admin Systems
WordProof Service Provider
i) System admin
ii) Smart contract oversight
iii) Discrete utility token for credit mgt

Z: This project uses public blockchain infrastructure -
writing to the prefered blockchain of the content creators.

Figure 36 — Data flow analysis: Content timestamp verification (Netherlands)

— **Behavioural UML**

Use case diagram



<includes>
Create blockchain timestamp record
Publish/edit verifiable web content
Connect or create blockchain account(s)
<includes>
Content publisher
Set up WordProof account
Maintain system: WordProof stack, utility token mgt and smart contracts
Service provider: WordProof
Content verifier
Verify content

Figure 37 — Use case diagram: Content timestamp verification (Netherlands)

Sequence design diagram

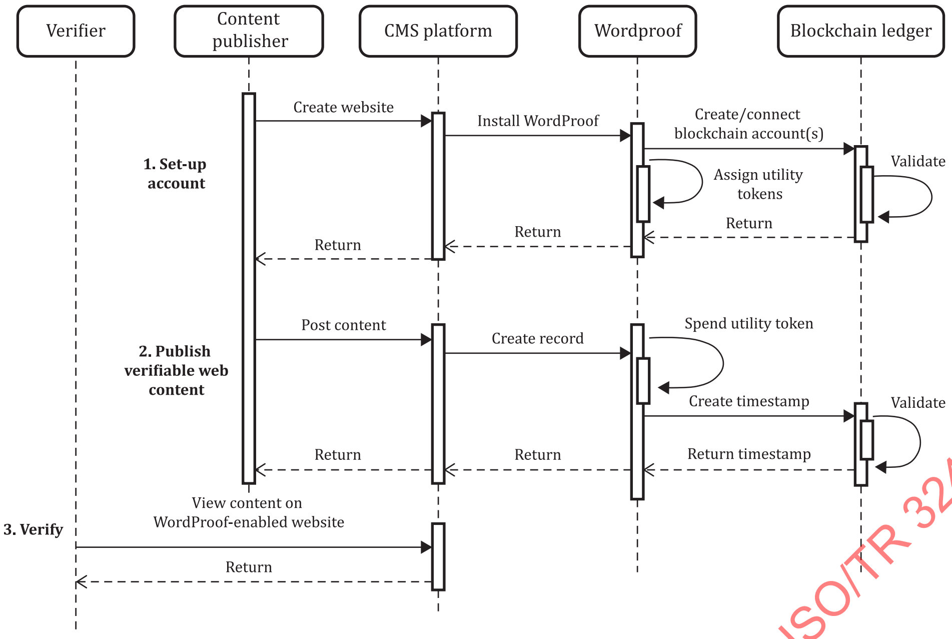


Figure 38 — Sequence diagram: Content timestamp verification (Netherlands)

Security, Privacy. Identity management:

Regarding security and privacy, the hash of content is added to the blockchain, not the content itself, because that might contain sensitive information. It is impossible to derive the content from the hash. In the end, no personal data is placed in the blockchain.

Regarding identity, Content Timestamp Verification users using WordProof's automated timestamping service create a ‘My WordProof’ account in an off-chain system with their name, email, website URL, and password. If a plan is chosen, accounts includes their address and optional VAT number.

WordProof employee access to the database is limited and employees have signed contracts against sharing information with third parties.

Pre- and post-conditions

Pre: Content must be transformable into a string of characters before it can be hashed and added to the blockchain.

Post: The transaction on the blockchain is indisputable proof that the content existed at the moment of the transaction

Non-functional conditions

Transactions need to be immutable and the network distributed so that the timestamps maintain value. Scalability and responsivness of the system as the usage of the solution increases.

Content Timestamp Verification easily adapts to blockchains conform protocols that are scalable, interoperable and reliable.

8.5.4 Force field analysis

Risk:

GDPR can be challenging as content in a blockchain, which is immutable by design.

Adaptation to evolving legal requirements.

Open source software:

- Scenarios engaged with Open Source Software:

1. Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.

6. Other: Timestamp standard

- Assessment of engagement in Open Source Software:

D. Open Source Software is critical for a successful adoption

F. It was easy to collaborate with Open Source Software communities

H. Open Source Software is critical for validation of implementations

Other information:

A key lesson learned is to timestamp first and then publish. Time matters, information flows fast so timestamping quickly will help avoid the problem of people claiming other's work;

Transactions for end-users are free to make timestamping content accessible for anyone.

Our first users thought manually timestamping was too difficult, so an automated service that timestamps in the background was created.

For further information: Wordproof[55].

8.6 Self-sovereign ID (SSI) (Cyprus)

8.6.1 Categories

Transversal Category

— 1. Cloud computing

— 2. Public sector information and open data

— 5. Electronic identification, trust services, e-signatures

— 6. e-Privacy

Horizontal Category

— 1. Identity Management

— 2. Data Provenance

— 3. Governance and DAOs

Vertical Category

— ISIC Section J - Information and communication

— Division 63 - Information service activities.

— Group/class - 6311 Data processing, hosting and related activities. (p. 56 - ISIC Rev. 4)

UN Sustainability Goals

— GOAL 3: Good Health and Well-being

— GOAL 9: Industry, Innovation and Infrastructure

- GOAL 12: Responsible Consumption and Production

Status

a) a “thought experiment”

b) approved but not implemented

c) in development or pre-production

8.6.2 Summary

Long description

The current lack of decentralized alternatives in identity management, leads the general public to “trust” and rely on large, centralized corporations and governments for the proper handling of their data; one centralized entity is, therefore, solely empowered with authentication and authorization functions.

This setup challenges four areas: Security, Privacy, Transparency and Trust (SPTT).

- Security issues involve identity theft, malicious attackers gaining control over users’ digital identity, or hackers gaining illegal access to users’ data.
- Correct processing of personally identifiable information (PII) is an important aspect of Privacy. Companies tend to state that subjects’ data will only be shared in a nonidentifiable form.
- Transparency is highly compromised in existing models regarding the way such centralized entities and their collaborating 3rd-parties share and use the PII and other non-sensitive personal data of online users.
- Trust: the problem of centralized data management persists in much the same way as all relevant SPTT challenges, where personal data associated with global social platforms are centrally stored on their private platform servers, leading to multiple security, privacy, transparency and trust issues

Distributed Identity Management with Blockchain seems to be the sole enabling technology of a decentralized, distributed identity management. This method ensures integrity of personal data while providing subjects with the opportunity to privately exchange verifiable claims about their identity, with a lower need for trust in large institutions that sometimes serve as intermediaries.

Changing the identity management model from a centralized or federated approach to a distributed, decentralized and self-sovereign approach through the use of blockchain technology can be beneficial. Putting people in control of their own data and letting them exchange personal data and attributes on their own terms, is the ultimate goal for a truly decentralized and user-empowering identity management platform.

Business problem or opportunity

- Privacy: Personal information is never shared through the network simply because the platform do not have access to this information.
- Intelligence: Intelligence automation and machine learning is embedded in the platform to provide smart personal profiling through predictive analytics.
- Reward: The platform enables Data Producers to monetize on their data shared with Data Consumers in a secured, transparent and auditable manner.

Scope

The solution can be applied at an international level with particular focus to regions that have already enforced Data Protection Regulations and Acts (e.g. GDPR, CCPA, etc.)

Insurance and Financial Sector:

a) provide KYC and customer onboarding functionalities

b) support predictive analytics that can be used for personalization of new products and services, creation and inspiration of new services targeting specific audiences, etc.

c) assist regular end users to decide/select what services and products would fit their needs (as per spending, health condition, insurance plans, loans, etc.)

Healthcare / Medical Sector:

a) host/store and provide controlled access to Electronic Health Records that users (data producers) store

b) enable the computation of predictive analytics on the user Health Records for public or private research

c) enable data monetization for data access by research and medical labs

Telecom, Media and Entertainment & Consumer Services and Retail

a) enable entertainment or other retail companies to access user data and understand better user preferences, likes, desires for new products, etc.

b) facilitate market user research studies and surveys, that the platform's users can participate and provide valuable input to data requestors

Government and NGOs

a) The platform can provide easy to access data, transaction logs, etc., for compliance with regulations.

Objectives

— Developing a global network platform where data subjects (including natural and legal persons) can create a cryptographic identity wallet, enabling them to store, manage, verify and validate their own identity data, as well as sharing and allowing processing of such data in a transparent and rewarding manner from data- requesting organizations.

— Providing data analytics and data insight tools to both data producers and consumers, to support decision making based on data already held by producers (identity data, social media or search engine activities, bank account transactions, electronic health records, insurance records, driving records, personality & psychometric data, etc.).

— Ensuring that data within the network are verified and validated through identity verification procedures, by, for instance, governmental and other certified, external validation mechanisms, currently available for identification and verification of data subjects' identity.

— Providing Data Ownership and Control of every processing activity performed within the Network, ensuring compliance with European and Domestic Data Protection Regulations and Laws (e.g. GDPR, e-Privacy, etc.).

— Disrupting the international data economy and market, by offering a highly scalable Marketplace App service supporting millions of users, and various functionalities applicable to different data types made available by data subjects, and useful to primary and secondary data consumers.

Stakeholders

Data Producers (DP) (Individuals, Organizations) Data Consumers (DC) (Usually Organizations)

Predicted outcomes

- General benefits: It can provide direct rewards to data owners (producers) for every use of their data. It can enable data owners and consumers to perform data-driven decisions using insights computed through their profile and usage.
- Benefits for the civilians/users/society: Civilians will receive enhanced privacy rights and improved quality of services. Data ownership allows consumers to profit and promotes the broad use of data, in a way that is beneficial to driving innovative applications.
- Benefits for Economy: In platforms where consumers own their data, they could sell it to multiple firms, stimulating competition, innovation, and triggering the emergence of new data economy and markets.

Why distributed ledger technology?

Blockchain is an enabling technology of a decentralized, distributed identity management. It contributes to the integrity of personal data while providing subjects with the opportunity to privately exchange verifiable claims about their identity, reducing the need for trust in large institutions that sometimes serve as intermediaries.

Changing the identity/data management model from a centralized or federated approach to a distributed, decentralized and self-sovereign approach through the use of blockchain technology would have great implications for society.

Putting people in control of their own data and letting them exchange personal data and attributes on their own terms, is the ultimate goal for a truly decentralized and user-empowering identity management platform.

8.6.3 User requirements

Functional requirements

Data Consumers are organizations that seek personal data to perform analysis of new target markets, send targeted advertisements, collect data for design of new products or services, etc.

Data Consumers require from the system the following:

a) Easy registration / on-boarding

b) Easy data requests

c) Easy data acquisition

d) Access to validated data

e) Easy / hassle-free data payments

f) Regulation compliance and easy auditing

Data Providers are individuals or organizations that manage and store securely their personal data on the platform and want to share specific data required by a Data Consumer for specific time, for specific purpose, and specific results. They expect reward from sharing or processing of such data.

Data Providers require from the system the following:

a) Easy registration / on-boarding

b) Easy data management

c) Secured data storage

d) Secured data sharing

e) Guaranteed data monetization

f) Secured money / wallet

g) Decision / support analytics

The platform supports basic functionalities that allow users from both sides (Data Producers (DPs) and Data Consumers (DCs)) to exchange data for money and/or services. These functionalities include:

a) user registration/onboarding, data verification, validation and storing

b) data request from DCs and matching with DPs

c) data monetization

d) data control, transparency and auditing

Onboarding:

Users or organizations (who can be DPs and/or DCs) can register with the platform, after providing identifiable information that can be verified with authorized (or governmental) services. When this step is completed, users can then store their verified data in encrypted form on the blockchain for future secured sharing under payment. Only a data owner can provide access to their data.

Data Requests:

DCs can formulate requests for accessing specific data, based on options allowed within data templates constructed by the platform. Thus, when a request is published in Data Marketplace, DPs whose data match said request (X) can choose to provide (or subscribe) to such request. This action effectively enables the requestor to get access to the stored data, via the blockchain.

Data Monetization:

The Data Modelling & Monetization Engine is responsible for continuously modeling user data, and providing valuations (price tags) to data requests. In effect, this module will allow DCs to assess how much their data request will cost, and decide if they want to publish it to the Data Marketplace or not.

When a DC data request is accepted by a DP, a Smart Contract is generated and placed in the blockchain for auditing purposes. The smart contract monitors the data sent to the DC, and decides completion of the transaction. Finally, it transfers the agreed monetary valuation to the specific DP's Wallet.

Users are given the opportunity to convert their valuable data into a financial asset. The Platform provides an external rating system that can be used everywhere on the internet. At the same time, the problem of honest reputation that many users face when searching for performers and companies online, will be decisively addressed.

Data Control, Transparency and Auditing:

By choice and based on the blockchain consensus mechanism, users will have control over the period within which data are made available to a given DC, and the number of times that access to such data for the purposes of processing has been granted.

Consent, and revocation of such consent, is achieved through data encryption and re-encryption mechanisms, and at all times available for users, as against 3rd-parties seeking to process users' personal data. Finally, all data transactions are logged on blockchain and all smart contracts are auditable by interested, and allowed end-users, DCs, or authorities (e.g. after regulatory request for compliance under GDPR).

Visualizations: Figures 39 to 44

— **Reference architecture**

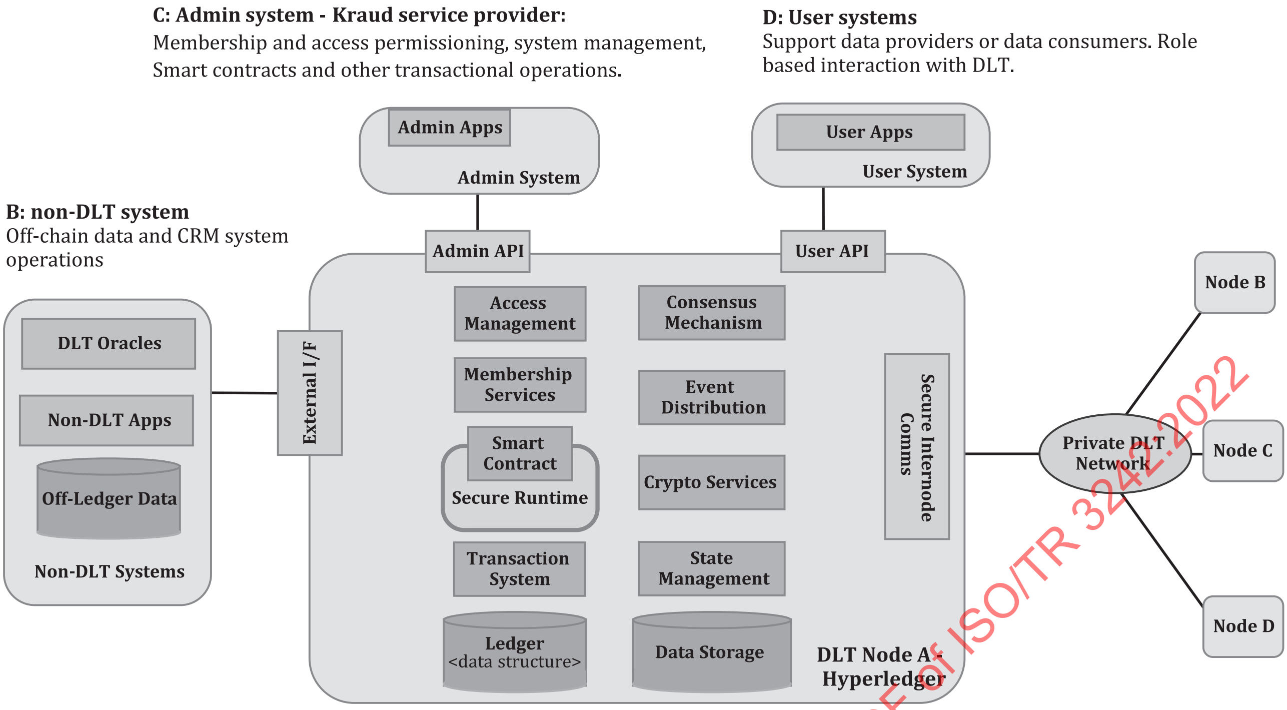


Figure 39 — Systems view architecture: SSI (Cyprus)

— **Data flow model**

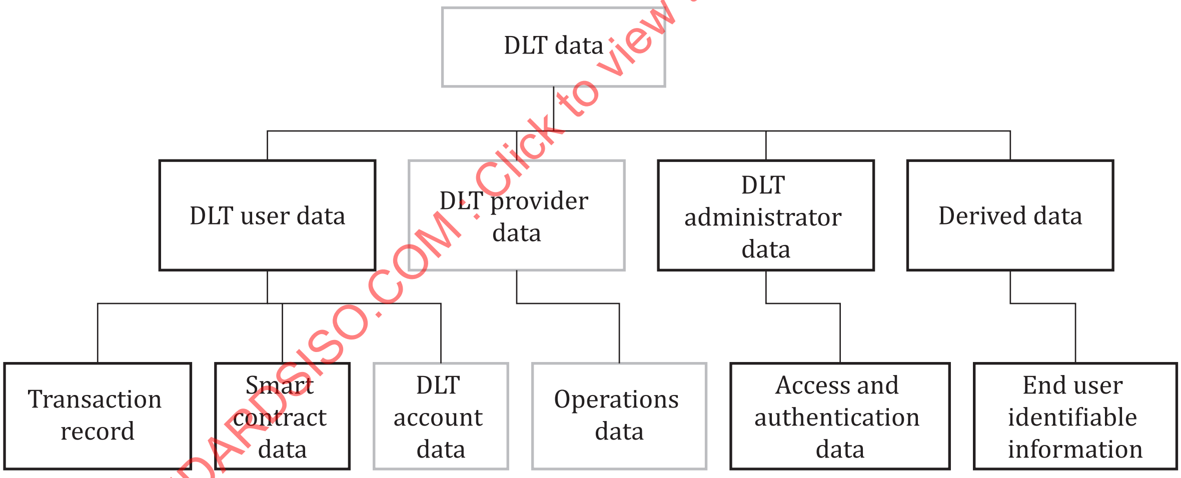
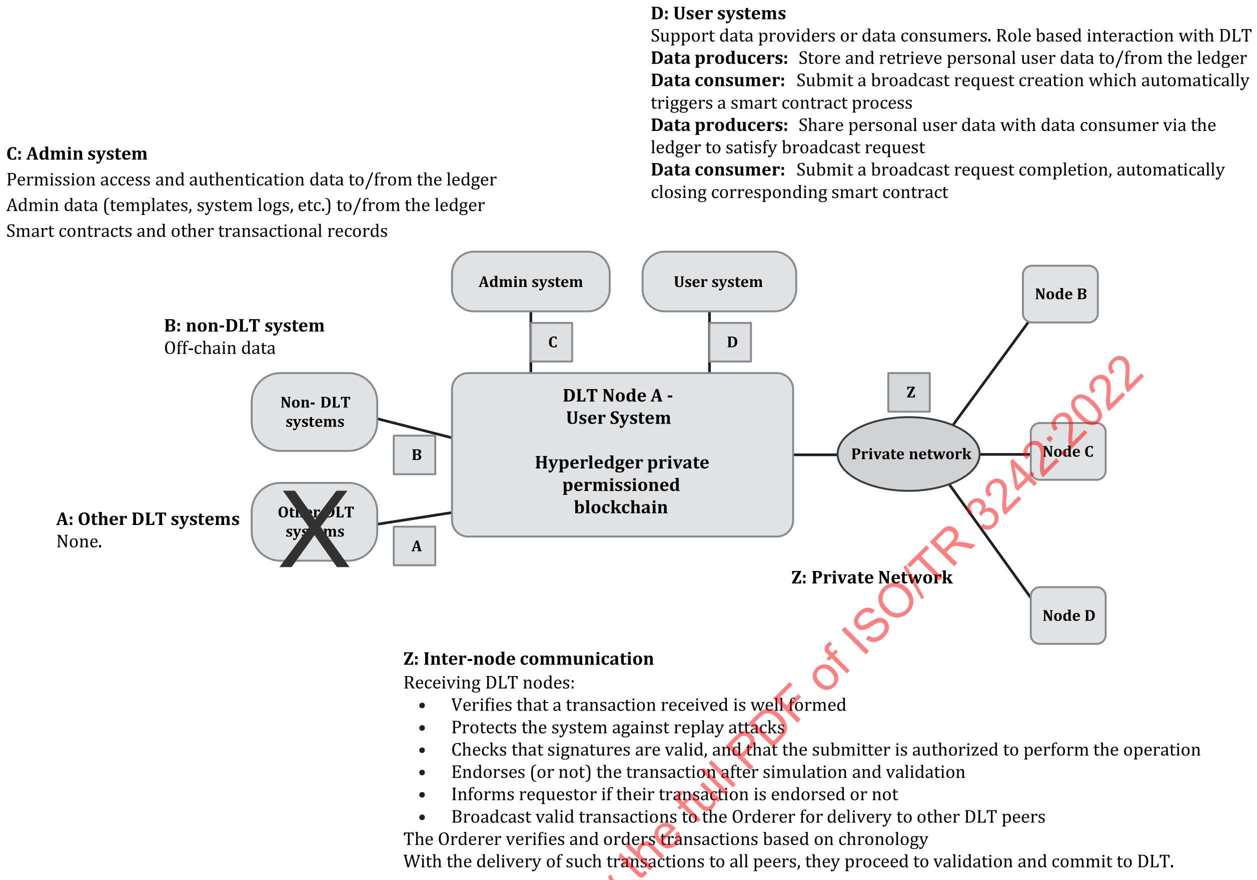


Figure 40 — Data flow analysis and stakeholder roles – SSI (Cyprus)



D: User systems
Support data providers or data consumers. Role based interaction with DLT
Data producers: Store and retrieve personal user data to/from the ledger
Data consumer: Submit a broadcast request creation which automatically triggers a smart contract process
Data producers: Share personal user data with data consumer via the ledger to satisfy broadcast request
Data consumer: Submit a broadcast request completion, automatically closing corresponding smart contract

C: Admin system
Permission access and authentication data to/from the ledger
Admin data (templates, system logs, etc.) to/from the ledger
Smart contracts and other transactional records

B: non-DLT system
Off-chain data

A: Other DLT systems
None.

Z: Private Network

Z: Inter-node communication
Receiving DLT nodes:

- Verifies that a transaction received is well formed
- Protects the system against replay attacks
- Checks that signatures are valid, and that the submitter is authorized to perform the operation
- Endorses (or not) the transaction after simulation and validation
- Informs requestor if their transaction is endorsed or not
- Broadcast valid transactions to the Orderer for delivery to other DLT peers

The Orderer verifies and orders transactions based on chronology
With the delivery of such transactions to all peers, they proceed to validation and commit to DLT.

Figure 41 — Data Flow analysis: SSI (Cyprus)

— **Behavioural UML**

User Diagram

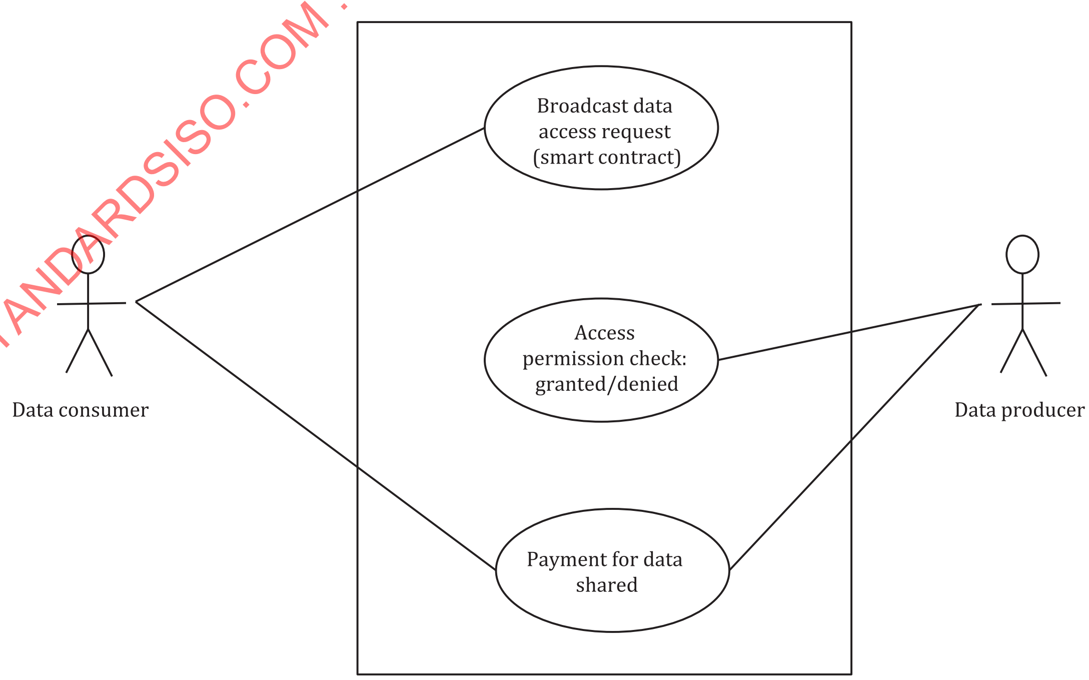

Broadcast data access request (smart contract)
Access permission check: granted/denied
Payment for data shared
Data consumer
Data producer

Figure 42 — Use case diagram: SSI (Cyprus)

Interaction Diagram

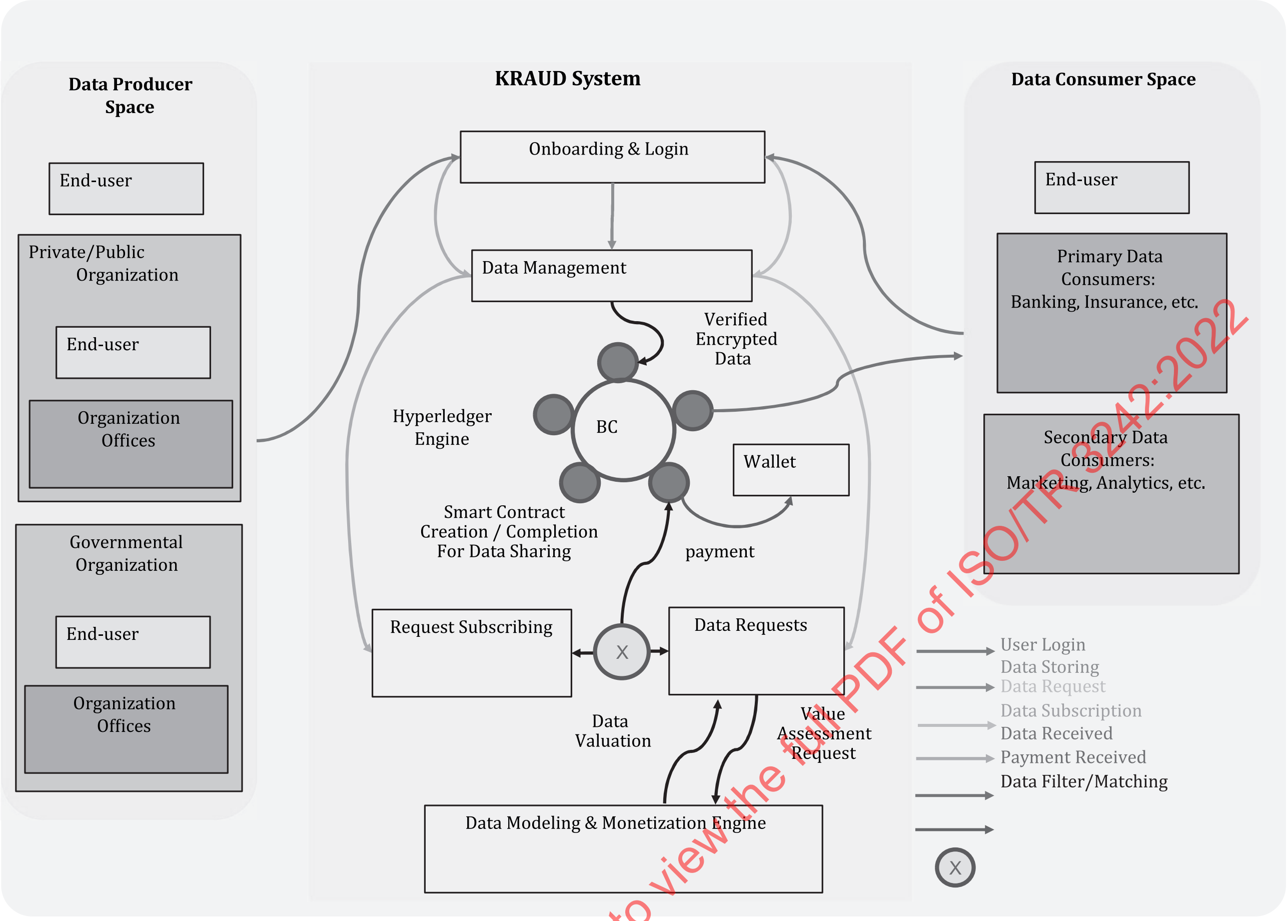


Figure 43 — Interaction diagram: SSI (Cyprus)

Sequence Diagram

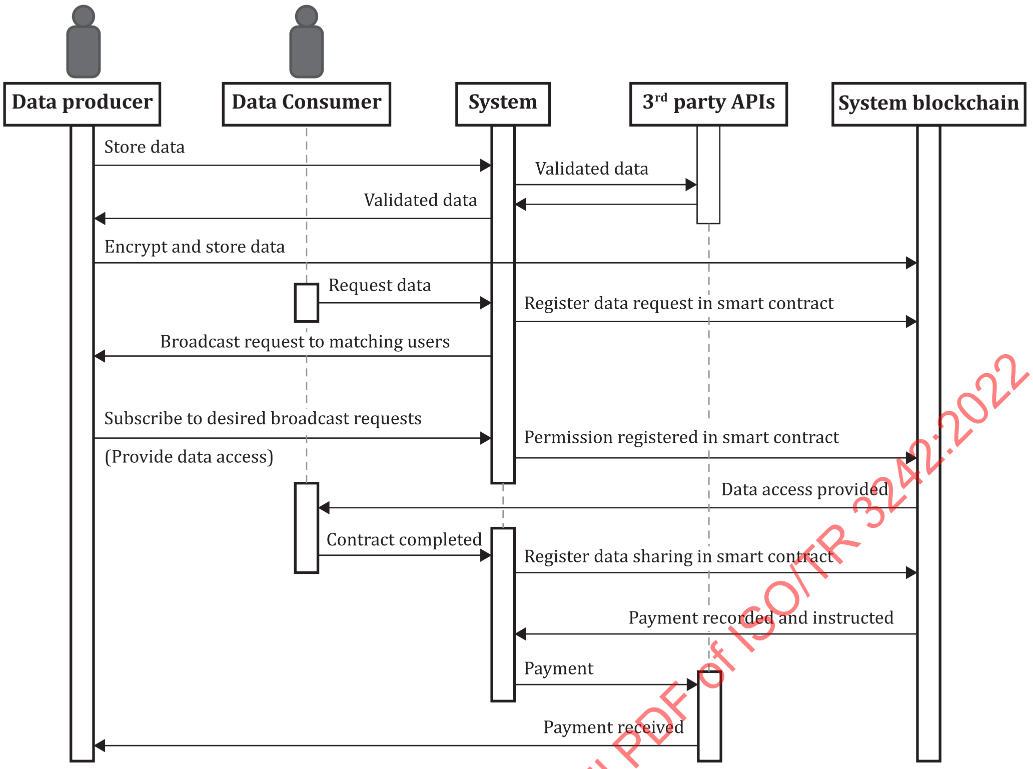

Data producer
Data Consumer
System
3rd party APIs
System blockchain
Store data
Validated data
Validated data
Encrypt and store data
Request data
Register data request in smart contract
Broadcast request to matching users
Subscribe to desired broadcast requests
(Provide data access)
Permission registered in smart contract
Data access provided
Contract completed
Register data sharing in smart contract
Payment recorded and instructed
Payment
Payment received

Figure 44 — Sequence diagram: SSI (Cyprus) – User registers

Privacy:

The only user data the platform has access at any moment are the necessary ones to allow a user to login/authenticate with the platform.

Such data are typically used by all online platforms to authenticate/register users, which are not sufficient to gain access to the user's personal data and operate with these data, since the user personal data are stored in encrypted form in the platform.

Such access to user's personal data is controlled by the user/data owner with cryptographic keys that only the data owner has.

Such data are stored encrypted on the blockchain, and no-one can access them without the user's personal private key.

Any machine learning methods that can be applied on user data are privacy- preserving, i.e. by design they cannot leak any sensitive information of the data owners (for example using differential privacy).

All data subjects' privacy rights under GDPR and other related regulations are maintained.

Data Protection Impact Assessment (DPIA) is executed on processing activities conducted in the platform that result into medium or high risk data transactions, for compliance with GDPR.

Security:

The platform uses secured technologies (such as HTTPs/TLS) to guarantee that only authorized parties login and communicate with the platform.

The platform uses secured technologies (such as cryptographic keys) to guarantee that only authorized parties can access/decrypt user data that are shared among parties.

All user data are stored in encrypted form to disallow unauthorized access.

Identity Management:

All user profiles created in the platform, are securely stored following industry standards and architectures on secure databases, to disallow unauthorized parties from accessing or modifying said data.

In particular, only system admins can view user login data/profiles for maintenance purposes.

Admins cannot view user personal data stored on Blockchain network, since they are encrypted with users' personal cryptographic key

Pre and post conditions:

Pre-conditions:

— Users realise blockchain technology benefits and users acceptance of this new digital vehicle for sharing personal information and identity management.

— Users who understand their new role as self-sovereign data owners.

— Widespread business acceptance of new digital forms of notarisation.

— Data Ownership and Control of every processing activity performed within the platform Network.

Post-conditions:

— Enhanced user privacy rights.

— Improved quality from businesses by facilitating the development of better services and products.

— Compliance of businesses with data protection regulations (GDPR), i.e. Data Inventory of processing activities embedded.

— Privacy By Design Principles Embedded.

Non-functional requirements:

User-related non-functional requirements (NFR):

— NFR1: Easy to use and understand: The user-facing modules such as the templates for inputting personal data, the broadcasting generation methods, and dashboards that show user's data valuation and broadcast participation are intuitive, clean and provide

— easy to use and easy to understand interfaces.

— NFR2: Easy development: The different components of the Service include documentation and/or tutorials to help non-savvy users to utilize the network and even deploy new Apps.

— NFR3: Time constraints: The different modules and interfaces provide results in a reasonable time that allow the execution of different applications in realistic time constraints, and without losing user engagement.

— NFR4: System Configuration. The different user-facing modules provide configuration or any possible customization options for end-users to personalize their experience with the system.

— NFR5: Legal compliance. All modules keep auditable logs of the transactions taking place, therefore making the business compliant with the GDPR and other EU- related legal frameworks. System-related non-functional requirements (NFR):

— NFR6: Scalability. The different modules and algorithms and provided APIs are able to handle thousands of concurrent (or not) users. This requirement affects the sub- systems in charge of interfacing with the users, the data storage and retrieval, and data analysis and valuation. The provided APIs can receive thousands of queries per second. Thus, they are designed and implemented to meet such scalability requirements.

- NFR7: System Security: The system provides state-of-the-art security protection to the stored data and the communications between users and the system, as well as between system components and the blockchain network.
- NFR8: Storage System Redundancy and Reliability: Due to the potentially high value of the collected data, including historical data, the system implements or considers options for redundant backup storage system to avoid or at least minimize potential loss of data.
- NFR9: Accuracy/Performance. The data sharing and valuation algorithms provide meaningful results to be used by users during broadcast generation. The algorithms use state of the art technology to achieve the better best accuracy possible. The methods to extract knowledge and validate data do not report misleading results.
- NFR10: Interoperability and modular design. The various platform components are capable of interfacing with new third-party APIs such as third-party data marketplaces, third-party organizations with official verification and validation APIs, third-party entities submitting new Apps requests and responses, etc.

8.6.4 Force field analysis

Legal considerations:

- The main question here is about liability on blockchains. Who is liable for the blockchain? The situation is quite different between permissioned (access control layer) and permissionless blockchains (accessible to anyone with no restriction).
- Access control, though in a permissioned blockchain might not mean that there is full control on any event occurring on it, and, because in a permissionless blockchain each user cannot be deemed liable for the actions of the whole blockchain, that is out of its control.
- Privacy compliance issues on blockchains is a complex issue and much uncertainty exists around it.

Risk:

Risk: Not enough resources to complete the product

- Mitigation Action: The team has an internal technical team, and also collaborates with external resources. Preventive Action: Concrete planning on resource management and task allocation to prevent resource depletion.

Risk: Turnover on team members

- Mitigation Action: Hold regular team meetings to discuss issues, exchange ideas & refresh morale and confidence.
- Preventive Action: Maintain friendly team spirit, perform team bonding activities (members know each other in personal life).

Risk: The end product is not viable to the data providers

- Mitigation Action: Using the MVP approach, the MVP based will be pivoted on user feedback and the product will be modified to produce a more viable and attractive solution.
- Preventive Action: Ensure end user interaction & involvement is high during the creation of expected user journeys. Also, ask frequently user feedback and share public updates.
- Risk: Fail to reach the market

- Mitigation Action: A modified/new go-to-market plan will be developed based on a pivoted MVP. Preventive Action: Build partnerships with companies, to customize and build a solution within the business for each one's needs.

Risk: Inadequate or poor software architecture/performance/ quality

- Mitigation Action: Adoption of standards and best practices in software development methodologies to ensure interoperability, performance and quality.
- Preventive Action: Develop a test plan, regression and performance as well as penetration testing and evaluation plan.

Risk: Overestimation of own IT capabilities

- Mitigation Action: Collaborate with external partners.
- Preventive Action: Build a DevOps Team with well qualified and experienced members.

Risk: Over relying on external resources

- Mitigation Action: Even though some parts of the project can be done by outsourcing partners, our internal technical team is involved in the process and knowledge is shared.
- Preventive Action: Ensure knowledge transfer sessions are conducted among DevOps Team and External Partners.

Other information: Kraud[31].

9 Use cases: Fintech

9.1 Accounts receivable financing system (China)

9.1.1 Categories

Transversal Category:

- 5. Electronic identification, trust services, e-signatures

Horizontal Category:

- Process Optimisation

Vertical Category:

- K - Financial and insurance activities
- Division = 64 - Financial service activities, except insurance and pension funding
- Group = 649 - Other financial service activities, except insurance and pension funding activities Class = 6492 - Other credit granting p. K 6492

UN Sustainable development goals:

- GOAL 17: Partnerships to achieve the Goal

Status:

- 5. in production/live implementation

9.1.2 Summary

Long description

This use case utilizes blockchain technology to record the transactions among core enterprise, upstream suppliers and downstream partners as well as the events of the transactions including signing contract, delivering goods, etc, This approach automates the financing management process, guarantees the data authenticity and limits loan fraud risks on the banks.

- Efficiency improvement on the Account Receivable Financing process with automated blockchain solution.
- Real-time and authentic data sharing among all the stakeholders including core enterprise, upstream suppliers and downstream partners, bank.
- Data security, integrity and traceability are ensured via blockchain technology to limits loan fraud risks on banks.

Business problem or opportunity

The use cases are currently mainly applicable to China, involving various enterprises in supply-chain and banks in China.

Scope

Automated, secured and efficient management of Account Receivable Financing process

Data operated on the supply chain is very important however it's not always visible, available or trusted.

As the core technology of a trusted value network, blockchain utilise asymmetric cryptographic algorithm, consensus mechanism, decentralization, permanency and immutability, which provides a share of data with bank and enterprise. Every node of the blockchain records the data of transactions and these data are immutable and traceable. It is conducive to solve the problem of information island in the supply chain finance business. The platform integrated the relevant transaction data from the blockchain so as to verify the authenticity of the trading behaviour. The technical characteristics of blockchain are that data can be traced but not be altered or deleted. With these characteristics, blockchain can help solve the credit problem of multi-level suppliers.

Objective

Core enterprise, upstream suppliers and downstream partners, bank

Stakeholders

Core enterprise, upstream suppliers, downstream partners and financial institutions such as banks.

Predicted outcomes

- Enhanced efficiency, reduced risk of loan loss, reduced operation cost
- Data operated on the supply chain is very important however it's not always visible, available or trusted.
- As the core technology of a trusted value network, blockchain utilise asymmetric cryptographic
- algorithm, consensus mechanism, decentralization, permanency and immutability, which provides a share of data with bank and enterprise.
- Every node of the blockchain records the data of transactions and these data are immutable and traceable. It is conducive to solve the problem of information island in the supply chain finance business.
- The platform integrated the relevant transaction data from the blockchain so as to verify the authenticity of the trading behaviour.
- The technical characteristics of blockchain are that data can be traced but not be altered or deleted. With these characteristics, blockchain can help solve the credit problem of multi-level suppliers

Why distributed ledger technology?

Utilizing blockchain technology to record the transactions among core enterprise, upstream suppliers and downstream partners as well as the events of the transactions including signing contract, delivering goods, etc., to automate the financing management process, guarantee the data authenticity and limits loan fraud risks on the banks.

9.1.3 User requirements

Functional requirements

The core enterprise requires the system to have functions such as contract establishment, contract modification, accounts receivable confirmation and payment.

The upstream suppliers or downstream partners require the system to have functions such as contract conformation, application for a loan, checking the contract status, processing the payment of the core enterprise.

The bank requires the system to have functions such as receiving the loan application, loan releasing, and investment management.

Visualizations: Figures 45 to 49

— **Reference architecture**

Systems view architecture

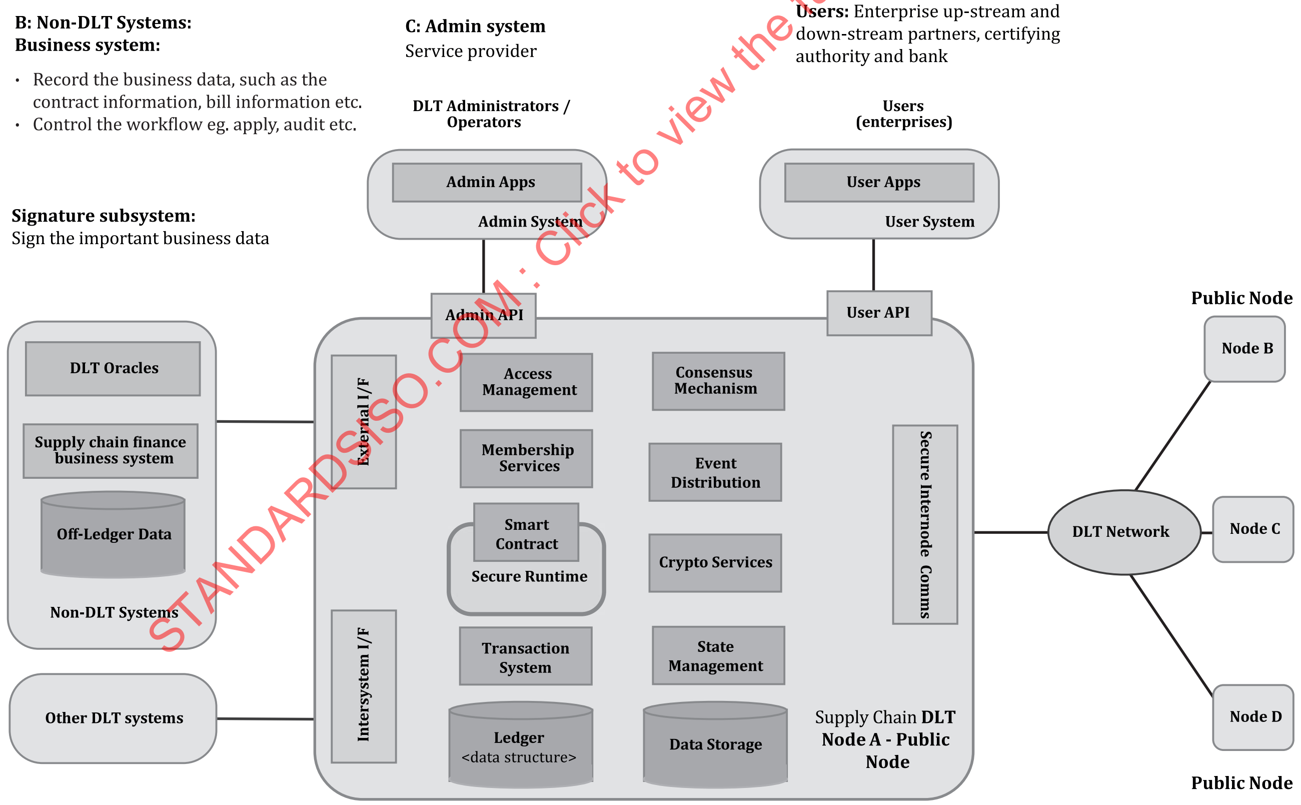


Figure 45 — System view architecture: Accounts receivable (China)

— **Data flow model**

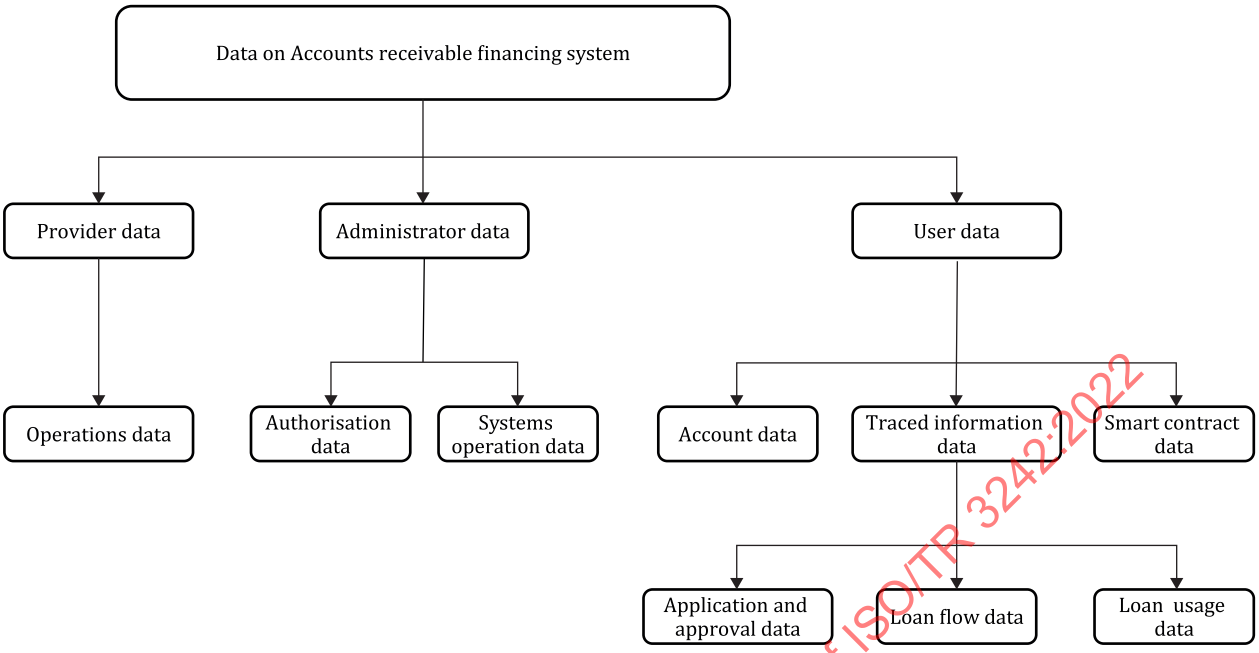


Figure 46 — Data flow analysis and stakeholder roles: Accounts receivable (China)

Identify the data flows triggered by the data-related operations of each stakeholder:

i) Stakeholders: **Core enterprise, upstream suppliers and downstream partners, bank, service provider.**
ii) Type of data flow (categories A- Z)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

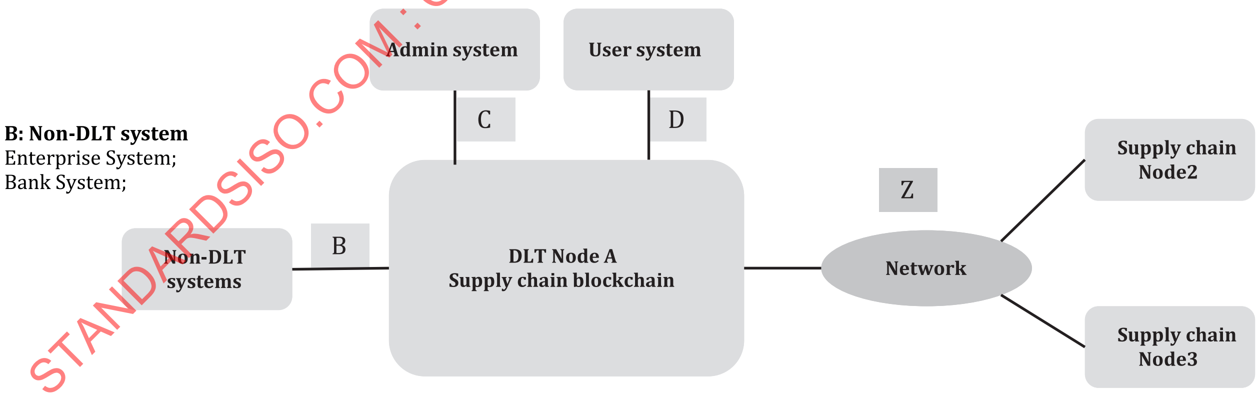


Figure 47 — Data flow analysis: Accounts receivable (China)

— **Behavioural UML**

Use case diagram and sequence diagram

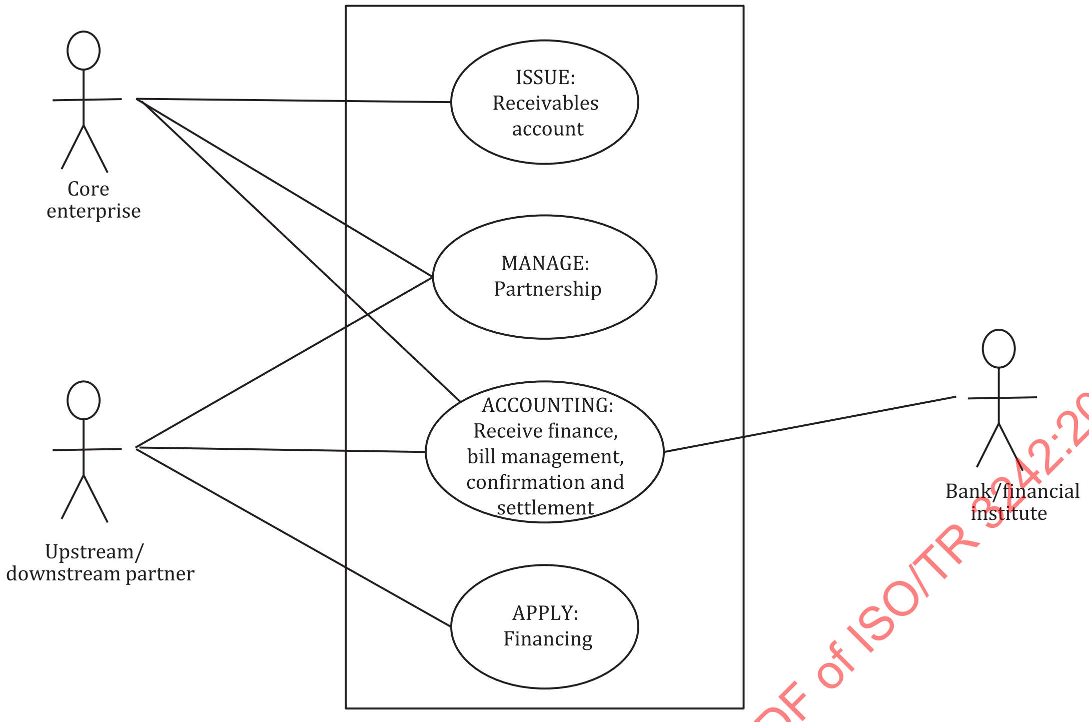

Core enterprise
Upstream/ downstream partner
ISSUE: Receivables account
MANAGE: Partnership
ACCOUNTING: Receive finance, bill management, confirmation and settlement
APPLY: Financing
Bank/financial institute

Figure 48 — Use case diagram: Accounts receivable (China)

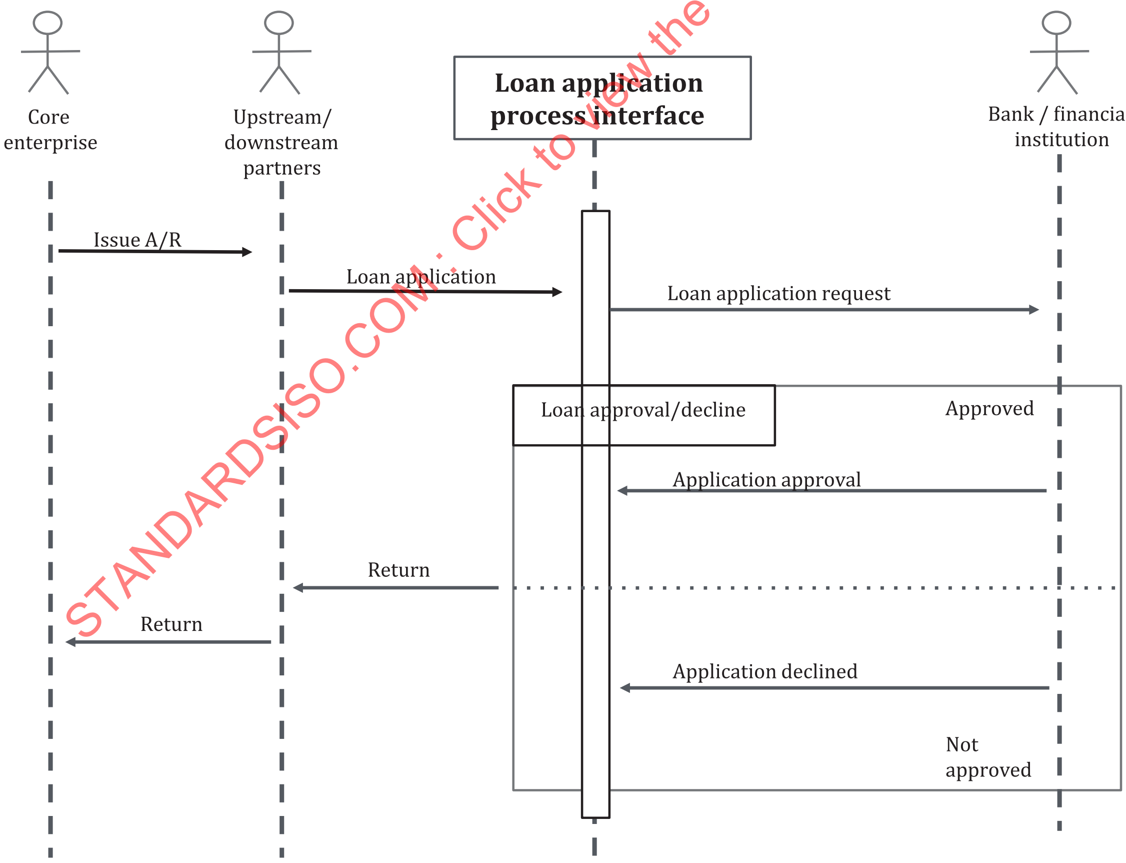


Figure 49 — Sequence diagram: Accounts receivable (China)

Performance - Transaction volume per second: 500 transactions / second. The supported maximum number of client connections: 1 000.

Response time: query response time is less than 1 second. Concurrency: The system supports 500 concurrent numbers.

The security of the data on the blockchain will be realized by the encryption scheme of asymmetric algorithm and advanced symmetric algorithm, the transmission and sharing of secret keys will be realized by the asymmetric algorithm, and the information on the blockchain will be encrypted by the advanced symmetric algorithm.

9.1.4 Force field analysis

Legal considerations:

The business of the enterprises is subject to relevant laws and regulations of the Chinese Constitution, the corporate law, and the Contract law and other Financial Laws.

Risk:

In this process, the problem of fraud between core enterprises and suppliers has not been solved. There can still be some risks for banks. However, this risk could be mitigated if the core enterprises and banks can sign an agreement and take part of the assets of core enterprises as insurance.

Receivable Financing System based on blockchain is an initial attempt to apply blockchain in the field of the practical application of supply-chain finance. As more enterprises participate in this system, more data and information will be accumulated on the system for the banks to further validate in order to constrain the risks.

Open source software:

- FISCO-BCOS as the blockchain
- MINIO as the file storage
- JDK1.8 for development language Node.js for web front-end
- Docker as the running container

Other information:

Further information: Digital China Information Service Co., Ltd[32].

9.2 Interbank loan reconciliation and settlement (China)

9.2.1 Categories

Transversal Category

- 5. Electronic identification, trust services, e-signatures

Horizontal Category

- 5. Process Optimization

Vertical Category

- 3. Banking, Financial Service and Insurance

UN Sustainability Goals

- GOAL 9: Industry, Innovation and Infrastructure

Status

- 5. in production/live implementation in Chin

9.2.2 Summary

Long description

This platform was designed to facilitate the clearing and reconciliation process for online, unsecured consumer loans via mobile devices. The loan is underwritten under a syndication model, wherein funding is jointly raised by the lead bank and other participant banks.

To ensure a smooth customer experience during the drawdown process, participant banks are required to make advanced deposits of provisional funds in VOSTRO accounts, i.e. an account a correspondent bank holds on behalf of another bank, opened at the lead bank. However, the process involving interbank clearing and settlement, as well as account reconciliation, grows increasingly complex as the number of participants increase.

In the traditional syndication model, banking systems only allow participant banks to view transaction journals and make reconciliations on a T+1 basis. The account information asymmetry in this process can increase participants' cost of capital, but the development of a real-time reconciliation system by independent participant banks is also not financially plausible. Nevertheless, a demand for visualized tools to monitor clearing and settlement and timely reconciliation remain in demand.

Business problem or opportunity

This platform is a solution to the aforementioned issues. System statistics also support this business case as well. The platform is used by three participant banks. In the traditional syndication model, banking systems only allow participant banks to view transaction journals and make reconciliations on a T+1 basis. The account information asymmetry in this process can increase participants' cost of capital, but the development of a real-time reconciliation system by independent participant banks is also not financially plausible. Nevertheless, a demand for visualized tools to monitor clearing and settlement and timely reconciliation remain in demand.

Scope

As interbank reconciliation is a global competitive challenge, the use case can be applied in the reconciliation process between different financial institutions and different financial products worldwide.

Objective

The objectives of the platform include simplifying the interbank reconciliation process, improving operational efficiency, and reducing operation costs.

Stakeholders

The lead bank and participant banks involve in reconciliation process.

Predicted outcomes

Reduce the settlement period to T+0 days from the industry average of T+1 to T+2 days.

Why distributed ledger technology?

The reconciliation process involves different participant banks. The development of a real-time reconciliation system by independent participant banks is not financially plausible. Besides, the clearing and reconciliation process involves the high-frequency, high-volume information and fund flows. At the same time, the operational management must meet strict access and security requirements.

9.2.3 User requirements

Functional requirements

— Actors: Lead Banks, participant banks

- One master node provides core DLT and maintains the system operation.
- Other participant banks are only responsible for conducting reconciliation.

Visualizations: Figures 50 to 53

- **Reference architecture**

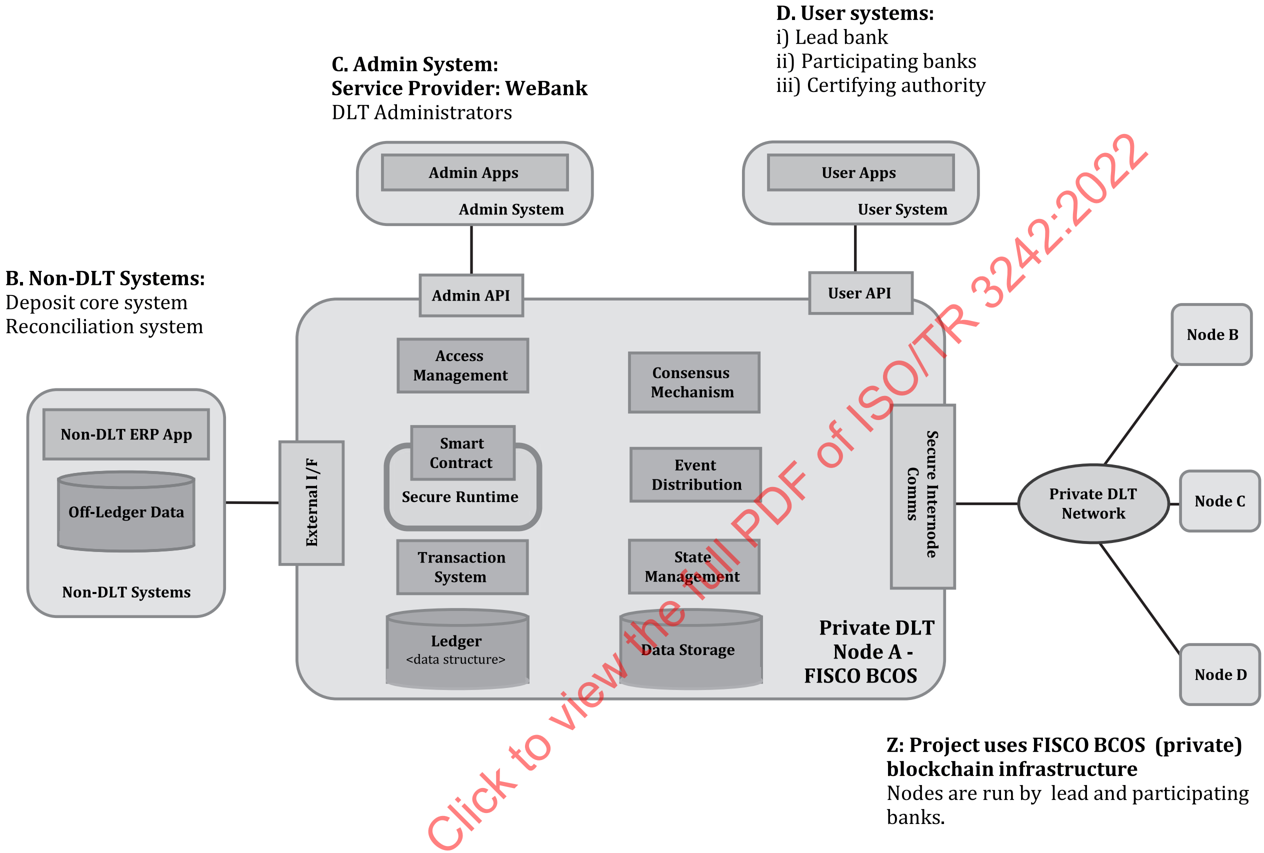


Figure 50 — System view architecture: Interbank reconciliation (China)

- **Data flow model**

Data flows triggered by the data-related operations of which stakeholders.

i) Specify the role of each stakeholder in facilitating the data flow: **Banks, service provider, certifying authority**
ii) Identify the type of data flow (See categories A- Z below)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

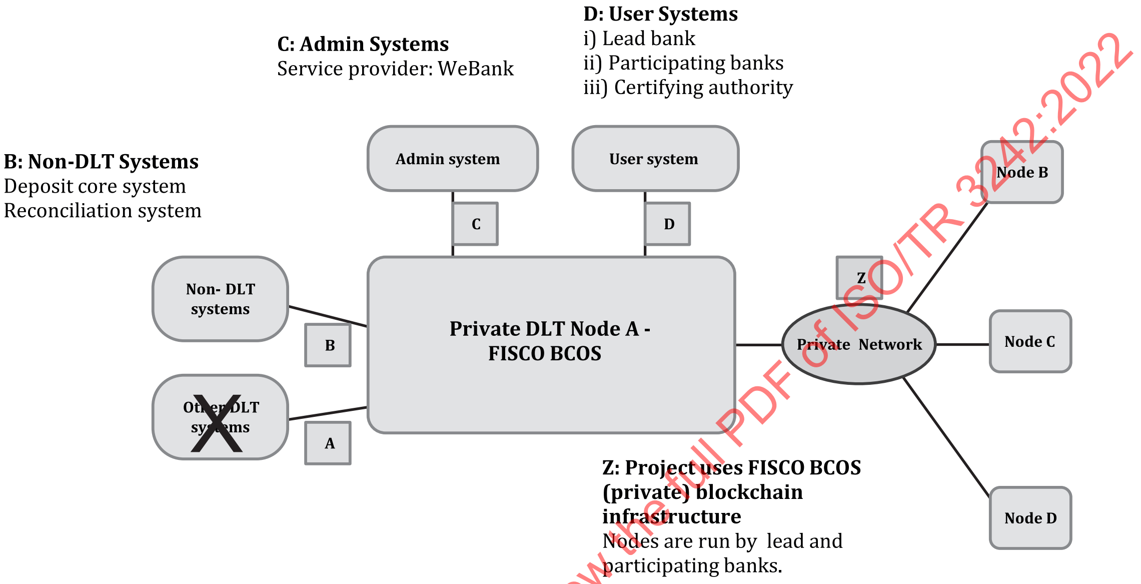


Figure 51 — Data flow analysis: Interbank reconciliation (China)

— **Behavioural UML**

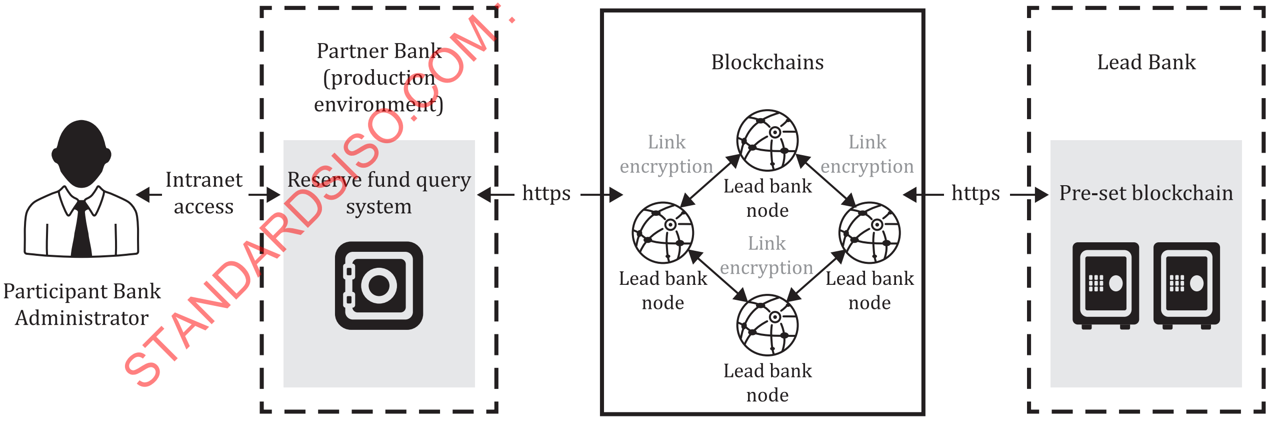


Figure 52 — Use case diagram: Interbank reconciliation (China)

Sequence Diagram

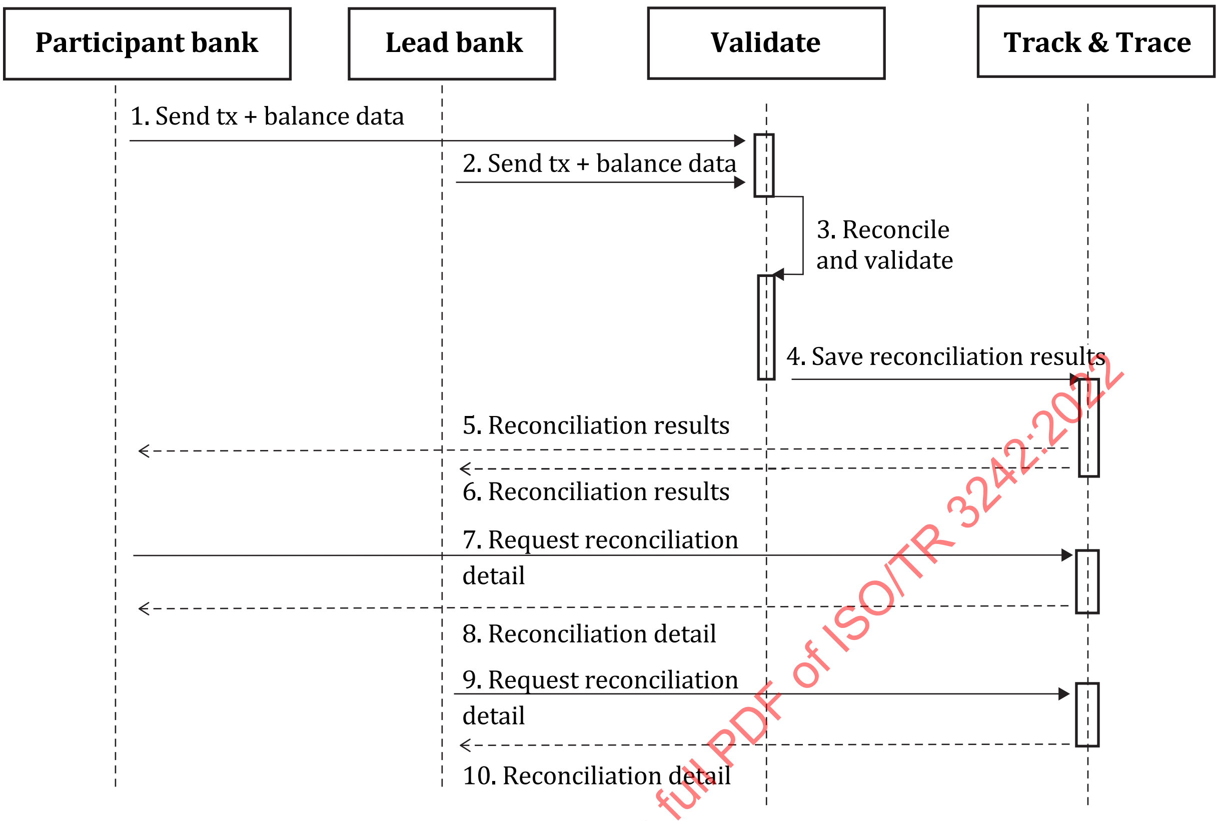

Participant bank
Lead bank
Validate
Track & Trace
1. Send tx + balance data
2. Send tx + balance data
3. Reconcile and validate
4. Save reconciliation results
5. Reconciliation results
6. Reconciliation results
7. Request reconciliation detail
8. Reconciliation detail
9. Request reconciliation detail
10. Reconciliation detail

Figure 53 — Sequence diagram: Interbank reconciliation (China)

9.2.4 Force field analysis

Legal considerations:

The application is under supervision of the local banking and monetary authorities and constrained by the related regulations and laws.

Risk:

Per compliance requirements, DLT system and existing banking system are applied separately, and so two systems are operating simultaneously in this use case. If DLT is fully acknowledged by the regulator in the future, it will be able to replace the traditional reconciliation system, which is where this use case brings the most important value. Therefore the risk of this use case is the regulator ultimately does not approve DLT to be applied in reconciliation.

Open source software:

- Privacy: access role control, zero-knowledge proof, homomorphic encryption, group signature, ring signature
- Performance: advanced consensus algorithm based on rPBFT
- Usability: easy to on board with SDK, sample implementation, deployment guide, monitoring and auditing tools
- Reliability: several applications in production with proven stability
- FISCO BCOS Documentation[33].

Other information:

WeBank Co., China[34].

9.3 Organized CHIT funds (India)

9.3.1 Categories

Transversal Category

- 1. Cloud computing
- 2. Public sector information and open data
- 5. Electronic identification, trust services, e-signatures

Horizontal Category

- 1. Identity Management
- 2. Data Provenance
- 3. Governance and DAOs

Vertical Category

- Use case authors define their use case by ISIC Section, division, group and class.
- Section = K - Financial and insurance activities
- Division = 64 - Financial service activities, except insurance and pension funding
- Group = 649 - Other financial service activities, except insurance and pension funding activities
- Class = 6492 - Other credit granting

UN Sustainable development goals

- GOAL 1: No Poverty
- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 10: Reduced Inequality
- GOAL 11: Sustainable Cities and Communities
- GOAL 17: Partnerships to achieve the Goal.

Status

- 5. In Production / Live implementation

9.3.2 Summary

Long description

Typical actors in an organized ROSCAs are Organizers, Subscribers, Regulators, Banks, Auditors and other Third Party Systems. Activities between actors are intermediated by Regulators whose role is to oversee whole-system compliance and to protect the interests of individual Subscribers and Organizers.

The Organized Chit Funds disintermediates the Regulator role to bring trust and transparency to system operations. This approach catalyses all activities between parties and enables new business models that promote financial inclusion.

Business problem or opportunity

ROSCA organizations in India operate on a very thin margin with restrictions across the segment in terms of alternate revenue opportunities. Subscribers, on the other hand, are also losing money in the name of ROSCAs by unscrupulous activities of some of the organizers. Regulators who play the role of intermediation between these two parties have less human resources to administer and monitor the activities. With multiple unknown parties involved in the ROSCA operations, the issue of Administration/Monitoring, Trust and Transparency across all the transactions is a big challenge in this segment.

Scope

This use case has national scope and is specifically for organised and regulated CHIT Funds. India as a country has legislation to support the ROSCA activity as per "The Chit Fund act of 1982". This use case has the scope of implementation across the country and can play an important role in financial inclusion if implemented correctly. Currently, this is implemented in the State of Telangana. The same use case can be expanded to multiple nations where social lending, self-help group activities are more prevalent. Since this use case has implemented long proven legislation, this can form the basis of implementation in countries where there is no law yet to govern this business. The smart contracts can be validated and vetted by the governance and working committees set up to make sure there is legal validity/backing to the transactions happening.

Objective

Increase the Trust and Transparency in the way ROSCA operations are conducted in the state/country. The smart contracts can be validated and vetted by the governance and working committees set up to make sure there is legal validity/backing to the transactions happening.

Stakeholders

— All ROSCA participants, Regulators, Organizers, many other ecosystem enablers.

Predicted outcomes

— Full transparency in the money movement of the ROSCAs,

— Full transparency in the Operations of the ROSCA organizations.

— Protect millions of subscribers interest in participating ROSCAs Standardization across the board

— Predictability and Understanding of the economic situation based on the ROSCA money in the system

— Economic Indicators helping to improve understanding of how people save and borrow.

— Financial Inclusion by building the credit profiles of these subscribers who are otherwise left out of formal financial institutions.

Why distributed ledger technology?

Chit fund (ROSCAs) as a financial instrument has many operational strengths and weaknesses. Blockchain can address many of the challenges discussed above which would reduce the information, interaction and innovation frictions (e.g. high fees, cash movements, reporting, auditing and potential fraud from the parties).

Using blockchain can, decrease the friction, and also increase the operational efficiency and entrust the belief in this financial product. This solution gives a transformative approach to this traditional industry by not just building the fundamentals of the system, but it will pave the way to build the credit identities of these subscribers who are otherwise left out in the formal banking financial services.

A blockchain based network of ROSCA group registry along with the subscribers will create immutable transaction records. This approach can build the credit profiles of these subscribers from the ground up and make them financially inclusive.

As smart contracts continue to evolve with more and more parties joining the consensus mechanism, it will achieve higher level of usability and trust. The platform will capture transactions, verify the data and can also work with third party systems such as financial institutions to enable smart transactions and distribute private keys for clients – to allow an automated and trusted financial transaction between all parties.

If established as described above, blockchain implementation has large potential to create a decentralized, disintermediated, inclusive financial solution unlocks the economic value and liquidity.

9.3.3 User requirements

Functional requirements

Visualizations: Figures 54 to 57

— **Reference architecture**

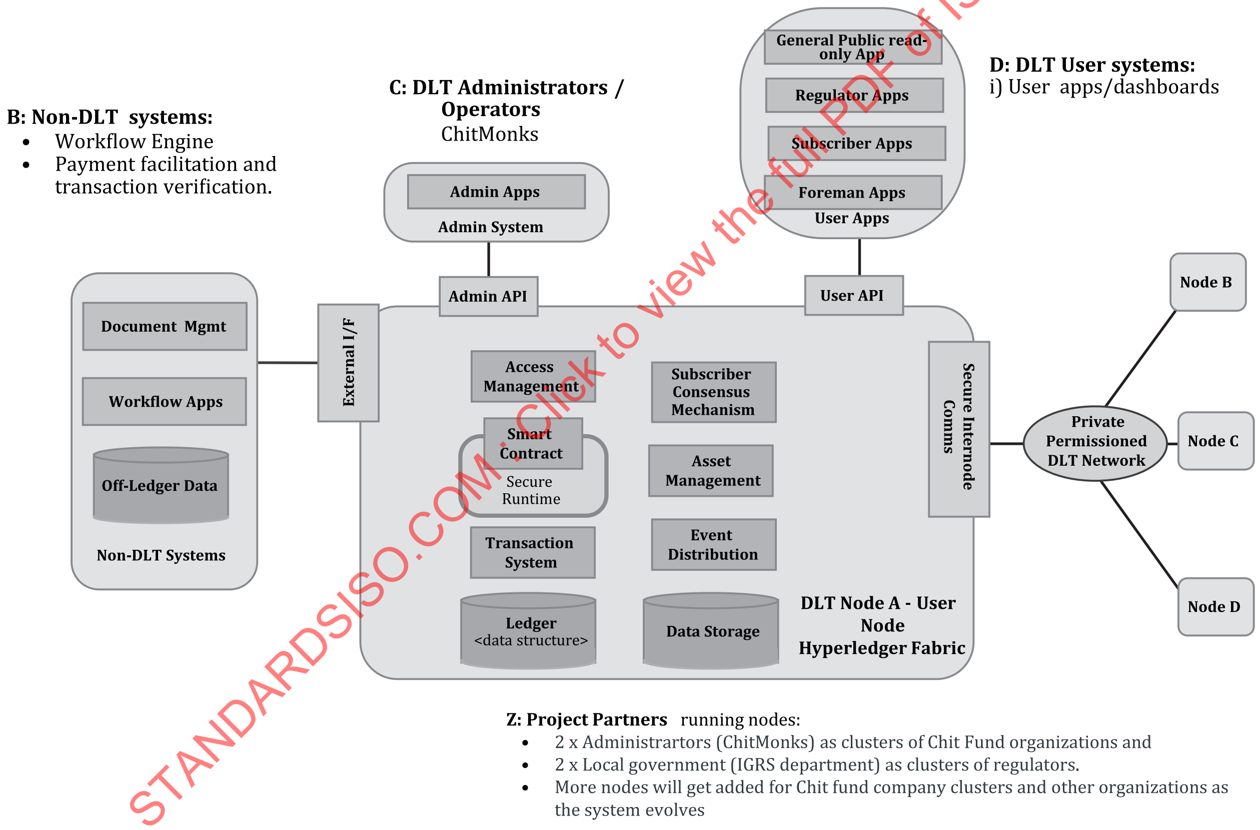

B: Non-DLT systems:
• Workflow Engine
• Payment facilitation and transaction verification.
C: DLT Administrators / Operators
ChitMonks
Admin Apps
Admin System
General Public read-only App
Regulator Apps
Subscriber Apps
Foreman Apps
User Apps
D: DLT User systems:
i) User apps/dashboards
Document Mgmt
Workflow Apps
Off-Ledger Data
Non-DLT Systems
External I/F
Admin API
User API
Access Management
Smart Contract
Secure Runtime
Transaction System
Ledger <data structure>
Subscriber Consensus Mechanism
Asset Management
Event Distribution
Data Storage
DLT Node A - User Node Hyperledger Fabric
Secure Internode Comms
Private Permissioned DLT Network
Node B
Node C
Node D
Z: Project Partners running nodes:
• 2 x Administrartors (ChitMonks) as clusters of Chit Fund organizations and
• 2 x Local government (IGRS department) as clusters of regulators.
• More nodes will get added for Chit fund company clusters and other organizations as the system evolves

Figure 54 — System view architecture: Organised CHIT funds (India)

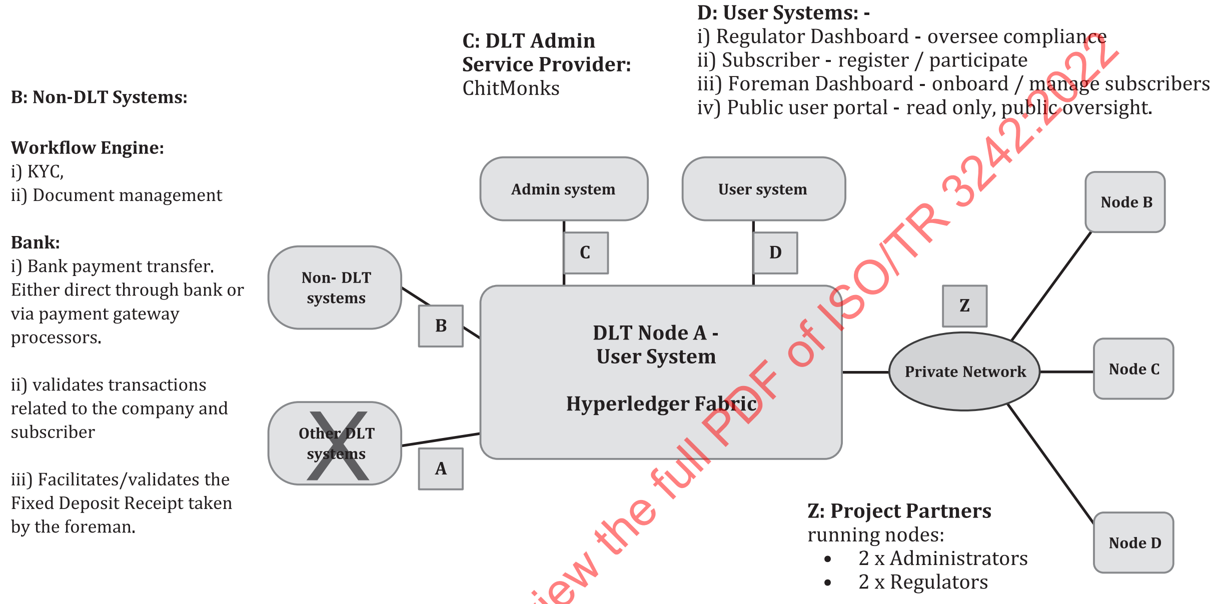
— **Data flow model**

There are three major actors in ROSCA business

Data flows triggered by the data-related operations of each stakeholder:

i) Stakeholders: Subscriber (active Chit group subscriber), Public User (any citizen), Regulator (ChitfundRegulator), Foreman (Chit fund company owner), Bank, Service Provider (ChitMonks).
ii) Type of data flow (categories A- Z)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system



D: User Systems: -
i) Regulator Dashboard - oversee compliance
ii) Subscriber - register / participate
iii) Foreman Dashboard - onboard / manage subscribers
iv) Public user portal - read only, public oversight.
C: DLT Admin Service Provider:
ChitMonks
B: Non-DLT Systems:
Workflow Engine:
i) KYC,
ii) Document management
Bank:
i) Bank payment transfer. Either direct through bank or via payment gateway processors.
ii) validates transactions related to the company and subscriber
iii) Facilitates/validates the Fixed Deposit Receipt taken by the foreman.
Admin system
User system
C
D
Non- DLT systems
B
DLT Node A - User System
Hyperledger Fabric
Other DLT systems
A
Z
Private Network
Node B
Node C
Node D
Z: Project Partners
running nodes:
• 2 x Administrators
• 2 x Regulators

Figure 55 — Data flow analysis: Organised CHIT funds (India)

— Behavioural UML

Use case diagram

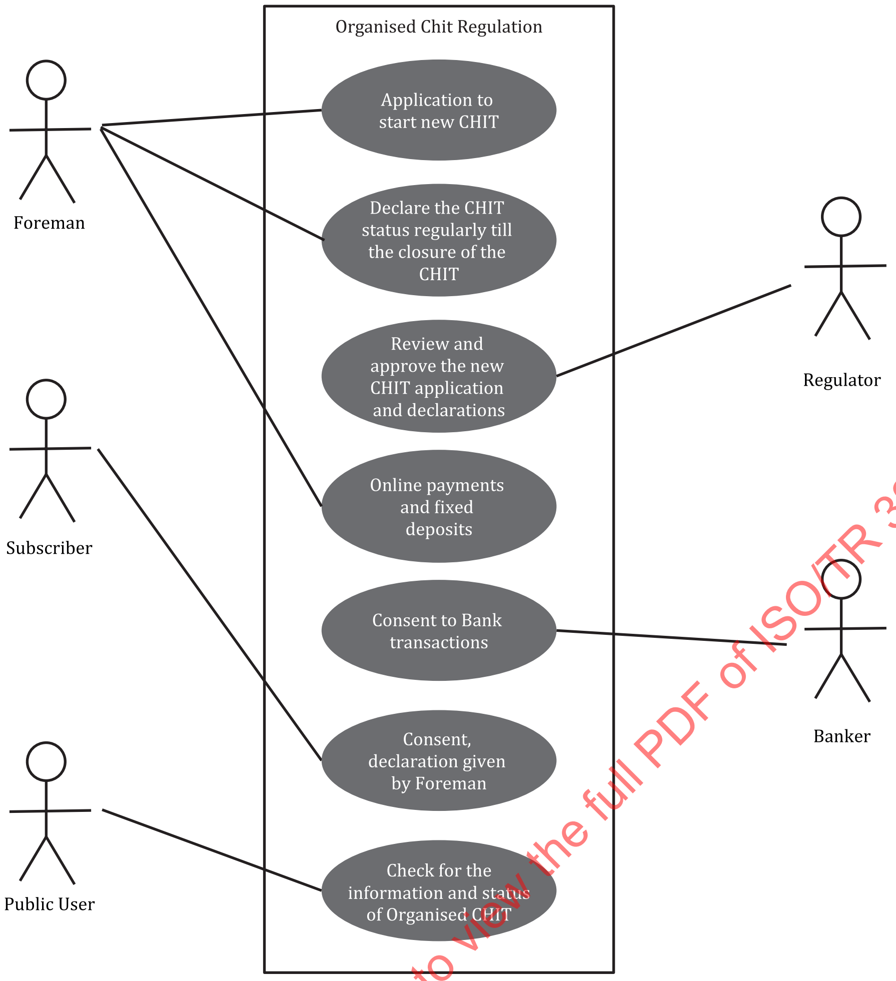

Organised Chit Regulation
Foreman
Subscriber
Public User
Regulator
Banker
Application to start new CHIT
Declare the CHIT status regularly till the closure of the CHIT
Review and approve the new CHIT application and declarations
Online payments and fixed deposits
Consent to Bank transactions
Consent, declaration given by Foreman
Check for the information and status of Organised CHIT

Figure 56 — Use case diagram: Organised CHIT funds (India)

Sequence Diagram

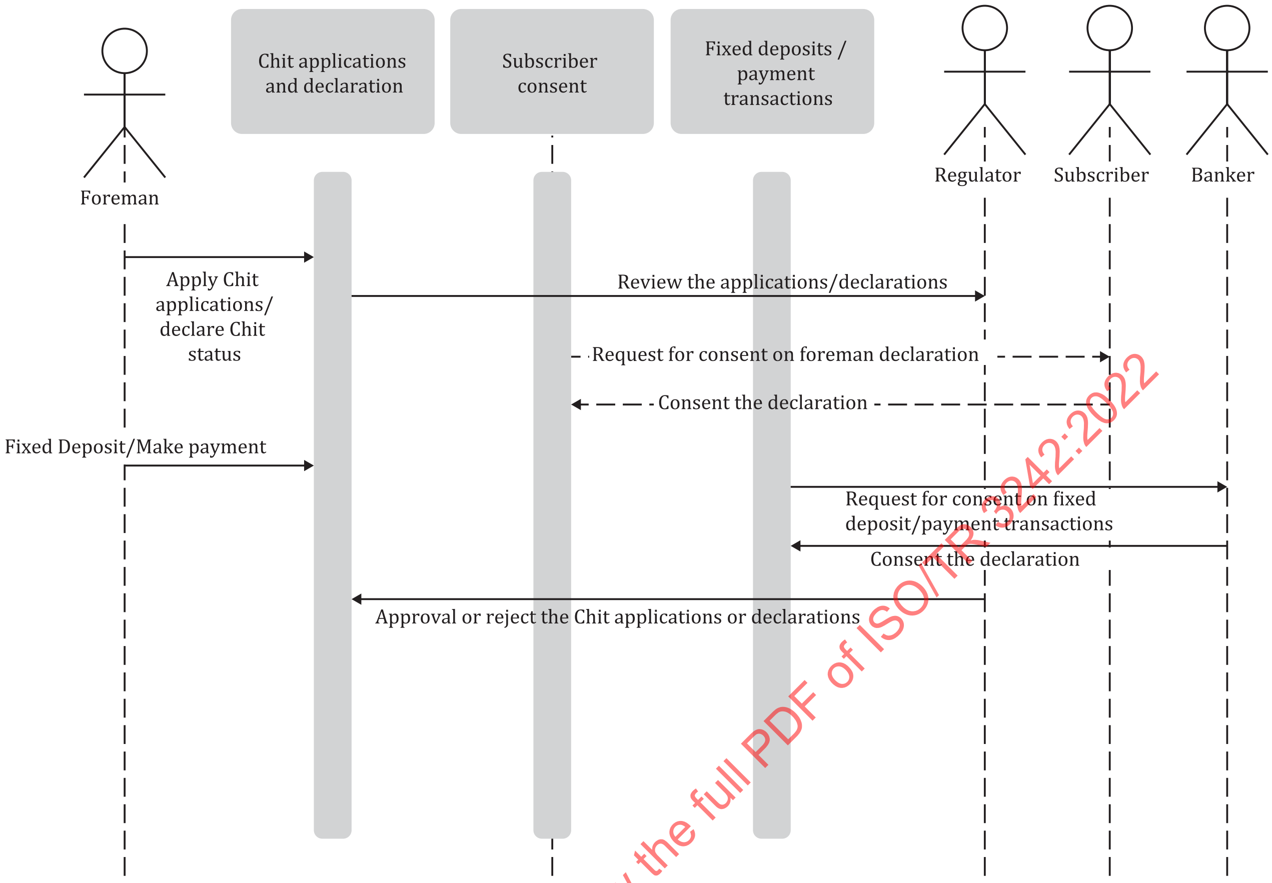

Chit applications and declaration
Subscriber consent
Fixed deposits / payment transactions
Foreman
Regulator
Subscriber
Banker
Apply Chit applications/ declare Chit status
Review the applications/declarations
Request for consent on foreman declaration
Consent the declaration
Fixed Deposit/Make payment
Request for consent on fixed deposit/payment transactions
Consent the declaration
Approval or reject the Chit applications or declarations

Figure 57 — Sequence Diagram: Organised Chit Funds (India)

Smart contracts:

This solution defines multiple chain codes for various transactions between Organizer and Regulator.

All the chain codes are embedded with Regulatory acts to make sure the Organizer is following the “The Chit Fund Act of 1982”. Any deviation from the Act, system would raise flags with different severity levels. There might be some scenarios, where severe deviations would cause in rejection of the transactions.

Categories for chain codes include:

- ROSCA Group Approval related chain code.
- ROSCA Group Modification related chain code ROSCA Group Closure related chain code.
- ROSCA Group Auction related activities chain code.
- Foreman Company registration and modification related chain code.
- Foreman Company Payments to subscriber related chain code.

Security, privacy and identity management:

All the users of the system would be able to access their organization data with permissioned access mechanisms in place. The user access roles would be defined by respective organization admins, they can define these roles only for their data. Any other data access would be permitted with the consent of the data owner.

All the data communication across the network would use TLS communication, that would encrypt all the data in transit.

Only approved entities would be allowed to participate in the network. Any malicious transactions would mean that the participant would be thrown out of the network.

Non-functional requirements:

Hyperledger Fabric is used as blockchain framework to build the private/permissioned blockchain network. Technically, there is no limit on the number of participants. It supports up to 2000 TPS, which is sufficient for the ROSCA transactions in the ecosystem.

The current business workload could be around 500 TPS at the peak load. With the other ecosystem players, the TPS can up to 1,000. These number could easily be handled by the Hyperledger Fabric.

9.3.4 Force field analysis

Legal considerations:

India has a legislation which governs the ROSCA operations – "The Chit fund Act of 1982". But one of the biggest constraints in disintermediating the governance completely is giving the legal validity to the smart contracts.

Outside India, this same use case can be used as an innovative business model to help spread the financial inclusion.

Risk:

While the system can now play an important role in the design of consensus policies and make sure the smart contracts written honour the transactions between parties seamlessly without any intermediation, the legal binding of these smart contracts are important to make the system completely auto-regulating.

In terms of business, it would be useful to have strong data governance entities in charge of defining who will have access to what information. Consent driven mechanisms (User-centric) will help take this use case to a very different level.

Referenced standards:

Technically, when looking at the use case, the node managers will be evolved over a period of time but beyond that, the available technologies and frameworks will surely help the use case enough.

Further information on Hyperledger Fabric Related Documentation[35] references and Chit Fund Act[36] and Chitmonks company information[37] are listed in the Bibliography.

Other information:

Implementation Status in Telangana:

- 14 Assistant Registrar of Chits (ARC) offices
- 724+ Chit fund Companies
- 1 452+ Branches
- 21 489+ Chit Groups (ROSCA Groups)
- 1 461,66+ Cr Auction Turn Over per month
- 17,532+ Cr of Money rotated per year

Benefits observed from implementing TChits:

The officials from the ARCs indicated that the system is helping them to monitor the entire process efficiently as indicated below:

- Monitoring of ROSCA company compliances has become easy.
- Minutes filing and monitoring of monthly reporting has been automated by the system.
- Voucher Details and separate account details compliance is automated by the system.
- Violations raised by the system is very useful. No need of manual monitoring about violations saving many man hours of work.
- All ARC offices have become cashless and the payments are handled only online.
- All the legacy data migration is done making the entire chit fund reporting activities digital. No more offline activity in any ARC Office now.
- Verification and Document management of the Details submitted by the foreman have become easy
- Various health parameters in the ROSCA businesses can be monitored now in real time and take proactive steps to mitigate future risks.
- Standardization across the board because of automated rule engine.
- Imposing fines are automated and hence the compliance is also increased.

Other achievements / benefits:

- Enforcing 100 % Discipline in chit fund company activities.
- Proactive administration / regulation of Chit fund business.
- Identification of patterns.
- Paperless, Presence less and Cashless – Reduces the carbon footprint, efficient document management, cut lot of indirect costs both to foreman and regulator.
- First of its kind of project which will set as a role model to the entire country.

Further information is given in Reference [37].

9.4 Transparent securitisation (Italy)

9.4.1 Categories

Transversal Category

- 5. Electronic identification, trust services, e-signatures
- 6. e-Privacy
- 8. Accessibility of ICT products and services

Horizontal Category

- 1.Identity Management
- 5. Process Optimisation
- 6. Automation

Vertical Category

- Section = K - Financial and insurance activities

- Division = 66 - Activities auxiliary to financial service and insurance activities
- Group = 661 - Activities auxiliary to financial service activities, except insurance and pension funding Class = 6619 - Other activities auxiliary to financial service activities - Specifically, marketplace facilitating securitisation transactions

UN Sustainability Goals

- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure GOAL 10: Reduced Inequality
- GOAL 11: Sustainable Cities and Communities

Status

- 3. in development or pre-production
- 8. an integration with current systems

9.4.2 Summary

Long description

The platform provided by Stonize is a digital marketplace for running end-to-end securitisation transactions. It allows the creation of blockchain based securities (security tokens), embedding secondary trading. It digitises paper deeds and, by using tokenisation, automates asset management embedding governance within algorithmic protocols, thus making deal execution accessible and efficient. Blockchain notarisation enables transparency on underlying assets performance (immutable data). This combination provides a one-stop solution for digital securitisations, which ultimately promotes financial inclusion and impacts the real economy and employment rate.

The platform allows an SPV to acquire assets (e.g. invoices) by digitally signing contracts, issuing and exchanging security tokens and notarising the key steps of the assets' processing and their performance. The platform integrates premium compliant KYC, AML and document preservation services and EU regulated digital identities (eIDAS is the EU regulation for Electronic Identification, Authentication and Trust Services[38]). Also it interacts with third- party custodians and exchanges. The user interface is based on a dApp that can be executed on a decentralised browser.

Business problem or opportunity

This platform solves the major issues of securitisation of:

- Low efficiency: traditional securitisation takes time and money (e.g. collateral PTF segmentation contracts management, data reconciliation);
- Low transparency: securitisation complexity can make the assessment on the value of the investment hard (e.g. performance of assets backing securities can be unclear)

This ends up in serving the real economy by providing cost-effective liquidity for SMEs' growth, which leverage lower capital cost and efficient private placements.

Scope

Stonize operates in the financial industry and, more specifically, in the securitisation market.

The impacted sectors include banking, insurance, factoring, leasing and other non-banking such as online lending.

The main current geographic target area is Europe.

For laws and regulations, there has been a great recent deal of progress in Europe, where a virtuous competition between member and non-member States is leading to the development of regulatory frameworks open to Blockchain and security tokens, particularly relevant for Stonize business. The most notable examples include Luxembourg, Liechtenstein, Switzerland, France and Germany.

Objective

Making finance more democratic, by distributing economic wealth more equally.

Stakeholders

- The platform users are all the operators across securitisation transactions (suppliers, originators, portfolio agents, servicers, SPVs, representatives of noteholders, and investors).
- In addition to platform users, are regulators / supervisor bodies (e.g. CONSOB, which is the Italian Companies and Exchange Commission, and Bank of Italy) and law enforcement (e.g. Guardia di Finanza) can benefit from a positive impact leveraging platform transparency.

Predicted outcomes

It is expected that securitisations to be run in a fully digital manner by leveraging platform accessibility and transparency. This will provide direct and timely liquidity to SMEs.

Why distributed ledger technology?

The platform is based on notarisation and tokenisation, which converts ownership rights into digital units of value. This is something that could not be done before.

Thanks to the platform securitisation stakeholders who manage the entire securitisation workflow more efficiently and with an “embedded trust”. Indeed, the way the platform employs permissionless blockchain renders asset management and performance tracking transparent and robust. The blockchain backbone provides a single source of truth, which brings efficiency (e.g. avoiding reconciliation effort) and catalyses trust among participants, encouraging parties to participate in securitisations even with unknown partners.

The technological issue has been tackled by developing the Trusted Token Transfer (T3) protocol, a proprietary solution that reduces the complexity of the securitisation. T3 makes the platform agnostic from the point of view of the blockchain technologies. However, this use case chooses Algorand for its advantages:

- It is an economically environmentally sustainable;
- It overcomes mining pool issues of private, federated and permissionless PoW-based blockchains;
- It has core functionalities implemented at Layer 1;
- It has a strong positioning as trusted partner for institutions;
- It has a shared vision of making finance more democratic.

9.4.3 User requirements

Functional requirements

a) Supplier: liquidity for its core business (e.g. factoring)

b) Originator: new investment opportunities (originators can “catalyse trust” by showing in a reliable manner their performance in order to attract investors)

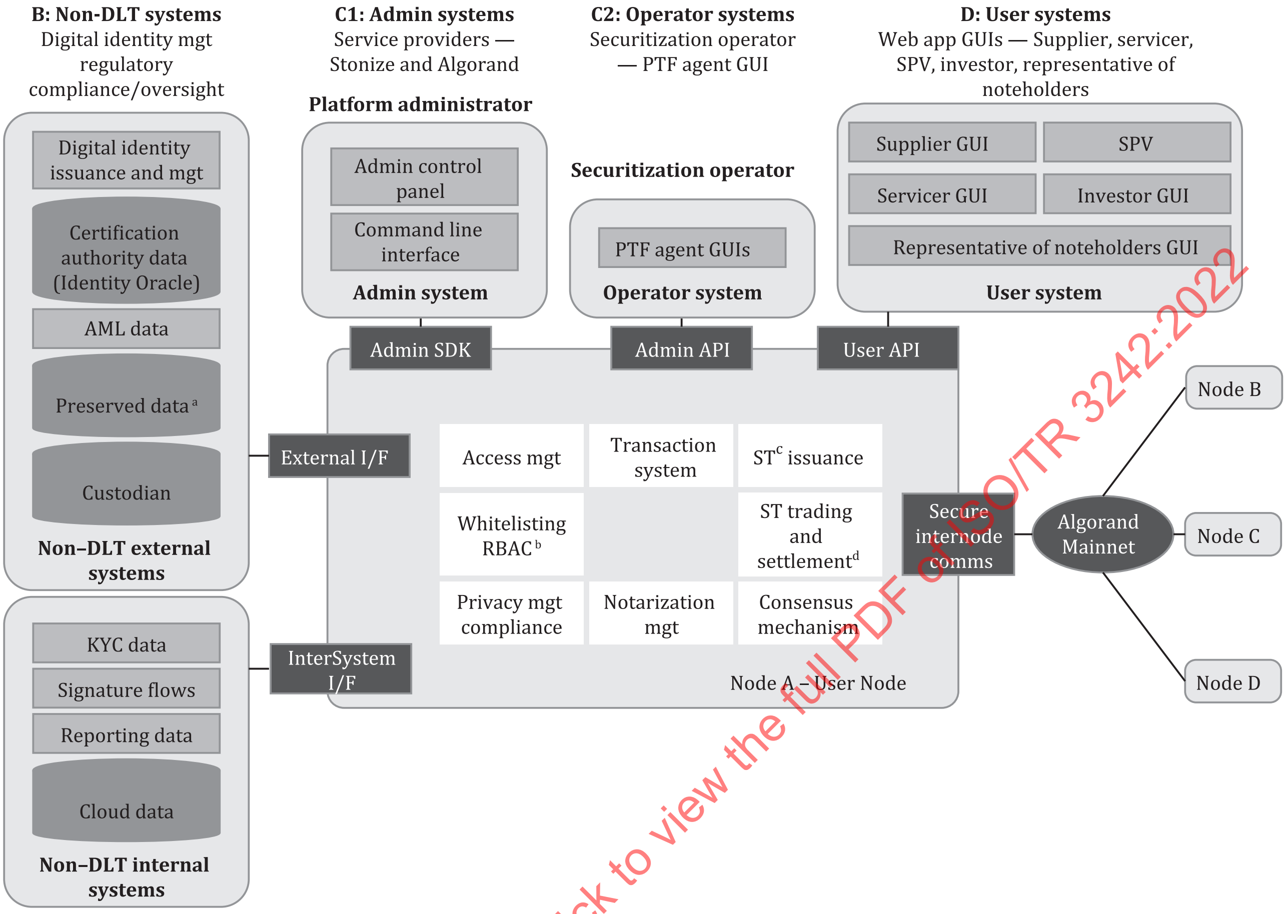
c) PTF Agent, SPV, Servicer, Representative of Noteholders: Efficiency

d) Investor: transparency

e) Regulators / Supervisor bodies and Law enforcement: ease and reliability of investigations

Visualizations: Figures 58 to 61

— Reference architecture



[a] For audit and compliance.

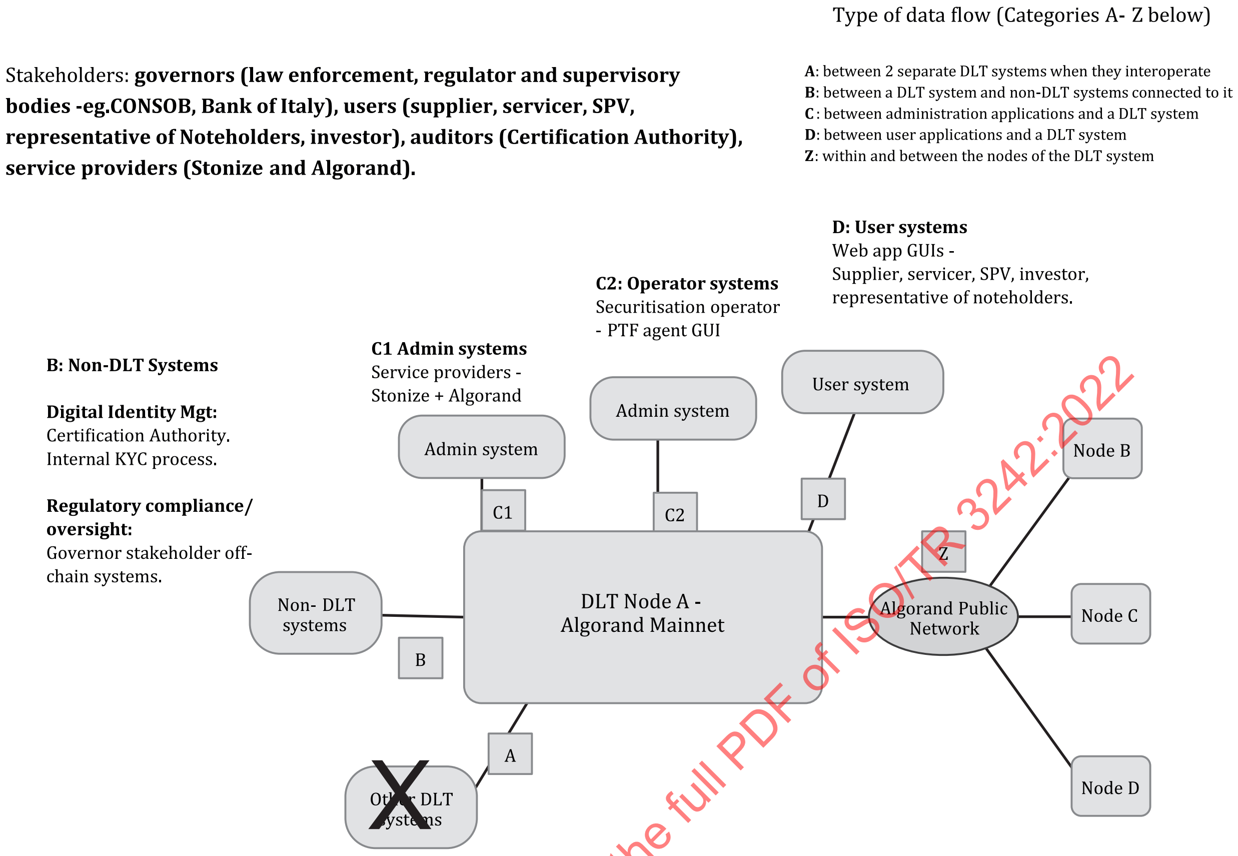
[b] Role-based asset control.

[c] Security token, implemented as ASA (Algorand Standard Asset) NF/NFT (Fungible/Non-Fungible Tokens).

[d] Implemented leveraging Algorand Layer-1 smart contract (ASC1): stateless smart contracts written in TEAL, automatically enforce custom rules and logic (e.g. freezing and clawback).

Figure 58 — System view architecture: Transparent securitisation (Italy)

— Data flow model



Type of data flow (Categories A- Z below)

Stakeholders: **governors (law enforcement, regulator and supervisory bodies -eg.CONSOB, Bank of Italy), users (supplier, servicer, SPV, representative of Noteholders, investor), auditors (Certification Authority), service providers (Stonize and Algorand).**

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

D: User systems
Web app GUIs -
Supplier, servicer, SPV, investor, representative of noteholders.

C2: Operator systems
Securitisation operator
- PTF agent GUI

C1 Admin systems
Service providers -
Stonize + Algorand

B: Non-DLT Systems

Digital Identity Mgt:
Certification Authority.
Internal KYC process.

Regulatory compliance/ oversight:
Governor stakeholder off-chain systems.

Figure 59 — Data flow analysis: Transparent securitisation (Italy)

— Behavioural UML

Use case diagram

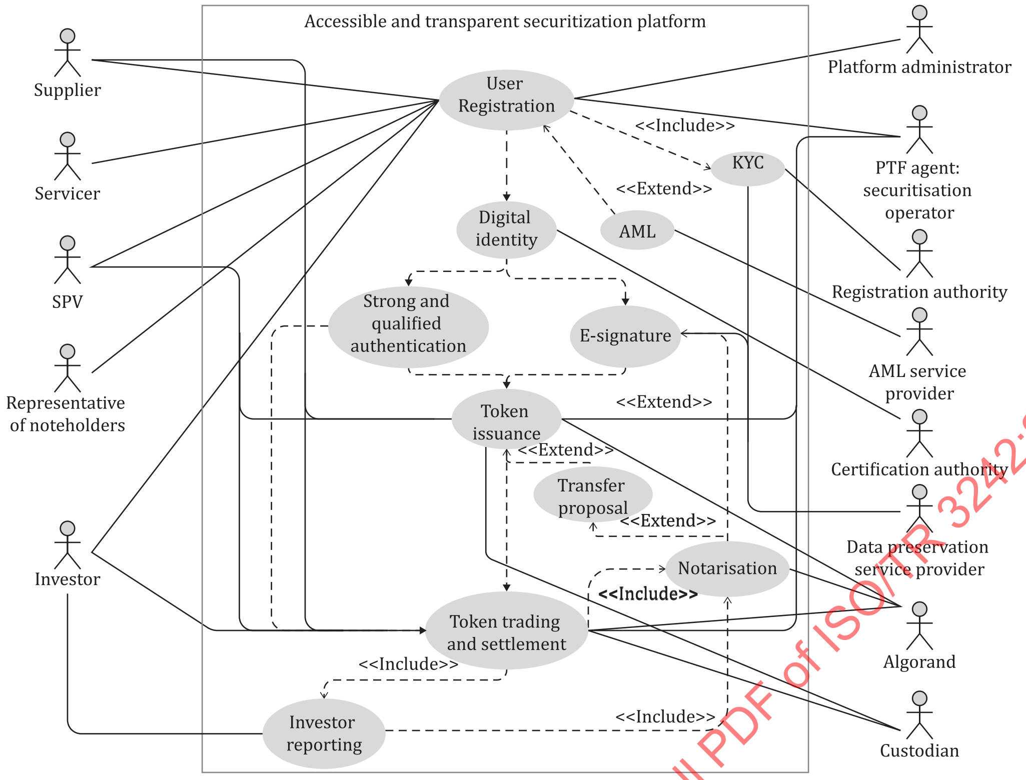


Figure 60 — Use case diagram: Transparent securitisation (Italy)

Interaction diagram

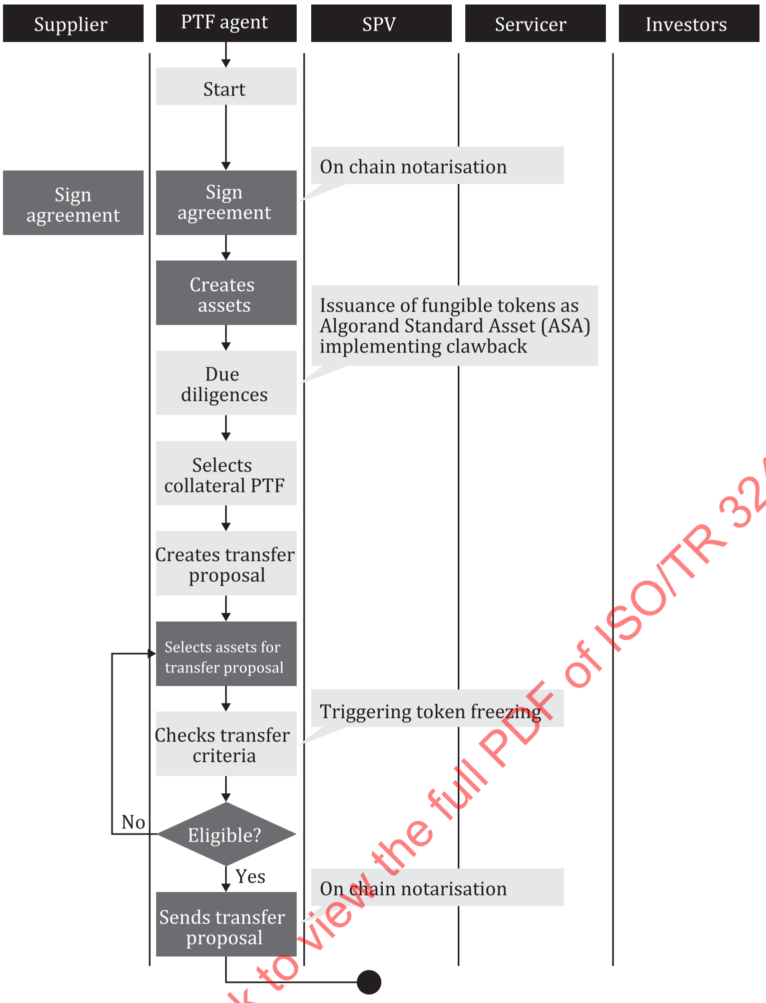


Figure 61 — Interaction diagram: Transparent securitisation (Italy)

Security, privacy and identity management:

As for the system security, considering that the entire approach is completely new to the securitisation industry, the main risk relates to the platform users. Its operators can be victims of cyber-attacks, especially those using social engineering, to take advantage of the low sensitivity to digitisation. To face cybersecurity risks, this use case is employing the highest security standards, risk relief features such as token freezing and clawback, token mirror, top-notch system auditors and, importantly, are educating clients especially against social engineering based attacks.

A fundamental aspect is related to privacy compliance with regulation (e.g. GDPR[15]) and user needs (i.e. supplier and investment confidentiality) and its apparent friction with the transparency of a permissionless blockchain such as Algorand. The issue is being addressed by using hashing techniques, pseudonymisation and multi-address wallets.

Identities are managed by an eIDAS compliant Certification Authority that, as a result of a self and remote KYC and (for specific user type) and automated AML, releases digital identity and electronic signature certificates for legally binding actions (strong and qualified authentications, authorisation, and signatures).

Pre and post conditions:

Pre-conditions:

— users' confidence in the use of electronic identity (e.g. for the e-signature of contracts)

- “post-hype” belief in permissionless blockchain
- availability of “digitised asset” (i.e. to standard digital representation of underlying assets)

Post-conditions:

- further evolution of the regulatory framework for blockchains (especially with reference to the exclusive custody of DLT-based digital securities)
- further adoption of electronic signatures (e.g. possibility to digitally sign also notarial deeds remotely)

Non-functional requirements:

- Digital identity: interoperability with and availability of Certification Authorities, AML and document preservation service providers.
- Blockchain requirements: highest level of decentralisation, real time verification, custodian integration, data integrity functionalities (freezing and clawback), audited technology and smart contracts.
- Others: usability, robustness, asset and process traceability, maintainability, agnosticity (meaning that the platform can be used with other blockchains), flexibility (meaning that the system can be delivered as a service or on premise).

9.4.4 Force field analysis

Legal considerations:

In addition to the legal considerations reported in this document, a major constraint is related to the fact that, by regulations, access to investment opportunities is today restricted to institutional investors (banks, insurance companies, investment/pension funds). However, the platform is designed in order to be accessible also to retail investors, starting from accredited ones. European regulatory framework could evolve in a way where institutions will be a trust reference for retail investors who took part in crowdfunding, peer-to-peer (P2P) lending, Initial Coin Offerings (ICOs) and stock market.

Risk:

The main risks are related to:

- Culture – the financial sector, with the exception of some specific areas, is not used to quickly embrace innovation from outside the financial institution.
- Regulation – although Blockchain and security token legal frameworks are evolving fast, here are still missing pieces in maintaining compliance with the traditional world, which hinders a fully digital process.
- Reputation – since securitization transactions are carried out on average on assets that have a total value of tens/hundreds of millions of euros, a strong brand can convert prospects into customers.
- Cybersecurity – (discussed above).

To overcome the cultural barrier, this use case leverages the most innovative stakeholders in the securitisation value chain and the operational efficiency needs of originators and portfolio agents

- Regarding regulation, although DLT technologies are being widely adopted in the various European legal systems, some operational holes still remain, such as those relating to custody. Important progress is expected in the most attentive jurisdictions of these aspects in the EU, such as Germany, where an important sector operator such as BitGo is starting its operations and applying to obtain the necessary licenses from the financial authority (BaFin). However, while this scenario evolves and full digital asset management is possible, Stonize employs a gradual approach for the custody, based on mirroring security tokens with traditional security.

- As for the reputation, this use case is plans to leverage the securitisation that the first client will launch in the second half of 2020 and Stoneize are executing a strategic partnership programme with institutional partners:
- Euronovate for the digital identity, electronic signatures and paperless workflow;
- Algorand for technology backbone, and the Italian National Research Council (CNR) for the technology transfer of research in the trust field.

Referenced standards:

Text

- Provisions, in the various jurisdictions, on securitisation (ex. Italian Law no. 130 of 30 April 1999).
- Data normalisation requirements, according to ESMA (EU 2017/2402)[39].
- European regulation on (eIDAS – EU Regulation 910/2014 of 23 July 2014[40] on electronic identification and repeals directive 1999/93/EC of 13 December 1999).
- The European General Data Protection Regulation (EU 2016/679[41]).
- Rules on the digital preservation of documents and data (e.g. art.44 of the Digital Administration Code in force in Italy).
- Various regulatory frameworks on blockchain and tokenization (e.g. Liechtenstein Blockchain Act, Switzerland Blockchain & Cryptocurrency Regulation, Luxembourg Bill 7364 on blockchain-based securities, France Decree no. 2018-1226 on the use of a blockchain for the representation and disposal of financial securities).

Open source software:

Scenarios:

Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.

Reference implementation (to show that a specification is implementable)

5. Test suites, unit tests, etc. for functionality tests Engagement:

B. Has evaluated/studied how to make meaningful use of Open Source Software

D. Open Source Software is critical for a successful adoption

Specific parts of the code will be open sourced (e.g. for design reasons, the smart contract handling the token issuance and transfer).

Others, such as the same T3 protocol, will be closed sourced but assessed using open source tools. This will provide a high level of transparency on the audit process and, in turn, will enhance further trust of this Stonize platform.

Other information:

In addition to the legal considerations reported in other parts of this document, a major constraint is related to the fact that, by regulations, access to investment opportunities is restricted to institutional investors (banks, insurance companies, investment/pension funds). However, the platform is designed in order to be accessible also to retail investors, starting from accredited ones.

Further information: Stonize S.r.l[42].

9.5 Pension process optimisation (China)

9.5.1 Categories

Transversal Category

- Electronic identification, trust services, e-signatures

Horizontal Category

- Process Optimisation

Vertical Category

- ISIC section: K-6530
- Section K - Financial and insurance activities
- Division 65 - Insurance, reinsurance and pension funding, except compulsory social security Group/ Class 6530 - Pension funding
- Source: ISIC. Rev. 4 (p.56

UN Sustainability Goals

- GOAL: Partnerships to achieve the Goal

Status

- In production/live implementation

9.5.2 Summary

Long description

Blockchain-based platform and smart contracts are making pension businesses and transactions more secure, efficient and cost-effective.

- The blockchain-based platform receives the payment receipt and application chart.
- The platform uploads the information to the blockchain. Then smart contracts automatically enforce obligations, which were set up in advance, and write the results to the blockchain.
- The related institutions obtain their part of information and requirements from the platform.
- After completing the assignments, the related institutions upload the results to the blockchain through the platform.
- The client receives the results from the platform.

Business problem or opportunity

The application of the blockchain technology allows the institutions to optimize the pension business process, enhance the development of automating pension business, as well as increasing capital utilization, and improving the customer experience.

Scope

The use cases are currently mainly applicable to China, involving various enterprises and employees in China.

Objective

Optimizing the pension business process by using the blockchain technology.

Stakeholders

- Agricultural Bank of China.
- China Taiping Insurance Group Ltd.
- The companies and their employees who have participated in this pension system

Predicted outcomes

- Enhancing efficiency. Shorten the business period from 2 weeks to 1 day to 2days.
- Improving capital utilization. Cost-saving.

Why distributed ledger technology?

As the core technology of a trusted value network, blockchain utilise asymmetric cryptographic algorithm, consensus mechanism, decentralization, permanency and immutability, which brings new opportunities for the development and innovation of pension business.

Blockchain technology allows every participant to become a node in the blockchain network. Therefore, every step of the business process can be recorded as data.

These data form a distributed ledger that is immutable and completely traceable. In other words, the data cannot be altered or deleted and it is easy to supervise.

The traditional pension business uses mail and paper receipts. The blockchain- based pension business is able to transfer the data from offline to online and secure the data.

The application of the blockchain technology allows the institutions to optimize the pension business processes, advance the automation of pension businesses, as well as increasing capital utilization and improving the customer experience.

9.5.3 User requirements

Functional requirements

The client requires the system to have functions, such as account establishment, pension payment, contribution payment, and investment management.

Visualizations: Figures 62 to 66

- **Reference architecture**

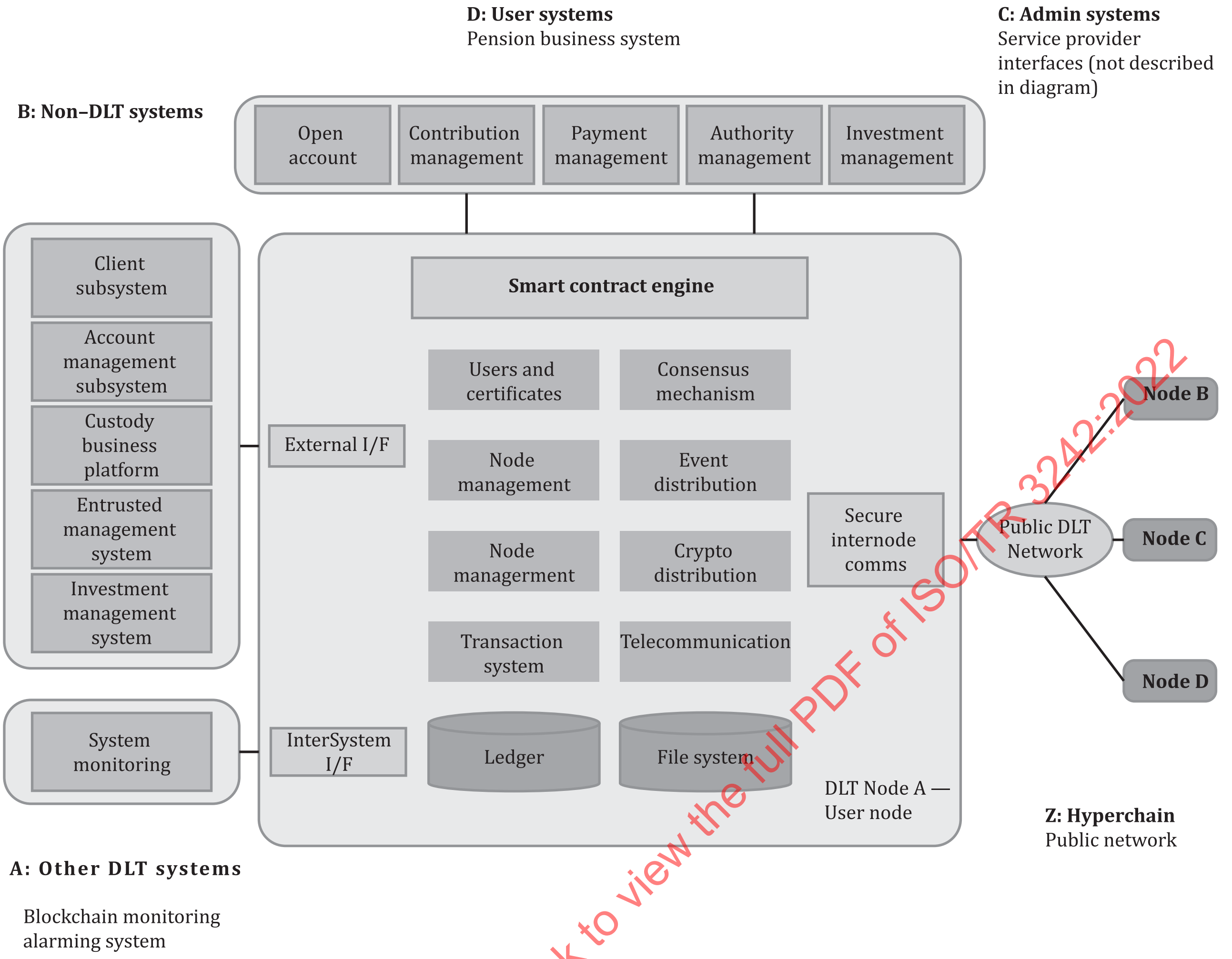


Figure 62 — Systems view architecture: Pension process optimisation (China)

— **Data flow model**

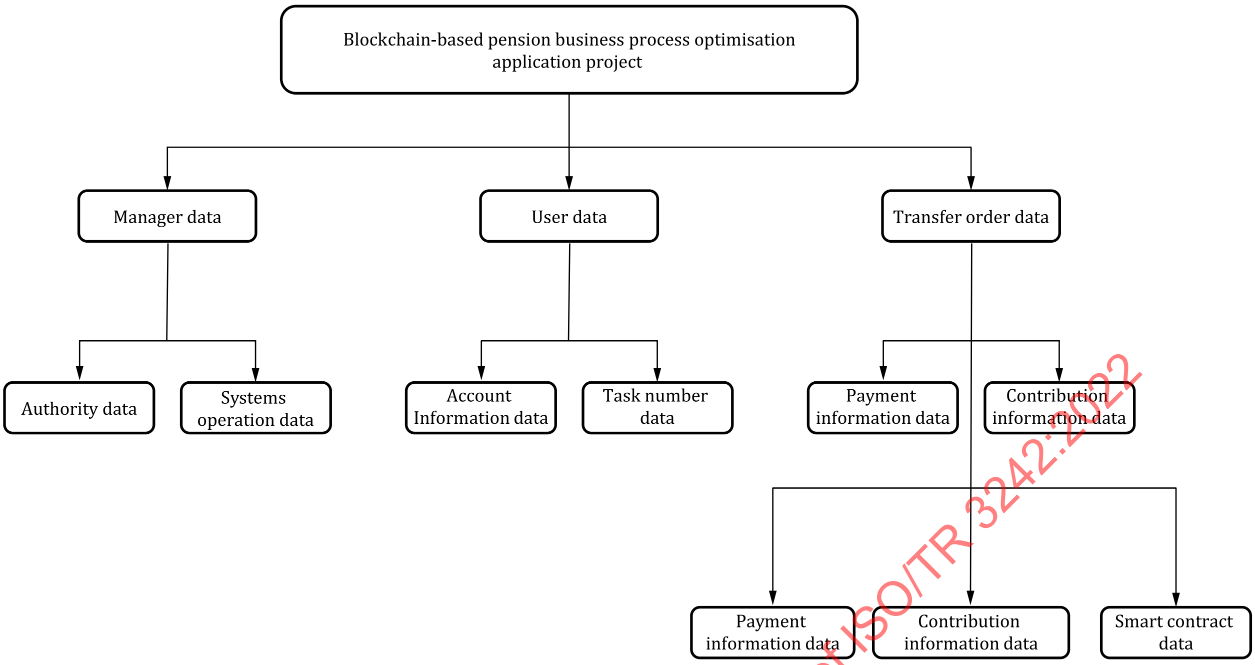


Figure 63 — Data flow and stakeholder roles: Pension process optimisation (China)

Data flows triggered by the data-related operations of which stakeholders:

i) Stakeholders: **Agricultural Bank of China, China Taiping Insurance Group Ltd., participants (users) Service provider (Hyperchain).**
ii) Type of data flow (Categories A- Z below)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

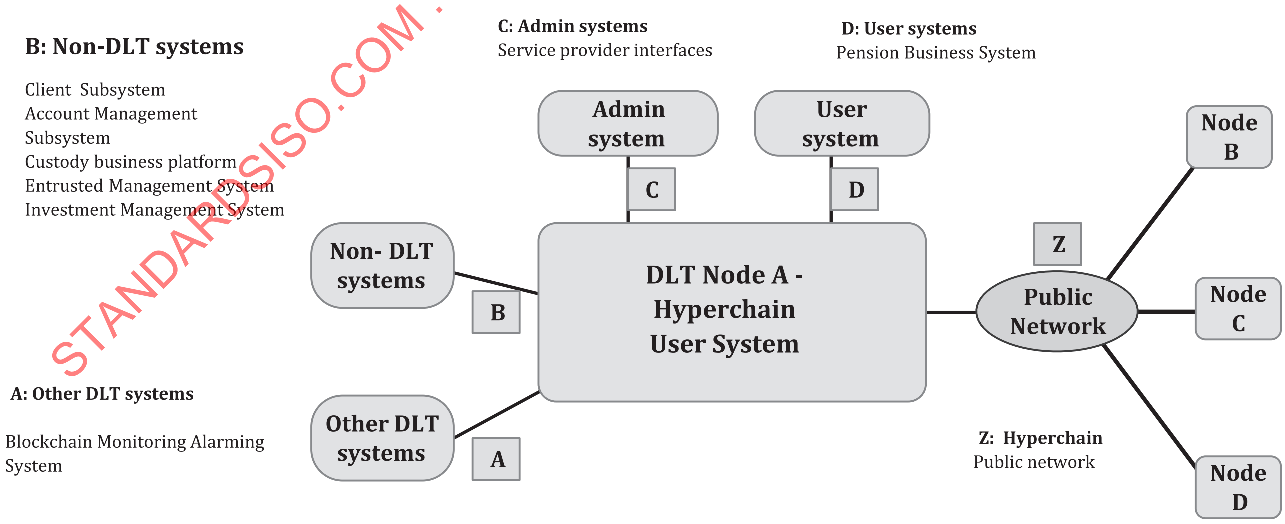


Figure 64 — Data flow analysis: Pension process optimisation (China)

— **Behavioural UML**

Use case diagram

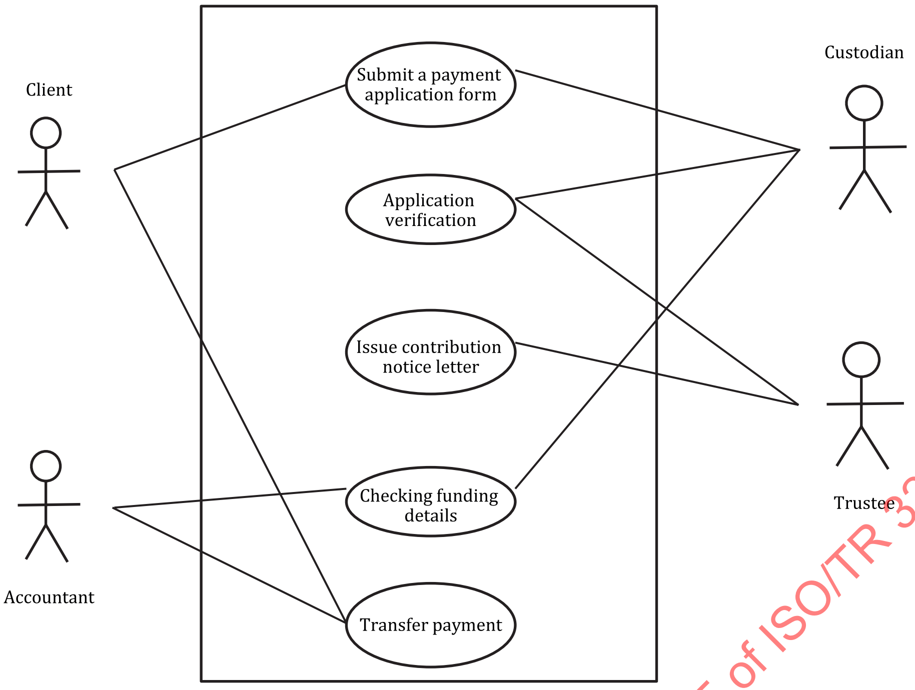


Figure 65 — Use case diagram: Pension process optimisation (China)

Sequence diagram

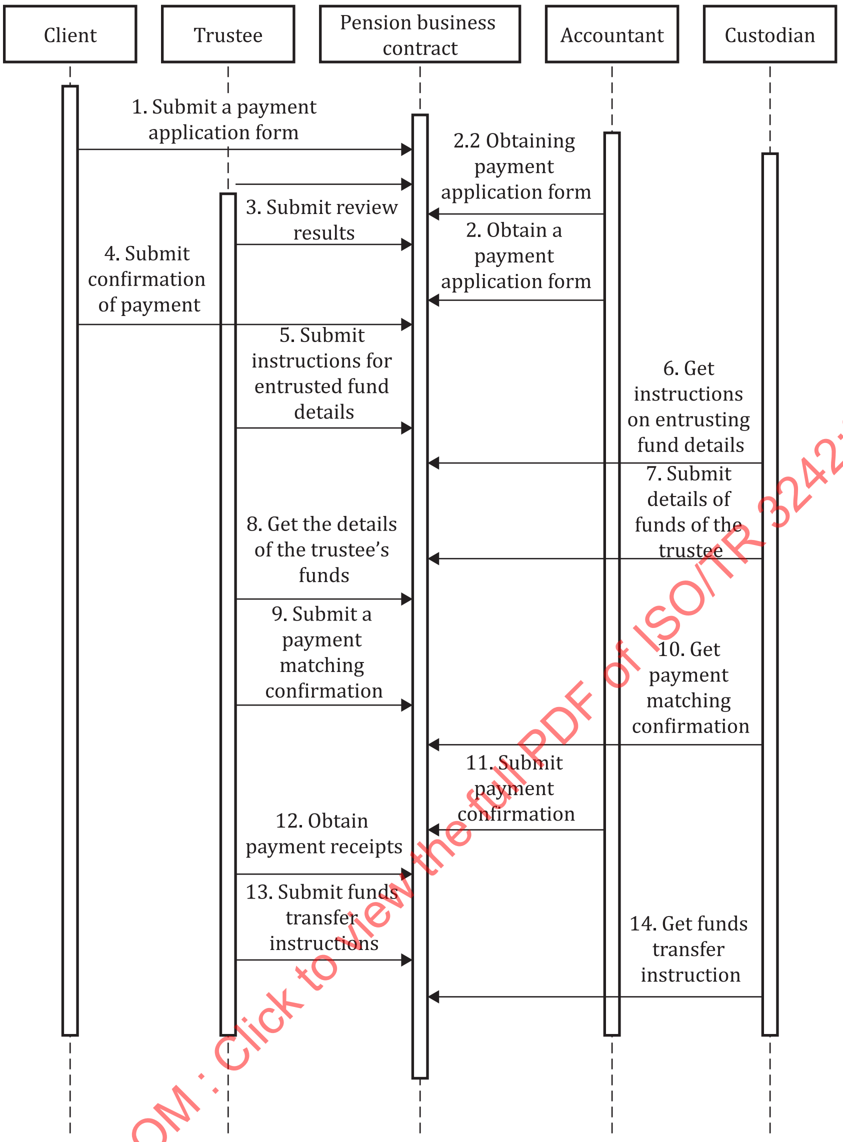

Client
Trustee
Pension business contract
Accountant
Custodian
1. Submit a payment application form
2.2 Obtaining payment application form
3. Submit review results
2. Obtain a payment application form
4. Submit confirmation of payment
5. Submit instructions for entrusted fund details
6. Get instructions on entrusting fund details
7. Submit details of funds of the trustee
8. Get the details of the trustee's funds
9. Submit a payment matching confirmation
10. Get payment matching confirmation
11. Submit payment confirmation
12. Obtain payment receipts
13. Submit funds transfer instructions
14. Get funds transfer instruction

Figure 66 — Sequence diagram: Pension process optimisation (China)

Security, privacy and identity management:

- The basic layer of the Hyperchain blockchain uses a pluggable encryption mechanism.
- The transport layer data is encrypted through the ECDH key negotiation technology, to ensure that the two parties can negotiate a key without sharing any information in the exchange. This key ensures the data can be transmitted securely by using the symmetric encryption algorithm.
- The platform adopts the national secret standard. The platform encrypts and transmits broadcast messages based on the SM4 symmetric encryption algorithm. It also signs the transaction by using the Elliptic Curve Digital Signature Algorithm (ECDSA) or national secret algorithm in order to prevent the information from being maliciously tampered with.
- The pension system platform adopts strict CA system control for the institutions' access control. The certificate issuance of all nodes is controlled by the platform. The self-built CA system is provided by Hyperchain and provides complete certificate life cycle management.
- The integration of decentralized CA architecture is through smart contracts. Nodes joining the network need to broadcast a join request to the network first. Other nodes vote and arbitrate

through a decentralized CA mechanism to decide whether the node can be joined. If the vote is passed, a certificate is sent to complete identity management and control.

Pre and post conditions:

- Pre-condition: The ownership of a Chinese pension business licence by the members of consortium blockchain who participate in the pension business.
- Post-condition: A controllable and trusted blockchain platform for participants.

Non-functional requirements:

- Transaction volume per second: 300 transactions/second the supported maximum number of client connections: 1 000.
- Performance - Transaction volume per second: 300 transactions/second; the supported maximum number of client connections: 1 000.
- Response time: query response time is less than 1 second/time; Daily transaction volume: over 5 million transaction volume; Concurrency: The system supports 500 concurrent numbers.
- Capacity - The system supports data archiving, off-chain migration, and high volume data storage.
- Usability - The system uses ECDSA, SM2, SM4, and SHA256 encryption algorithms to ensure system security.

9.5.4 Force field analysis

Legal considerations:

The business design of pension projects are subject to relevant laws and regulations of the Chinese Constitution, the Labour Law, and the Social Insurance Law.

Risk:

The pension system will face some risks and problems when it wants to extend its business. For instance, some ongoing businesses need to transfer to the new pension system.

The possible scenario is requiring the system to connect with another consortium blockchain, which can have a different technical structure to the ABC-Taiping pension system. This technical difficulty can cause some uncertainties in data storage and data consistency.

Other information:

The existing business scenarios in the blockchain-based pension system are no longer sufficient to meet our assumptions and needs.

Use of an autonomous and controllable consortium blockchain, Hyperchain.

However, another influential consortium blockchain is using Fabric. These two blockchains belong to heterogeneous chains.

Use of cross-chain technology BixtHub to build a bridge between the two chains.

9.6 Decentralised Charity Platform (the Republic of Korea)

9.6.1 Categories

Transversal Category

- Public sector information and open data

- Electronic identification, trust services, e-signatures
- Accessibility of ICT products and services

Horizontal Category

- Data Provenance
- Process Optimization
- Automation

Vertical Category

- Classification: Q-0123
- Section Q - Human health and social work activities
- Division 88 - Social work activities without accommodation
- Group 889 - Other social work activities without accommodation
- Class 8890 - Other social work activities without accommodation

UN Sustainability Goals

- No Poverty
- Zero Hunger
- Good Health and Well-being
- Quality Education
- Clean Water and Sanitation
- Reduced Inequality
- Sustainable Cities and Communities

Status

- In production/live implementation

9.6.2 Summary

Long description

The most urgent problem facing the Korean donation industry is the transparency and reliability of donation fund management, and securing the market potential of donation services and stabilizing decentralization of blockchain technology to create a micro-donation ecosystem that can be practically used by all citizens.

To this end, the use case has three goals:

- Revitalization of micro donation ecosystem,
- autonomous operating systems based on encryption, and
- building a platform that guarantees reliability/efficiency, and the Ethereum and POA consensus algorithm.

Based on the “Luniverse” blockchain technology, commercial donation using apps/web services were launched in November 2019. By June 2020, more than 3,000 general donors have joined and are raising a total of more than 150 thousand US dollars.

Business problem or opportunity

The fundamental problem is the intensification of social inequality, and the development of ICT technology that paid attention to the possibility that collective small-scale donations such as crowdfunding can replace traditional donations.

- The first barrier is low awareness of donations and lack of trust in donor organizations' fund operation. The embezzlement and wrong fund management by some donor organizations has created problems that have led many to avoid donations.
- The second barrier is a blockchain technology. Blockchain is the most promising solution to ensure donor organizations' credibility and facilitate micro-donation, but it is still in its infancy. Technological challenges to be solved at a practical level such as the right amount of performance, reliability and safety of payment, securing of autonomous operating system, and judgement and selection of good donation are scattered.

Scope

In this use case, to revitalize the Republic of Korea's donation ecosystem, this blockchain platform makes it is possible to register various campaigns presented by all non-profit organizations established in the Republic of Korea, and it provides app/web services for all Korean citizens to participate as donors.

The entire process of donation process from campaign registration to the donation fundraising by fiat money was built to operate based on a blockchain and smart contracts. Further development is underway in 2020, in which the fundraising amount is delivered to the final beneficiary's wallet and is actually used through linkage with the voucher system.

Objective

To solve the problems of the Korean donation ecosystem raised by this case, the following three core goals were set and promoted across the Republic of Korea.

- Revitalize of micro donation ecosystem
- Establish autonomous donation system (based on smart contract)
- Build a platform with reliability / efficiency

Stakeholders

The key stakeholders of this use case include the donors, beneficiaries, donation management organizations, payment agencies, and charity consortium.

Predicted outcomes

With the activation of the micro donation culture in which all citizens participate, the service can not only distribute wealth from donors to beneficiaries, but also secure the efficiency and transparency of many human and material resource operations that are put into the donation industry. It also seeks to improve the soundness of donor organizations and create meaningful social impact.

The role of this blockchain this use case is to expand and supply secured infrastructure technologies to other application fields. These include, blockchain ledgers that have secured reliability and performance, payment systems linked to secure fiat currencies, and a donation culture that allows users to participate voluntarily. In the future, this use case aims to provide a potential donation ecosystem by activating Charity as a Service, with a white label solution.

Why distributed ledger technology?

Decentralized charity platform promises some notable advantages for charitable organizations and donors, which include:

- Procedural transparency: each donation transaction is unique, which means that it is also easily tracked through the blockchain. The higher level of transparency and public accountability can ease donors' minds and encourage them to give while also reinforcing the charity's reputation for integrity.
- Global and decentralized: most blockchain networks present high levels of decentralization, meaning that they do not need to rely on a centralized government or other institution. Thus, funds can move directly from donors to charities, and the decentralized nature of blockchain makes it uniquely suitable for international transactions
- Digital agreements: blockchain makes it easier to share and store digital data, and can also be used to ensure that important documents or contracts cannot be modified without the approval of all involved members.
- Cost reduction: blockchain technology has the potential to simplify the way charities are managed, automating parts of the process and reducing the overall costs by requiring fewer intermediaries.

9.6.3 User requirements

Functional requirements

- Donor: Transparent donation monitoring, influence proportional to the accumulated donation amount, participation in donation campaign evaluation and selection of bad campaigns.
- Donation campaign operator: Donation campaign planning, strict donation execution by smart contract, experiment with various donation campaigns.
- Beneficiary: Donation delivery by smart contract, use points and vouchers that fit the purpose.
- Payment agency: Payment service to guarantee fiat currency exchange, support for donation participation in various ways such as mobile and web.

Visualizations: Figures 67 to 70

- **Reference architecture**

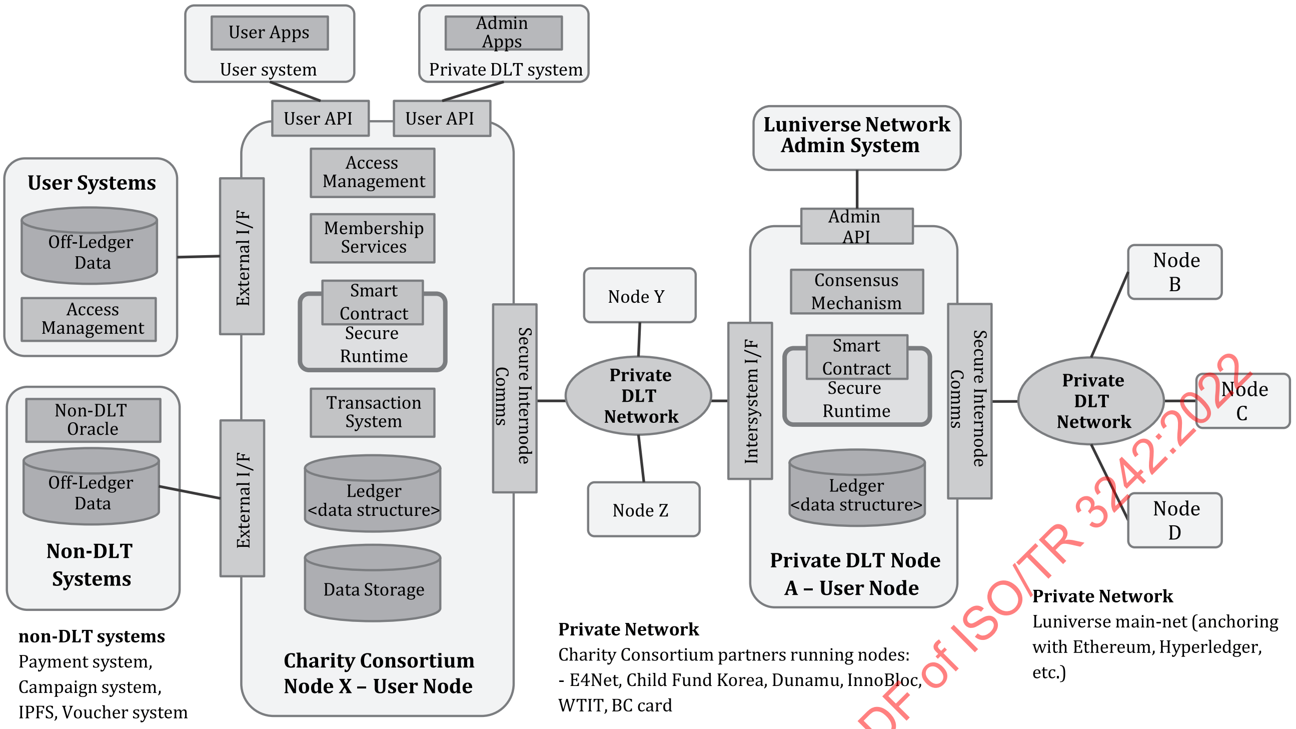


Figure 67 — Systems view architecture: Decentralised Charity Platform (the Republic of Korea)

— Data flow model

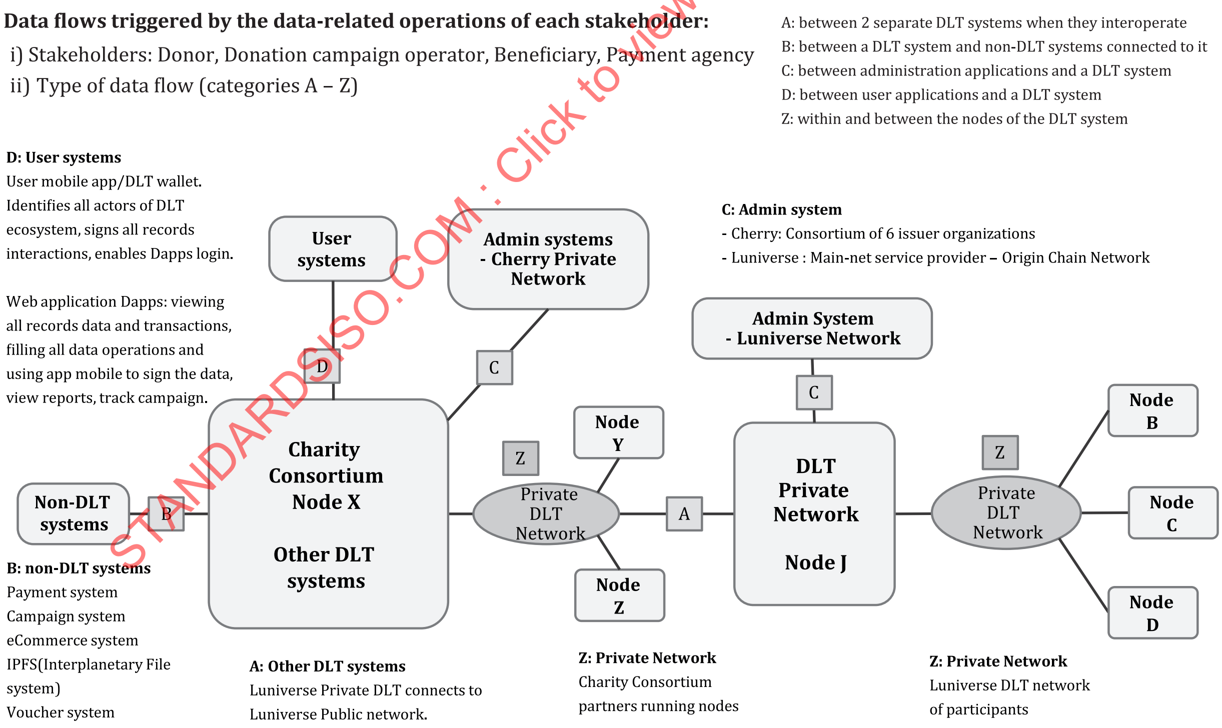

Data flows triggered by the data-related operations of each stakeholder:
i) Stakeholders: Donor, Donation campaign operator, Beneficiary, Payment agency
ii) Type of data flow (categories A – Z)
A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system
D: User systems
User mobile app/DLT wallet. Identifies all actors of DLT ecosystem, signs all records interactions, enables Dapps login.
Web application Dapps: viewing all records data and transactions, filling all data operations and using app mobile to sign the data, view reports, track campaign.
User systems
Admin systems - Cherry Private Network
C: Admin system
- Cherry: Consortium of 6 issuer organizations
- Luniverse : Main-net service provider – Origin Chain Network
Admin System - Luniverse Network
D
C
C
Charity Consortium Node X
Other DLT systems
Non-DLT systems
B
Z
Node Y
Private DLT Network
Node Z
A
DLT Private Network
Node J
Z
Private DLT Network
Node B
Node C
Node D
B: non-DLT systems
Payment system
Campaign system
eCommerce system
IPFS(Interplanetary File system)
Voucher system
A: Other DLT systems
Luniverse Private DLT connects to Luniverse Public network.
Z: Private Network
Charity Consortium partners running nodes
Z: Private Network
Luniverse DLT network of participants

Figure 68 — Data flow analysis: Decentralised Charity Platform (the Republic of Korea)

— Behavioural UML

Use case diagram

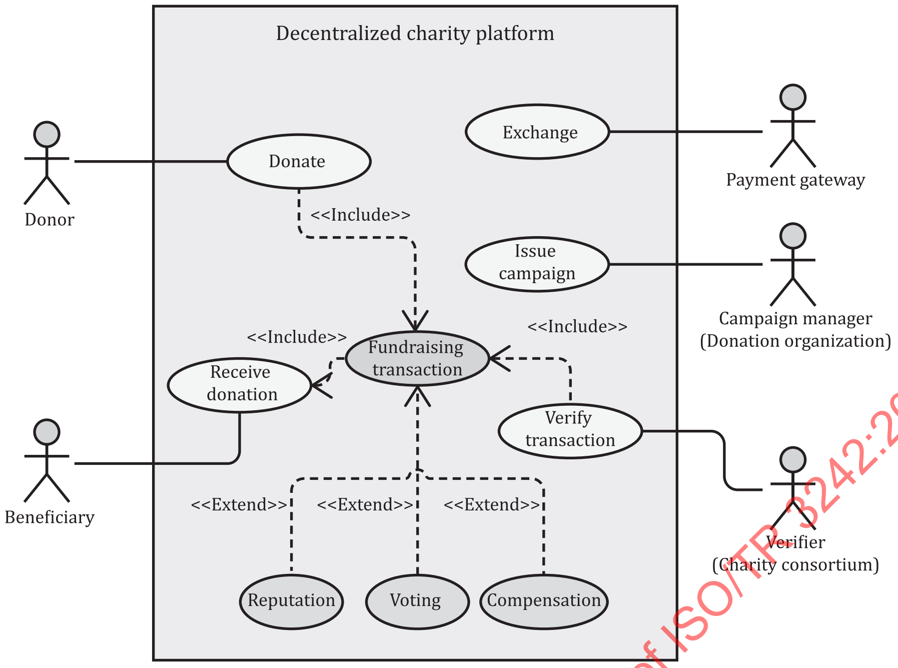


Figure 69 — Use case diagram: Decentralised Charity Platform (the Republic of Korea)

Sequence view diagram

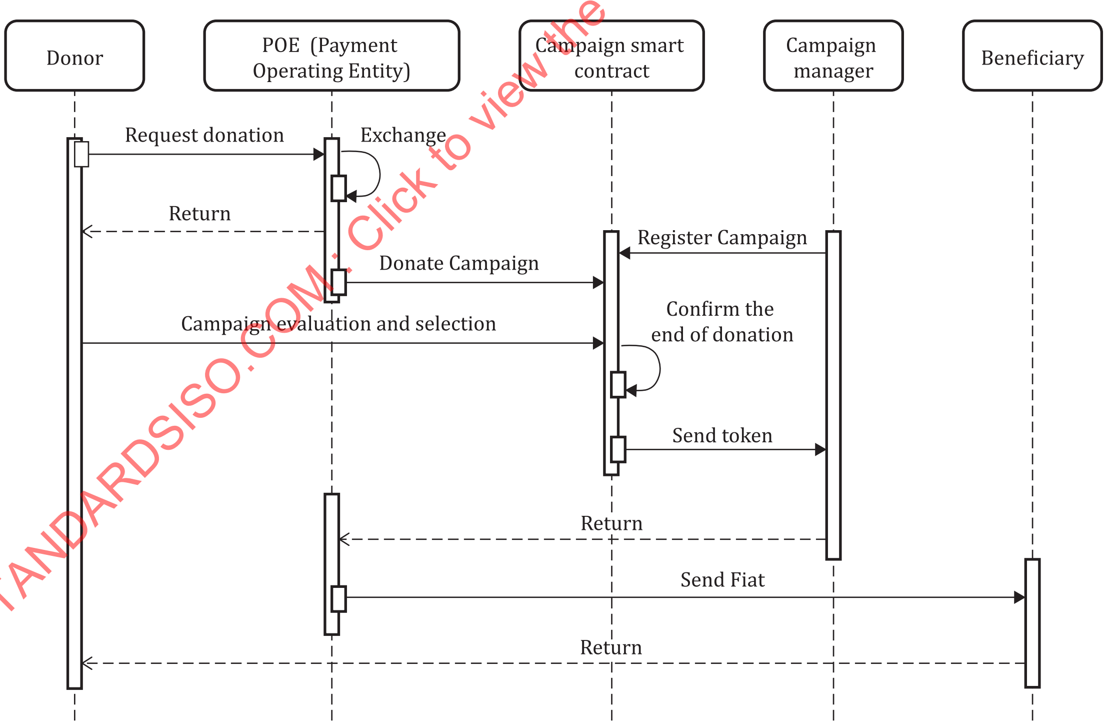


Figure 70 — Sequence diagram: Decentralised Charity Platform (the Republic of Korea)

Smart Contracts

Smart contracts in use case were applied to three areas: inter-blockchain interlocking, autonomous curation processing, and donation token payment/payment.

- Interlocking between blockchain chains: Donation token raising/execution, main/side chain bridge, public/main chain bridge, pegging of main/side chain.

- Autonomous curation handling: donation impact management, voting management, and objection.
- Payment/payment of donation tokens: Charge donation tokens, refund, exchange money, link payment agencies.

Security, privacy and identity management:

The identity management is guaranteed through the creation of a wallet for each actor, the private key is saved on the individual device of the actor and the privacy of the data is guaranteed by cryptography algorithms.

- Only authorized access is allowed for all resources such as network communication section and database.
- Option to directly manage the user of the key management to prevent the loss and hacking of the user's private key.
- Enhance security by utilizing a key management system based on a hardware security module (HSM).
- Provide high security beyond the level required by the industry by performing communication channel level encryption and end-to-end data encryption on sensitive information such as personal identification information and private key.

Pre and post conditions:

An internet connection is required to access the Cherry (donation app) and portal, and also for the verification process which checks against Luniverse's distributed ledger.

Non-functional requirements:

Applying a private blockchain for performance cannot completely address the concern about reliability, which is the most important value in the donation process. Therefore, solving the trade-off problem that ensures decentralized reliability without central control while securing performance such as transaction speed is necessary. Also, due to the nature of the donation process, frequent exchange of values with fiat money is essential, so there is a need to solve this transaction stability that must secure the reliability of external data input linked with fiat without compromising decentralized characteristics.

An internet connection is required to access the Cherry (donation app) and portal, and also for the verification process which checks against Luniverse's distributed ledger.

9.6.4 Force field analysis

Legal considerations:

There are legal restrictions on legal tender and settlement in the Republic of Korea.

- Problems with payment fees such as credit cards and CMS.
- The donation law has a problem with using regulations within 15 % of the amount raised.
- Problem of registering a fundraising amount of more than 100 thousand dollars.

Risk:

The introduction of open blockchain technology has a problem with its stability when the number of node participants is too small. In this use case, the plan is to gradually increase the number of node participants with a thorough system testing to analyse the stability verified from a pilot project.

There are no constraints on commercialization other than technical and legal restrictions.

Open source software:

- 1. Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.
- 2. Reference implementation (to show that a specification is implementable)
- 3. Required part of a standardization deliverable
- 4. Complementary to a standardization deliverable
- 5. Test suites, unit tests, etc. for functionality tests

Assessment of your engagement in Open Source Software.

- D. Open Source Software is critical for a successful adoption
- F. It was easy to collaborate with Open Source Software communities
- H. Open Source Software is critical for validation of implementations.

Other information:

The decentralized charity platform was selected and promoted as a national project by Ministry of Science and ICT from April 2019 based on the experience of developing donation apps by E4NET. And it ended successfully at the end of 2019. The plan is to prepare for a full-scale expansion to complete decentralization technology in 2020.

The implications obtained through this example are as follows.

- The importance of approaching the project to innovate creatively, of not following the structure and process of the existing donation industry. This use case focused on changing the structure of the limited donation process centred on a small number of large donation organizations to enable various open campaigns, and to enable donors to participate directly in the operation of the campaign.
- Above all, it is important that the best companies with the necessary skills to build and operate the donation platform can work together. This includes the Republic of Korea's largest children's public foundation, Dunamu (the Upbit operator) with blockchain technology expertise, smart contracts, and technology specialists Innoblock, BC Card, etc.
- It was a project aimed to solve social problems by bringing up a participation rate of the entire nation in donation culture and to achieve a breakthrough in blockchain technology. Providing a service that everyone can easily participate in and a practical solution to the difficulties of the blockchain is facing can help create a desirable blockchain ecosystem.

10 Use cases: Supply Chain

10.1 International trade transparency (Singapore)

10.1.1 Categories

Transversal Category

- 5. Electronic identification, trust services, e-signatures
- 7.e-Infrastructures for research
- 8.Accessibility of ICT products and services

Horizontal Category

- List text.
- 1. Identity Management
- 2. Data Provenance
- 3. Governance
- 5. Process Optimisation
- 6. Automation

Vertical Category

- Section J - Information and communication (p. 56, ISIC, Rev.4) Group 631 Data processing, hosting and related activities; web portals

UN Sustainability Goals

- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 10: Reduced Inequality
- GOAL 11: Partnerships to achieve the Goal

Status

- 5. in production/live implementation
- 6. a completed trial or pilot
- 8. an integration with current systems

10.1.2 Summary

Long description

TradeTrust is a digital utility that comprises a set of globally-accepted standards and frameworks that connects governments and businesses to a public blockchain to enable trusted interoperability and exchanges of electronic trade documents across digital platforms.

- Legal Harmonisation: Providing legal validity for electronic negotiable documents.
- Standards Development: Developing international standards that this company can conform with.
- Accreditation Structure: Certifying technical solutions in accordance with relevant requirements.
- Software component: A set of open-source codes that can easily integrate backend solutions to the TradeTrust network.

This initiative is supported by Infocomm Media Development Authority, Singapore

Business problem or opportunity

This use case aims to provide participants with the proof of integrity and provenance for these electronic documents, addressing the inefficiencies caused by manual verification processes that resulted from a lack of trust. It aims to promote greater use of digital documents for cross border trade, help lower operating costs for businesses and government authorities and facilitate faster movement of goods across borders.

It addresses the issue of paper-based bills of lading, and how the ownership transfer of the title document (e.g. negotiable bills of lading) could be from person A using system A to person B using System B (see User Requirements diagrams).

Scope

The use case application is available to all locations/countries and is international. The code is open sourced.

While the title-transfer mechanism was designed to be MLETR-compliant (Model Law on Electronic Transferable Records), applicable laws and regulations will be dependent on the users.

Objective

The objective is to conduct transfer of title-documents across 2 different systems.

Stakeholders

International Trade community e.g. Carriers, importers, exporters, banks, forwarders, and other intermediaries

Predicted outcomes

Transfer of ownership of title document (e.g. Bill of lading) from one party to another.

Why distributed ledger technology?

- Public and Permissionless (e.g. No central governance authority)
- Data Provenance
- Irrevocable and tamper-resistant transactions
- Fraud minimisation

10.1.3 User requirements

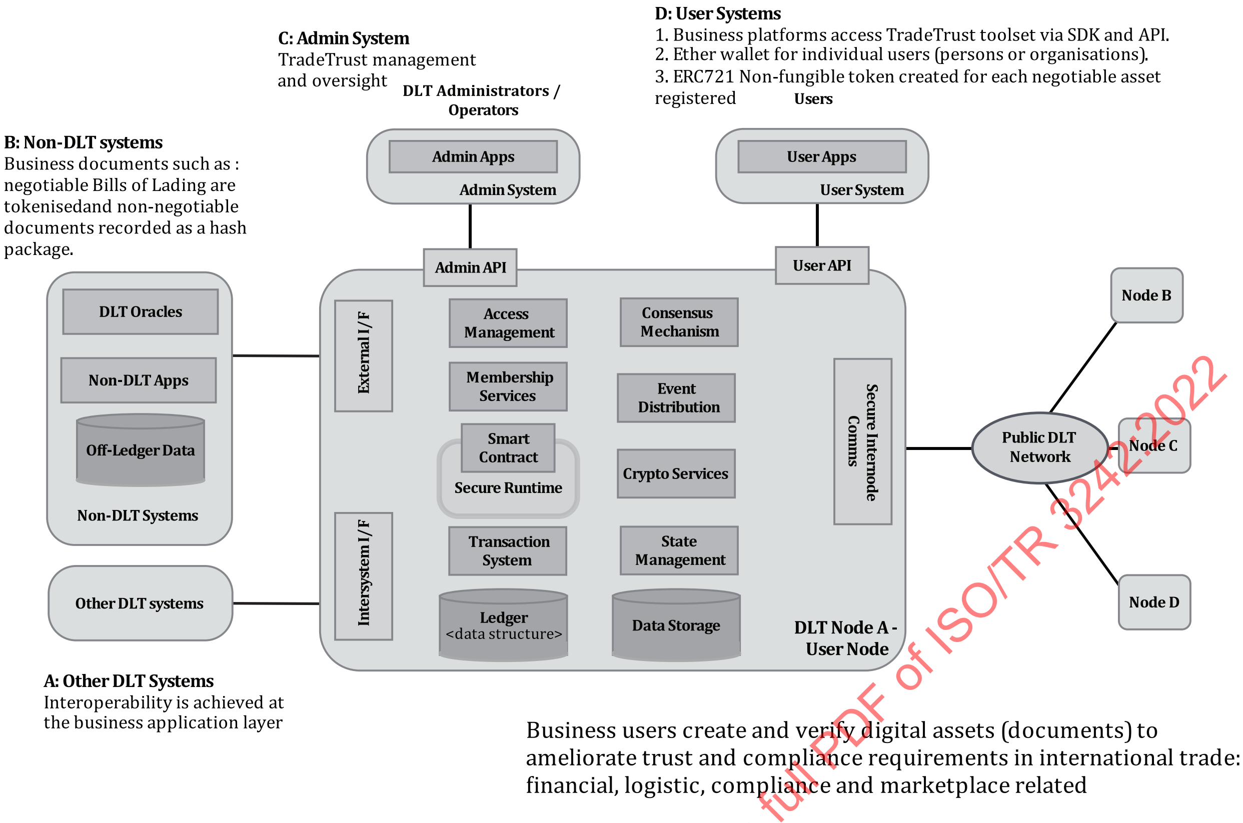
Functional requirements

Key design principles:

- Public and Permissionless: No central governance authority
- Data Off-Chain: Preserves data confidentiality
- Payload Agnostic: No data format or standard restriction
- Open-Source: Full transparency for faster adoption
- MLETR-Compliant: Meet the requirements of the law (for electronic negotiable documents)

Visualizations: Figures 71 to 75

- **Reference architecture**



C: Admin System
TradeTrust management and oversight

D: User Systems
1. Business platforms access TradeTrust toolset via SDK and API.
2. Ether wallet for individual users (persons or organisations).
3. ERC721 Non-fungible token created for each negotiable asset registered

B: Non-DLT systems
Business documents such as : negotiable Bills of Lading are tokenisedand non-negotiable documents recorded as a hash package.

A: Other DLT Systems
Interoperability is achieved at the business application layer

Business users create and verify digital assets (documents) to ameliorate trust and compliance requirements in international trade: financial, logistic, compliance and marketplace related

Figure 71 — System view architecture: International trade transparency (Singapore)

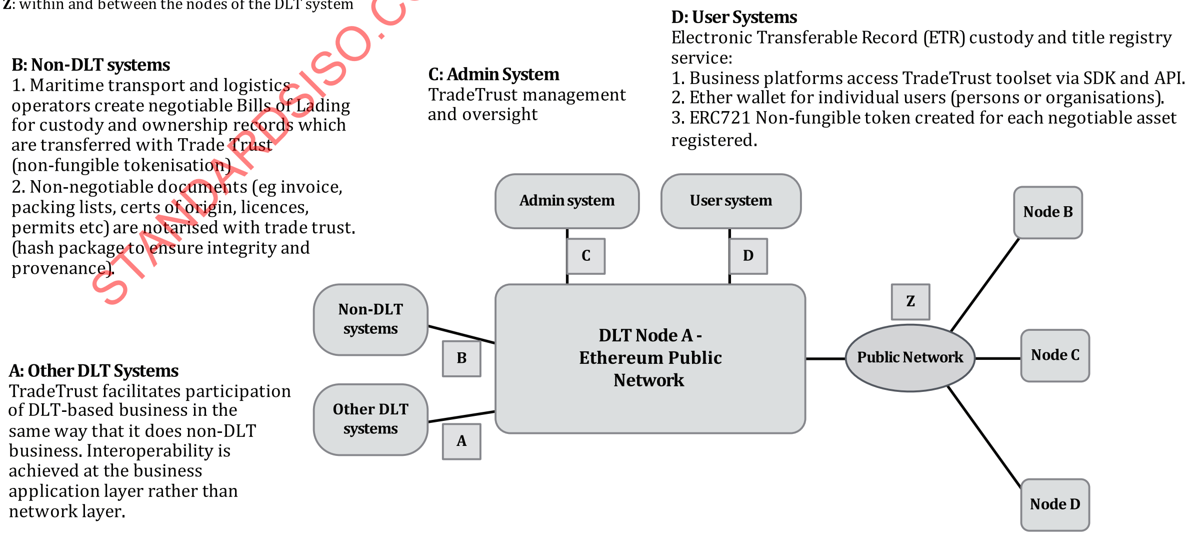
— **Data flow model**

Data flows triggered by the data-related operations of each stakeholder:

i)Stakeholders: Business users (create and verify digital records), BDLT service provider: TradeTrust.

ii)Type of data flow(categories A-Z)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non -DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system



D: User Systems
Electronic Transferable Record (ETR) custody and title registry service:
1. Business platforms access TradeTrust toolset via SDK and API.
2. Ether wallet for individual users (persons or organisations).
3. ERC721 Non-fungible token created for each negotiable asset registered.

B: Non-DLT systems
1. Maritime transport and logistics operators create negotiable Bills of Lading for custody and ownership records which are transferred with Trade Trust (non-fungible tokenisation)
2. Non-negotiable documents (eg invoice, packing lists, certs of origin, licences, permits etc) are notarised with trade trust. (hash package to ensure integrity and provenance).

C: Admin System
TradeTrust management and oversight

A: Other DLT Systems
TradeTrust facilitates participation of DLT-based business in the same way that it does non-DLT business. Interoperability is achieved at the business application layer rather than network layer.

Figure 72 — Data flow analysis: International trade transparency (Singapore)

— **Behavioural UML**

Use case diagram

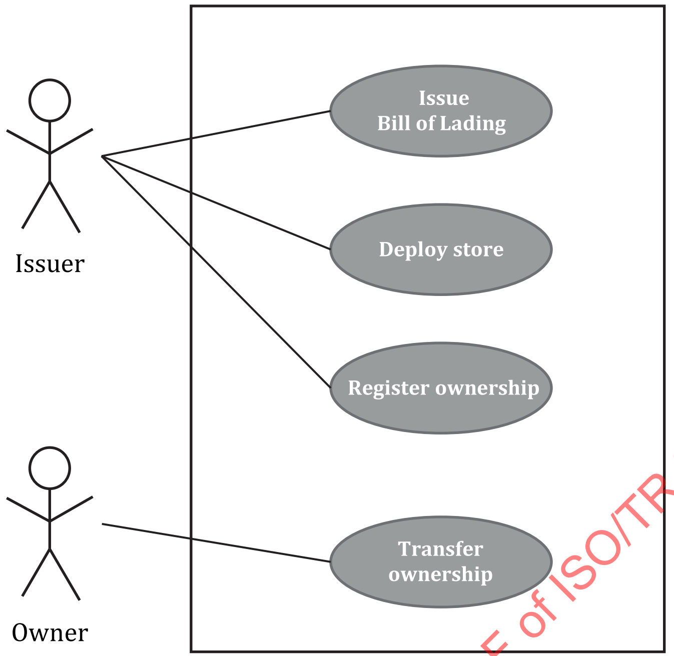


Figure 73 — Use case diagram: International trade transparency (Singapore)

Sequence diagram - Issue Bill of Lading

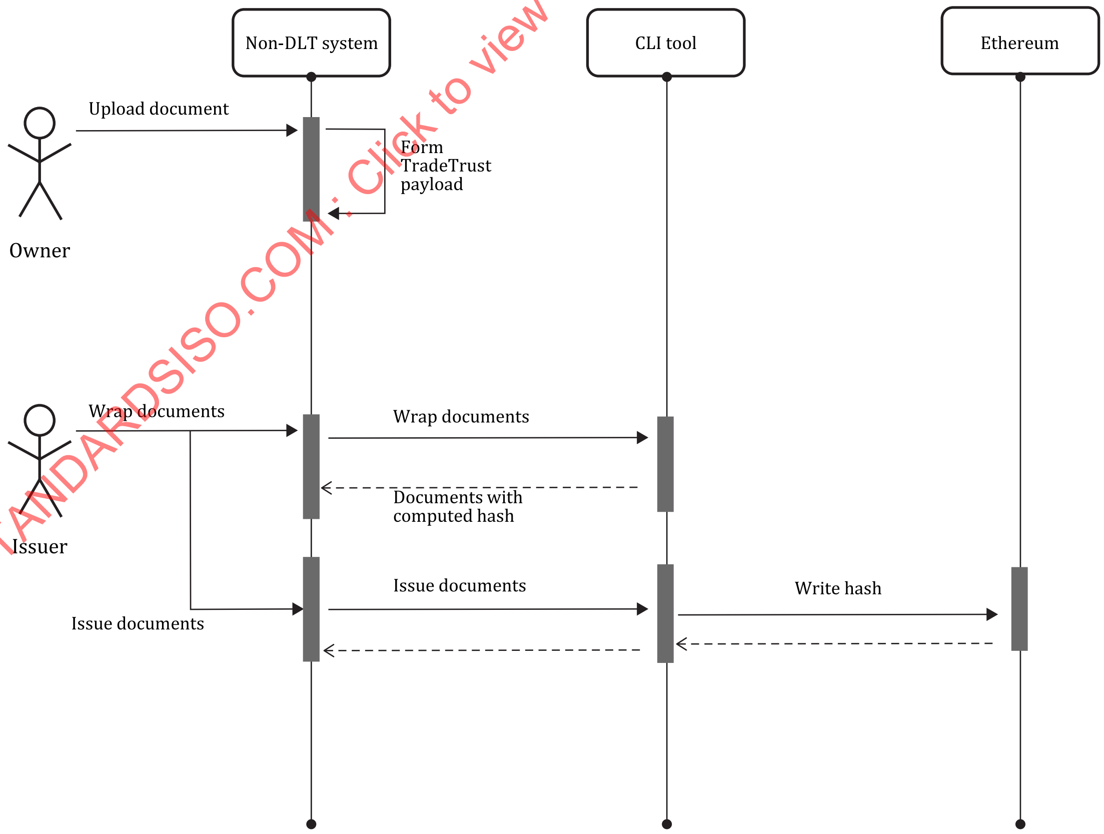


Figure 74 — Sequence diagram: International trade transparency (Singapore) – Issue Bill of Lading

Sequence diagram - Transfer ownership of Bill of Lading

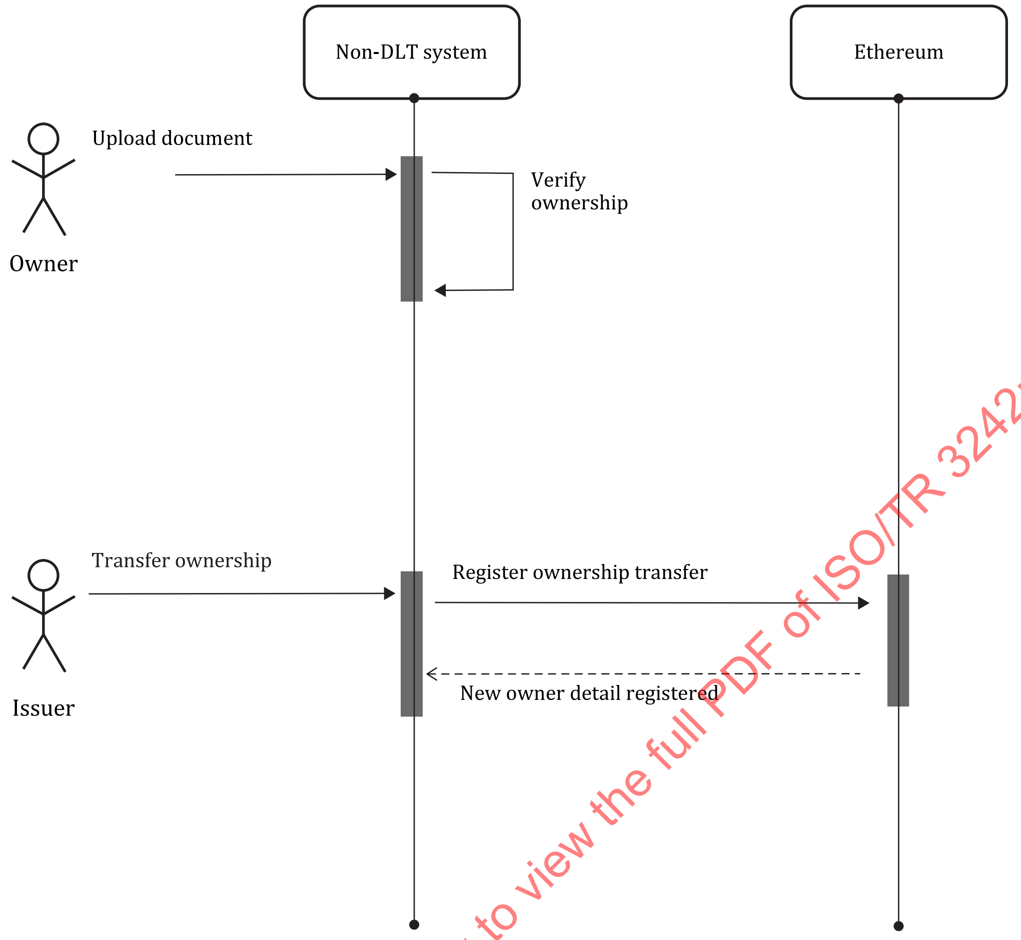


Figure 75 — Sequence diagram: International trade transparency (Singapore) –Transfer ownership of Bill of Lading

Smart contracts:

Document Store smart contract: this smart contract is deployed once per issuer, by the issuer himself. The responsibilities are:

- To only allow modifications by the owner.
- Store and retrieve a list of hashes that have been issued, and when they were issued.
- Store and retrieve a list of hashes that have been revoked, and when they were revoked.

Title Escrow smart contract: this smart contract is deployed to allow more than 1 owner to enter into a joint ownership to effect transfer of token.

Security, privacy and identity management:

Document holder can decide with whom to share the document, as well as which parts of the document to share.

When the verifying party uploads the document to the TradeTrust.io portal for verification, the portal does not store a copy of the document. Thus, ensuring the certificate is held only by intended recipients of the data.

Verification does not require an interaction with the issuer's system, thus reducing the need to expose a public endpoint, which in turn reduces the potential attack surface.

Pre and post conditions:

An internet connection is required to verify TradeTrust documents against Ethereum's distributed ledger and an additional Ethereum wallet and credit/gas is required to generate TradeTrust document or perform transfer of title documents.

Non-functional requirements:

As TradeTrust offers an open sourced component aimed at international audience, and as blockchain is a new technology for the industry, well-written documentation would be easy for a user to pick up and use.

To maintain trust among different users across the network, transactions can be recorded on a public network to remain transparent while ensuring privacy for the users.

10.1.4 Force field analysis

Legal considerations:

Some constraints could revolve around determining users' identity.

Risk:

Blockchain being a new technology, it is not easy for non-technical trained people to use (e.g. wallet ids) despite a user-friendly interface.

Referenced standards:

UNCITRAL Model Law on Electronic Transferable Records (MLETR)-compliant.

Open source software:

Scenarios:

- Interoperability aspects of software systems or applications, such as an API, protocol, data structures, etc.
- Reference implementation (to show that a specification is implementable)
- Required part of a standardization deliverable
- Complementary to a standardization deliverable
- Test suites, unit tests, etc. for functionality tests

Engagement in Open Source Software.

- B. Has evaluated/studied how to make meaningful use of Open Source Software
- D. Open Source Software is critical for a successful adoption
- F. It was easy to collaborate with Open Source Software communities
- H. Open Source Software is critical for validation of implementations

Other information:

TradeTrust Framework started off with the aim to tap on opportunities provided by new digital technologies and work with various countries to accelerate digital innovation in global trade.

The industry sees the value and need for digitalizing Title documents (e.g. Bills of Lading) so that the trade process will be more efficient.

Further information:

Trade Trust, Infocomm Media Development Authority, Singapore[43].

The Trade Trust code is open sourced and available on gihub[44].

10.2 Maritime Bill of Lading (Israel)

10.2.1 Categories

Transversal Category

- 1. Cloud computing
- 2. Public sector information and open data
- 5. Electronic identification, trust services, e-signatures

Horizontal Category

- 5. Process Optimization

Vertical Category

- Section H, Transportation and storage
- Division 52, Warehousing and support activities for transportation Group 522, Support activities for transportation
- Class 5229 Other transportation support activities

UN Sustainability Goals

- GOAL 8: Decent Work and Economic Growth
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 14: Life below Water
- GOAL 15: Life on Land

Status

- 4. in trial or pilot

10.2.2 Summary

Long description

This use case is an initiative of the International Port Community Systems Association in Israel. There are a number of direct players in the Bill of Lading (BoL) process:

- In the exporting country: Exporter, Exporter's customs agent, Exporter's shipping agent, advising bank.
- In the importing country: Importer, Importer's customs agent, Importer's shipping agent, Issuing bank
- The physical BoL is a pain point to the community:
- Business risk: Lose, forgery, delay in delivery of physical document, commercial disputes.
- High handling time & costs: Issue, deliver, validate, compare, process, change physical documents.

The IPCSA Blockchain based Digital BoL service will allow all those business process players to issue, approve and endorse the BoL.

The BoL is a transferable document, in any given moment only one entity can "hold" the BoL, in other words, be the owner of the cargo. Blockchain eliminates the Double Spending Problem, once the BoL is moved from "holder" A to B, the transaction is written in the immutable Blockchain ledger, then it is visible to all participants so "holder" A can't now transfer it again to C.

PCSs added value to Blockchain based Digital BoL process:

- Existing trusted networks for process harmonization and integration.
- Adding real time port processes information to reduce risk
- Bridging different technology adoption levels
- Gateway for local and global network
- Gateway to government authorities

Business problem or opportunity

A recent study of Digital Container Shipping Association (DCSA) estimates a potential $4bn could be saved per annum at a 50 per cent digital BoL adoption rate by the container shipping industry.

Scope

There has been a pilot with more than 20 stakeholders of the maritime trade in: Spain, Ukraine, Israel, Germany, Italy, and China.

Objective

The pilot conclusions, technical and ecosystem, will be used as the base for the development and the implementation of the production phase which is expected to deliver significant savings in time and money to all participants in maritime supply chain while maintaining a high level of information security, reducing risks and preventing forgeries.

Stakeholders

- Exporters, Importers, Customs agents, Shipping agents, Banks

Predicted outcomes

- Applying IPCSA Blockchain BoL service will reduce the industry pain points:
- Lower probability for frauds that leads to reduces business risk.
- Using real Port data (through PCS) such as arrival/departure time, reduces risk by receiving online first- hand information.
- Reduce handling time and costs.
- Reduce storage costs.
- Better service for the customers.

Why distributed ledger technology?

The BoL is sensitive to the ‘double spending’ problem: the same digital file being ‘copy-and-pasted’ and transferred multiple times. For that reason, existing digital signature solutions are not enough to digitalize, but blockchain technology offers a solution. Using Smart contract and workflow will reduce handling time, especially when changes are made in a BoL.

10.2.3 User requirements

The business logic of the existing manual workflow was transformed to a blockchain smart contract:

The Ship Agent, after receiving the cargo, issues the BoL and forward it to the Exporter;

The exporter after reviewing forward it to the Advising Bank;

- The Advising Bank after reviewing forward it to the Issuing Bank; In the importing country:

The Issuing Bank after reviewing forward it to the Importer;

The Importer after reviewing forward it to the Ship Agent;

- The Ship Agent after reviewing sends a delivery order to the port and to the importer with which he can release the cargo from the port (the delivery order is already digital in most of the ports served by IPCSA members).

From the moment a stakeholder is added to the transaction he can:

- See the status of the BoL (who is the holder in a given time)
- See the status of the cargo (such as loaded/unloaded) using real Port data that exists in PCSs.

The early adopters will have a possibility to connect directly to the Blockchain network and for the others a web application was developed using Rest API for the connection to the web application.

The smart contract enforces the restrictions according to the business rules, for example only the shipping agent can issue a BoL in the exporting country.

Using Blockchain distributed immutable ledger gives built-in security and transparency to the solution.

Functional requirements

The early adopters will have a possibility to connect directly to the Blockchain network, which will give them the possibility to integrate to their internal systems and minimize manual data entry/retrieving.

For the others a web application was developed. Actors include:

PCSs, Banks, Customs Agents, Exporters, Importers, Shipping Companies from Spain, Ukraine, Israel, Germany, Italy, China.

Visualizations: Figure 76 to 79

- **Reference architecture**

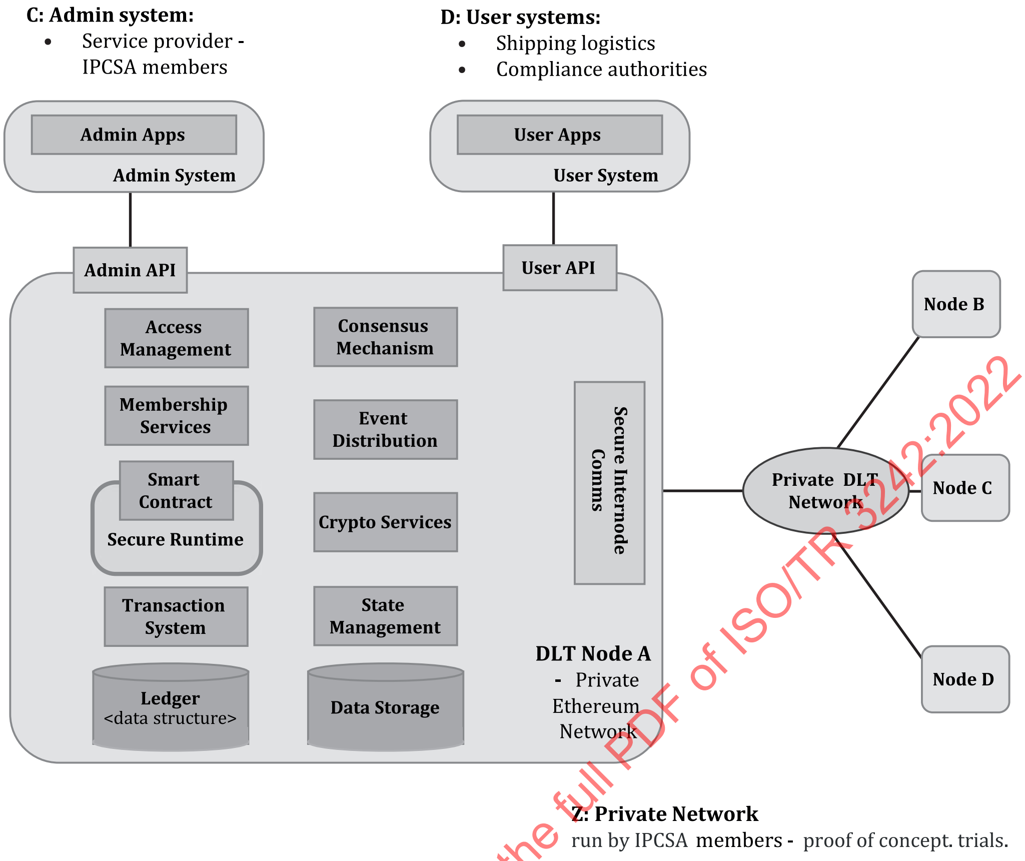


Figure 76 — Systems view architecture: Maritime bill of lading (Israel)

— **Data flow model**

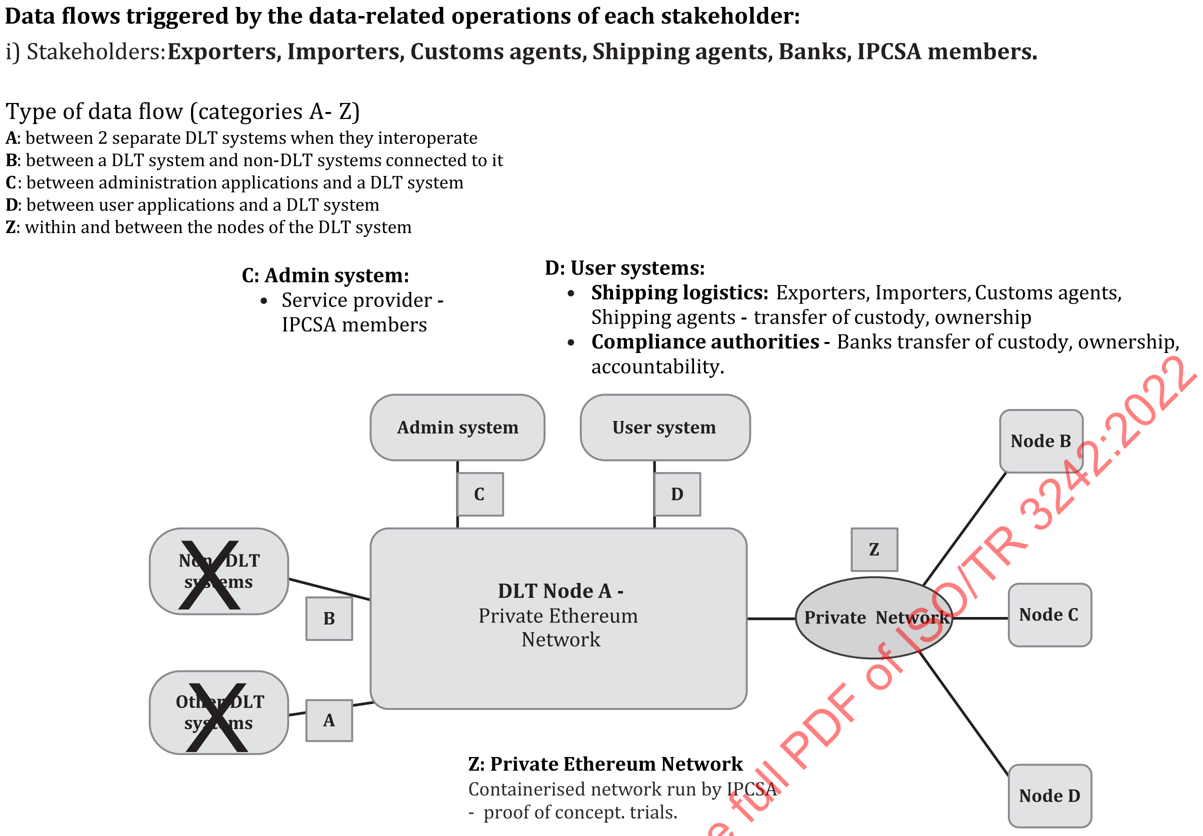

Data flows triggered by the data-related operations of each stakeholder:
i) Stakeholders: Exporters, Importers, Customs agents, Shipping agents, Banks, IPCSA members.
Type of data flow (categories A- Z)
A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system
C: Admin system:
Service provider - IPCSA members
D: User systems:
Shipping logistics: Exporters, Importers, Customs agents, Shipping agents - transfer of custody, ownership
Compliance authorities - Banks transfer of custody, ownership, accountability.
Admin system
User system
C
D
Non-DLT systems
B
DLT Node A - Private Ethereum Network
Other DLT systems
A
Z
Private Network
Node B
Node C
Node D
Z: Private Ethereum Network
Containerised network run by IPCSA
- proof of concept. trials.

Figure 77 — Data flow analysis: Maritime bill of lading (Israel)

— **Behavioural UML**

Use case diagram

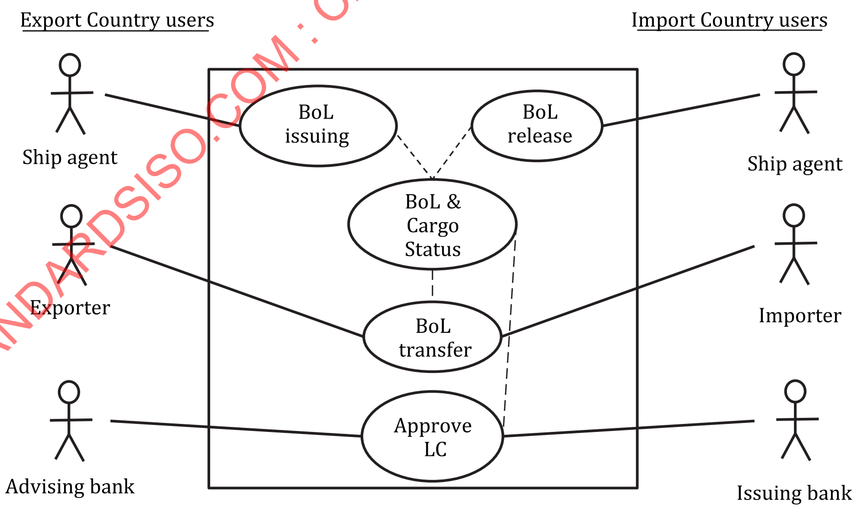


Figure 78 — Use case diagram: Maritime bill of lading (Israel)

Interaction diagram

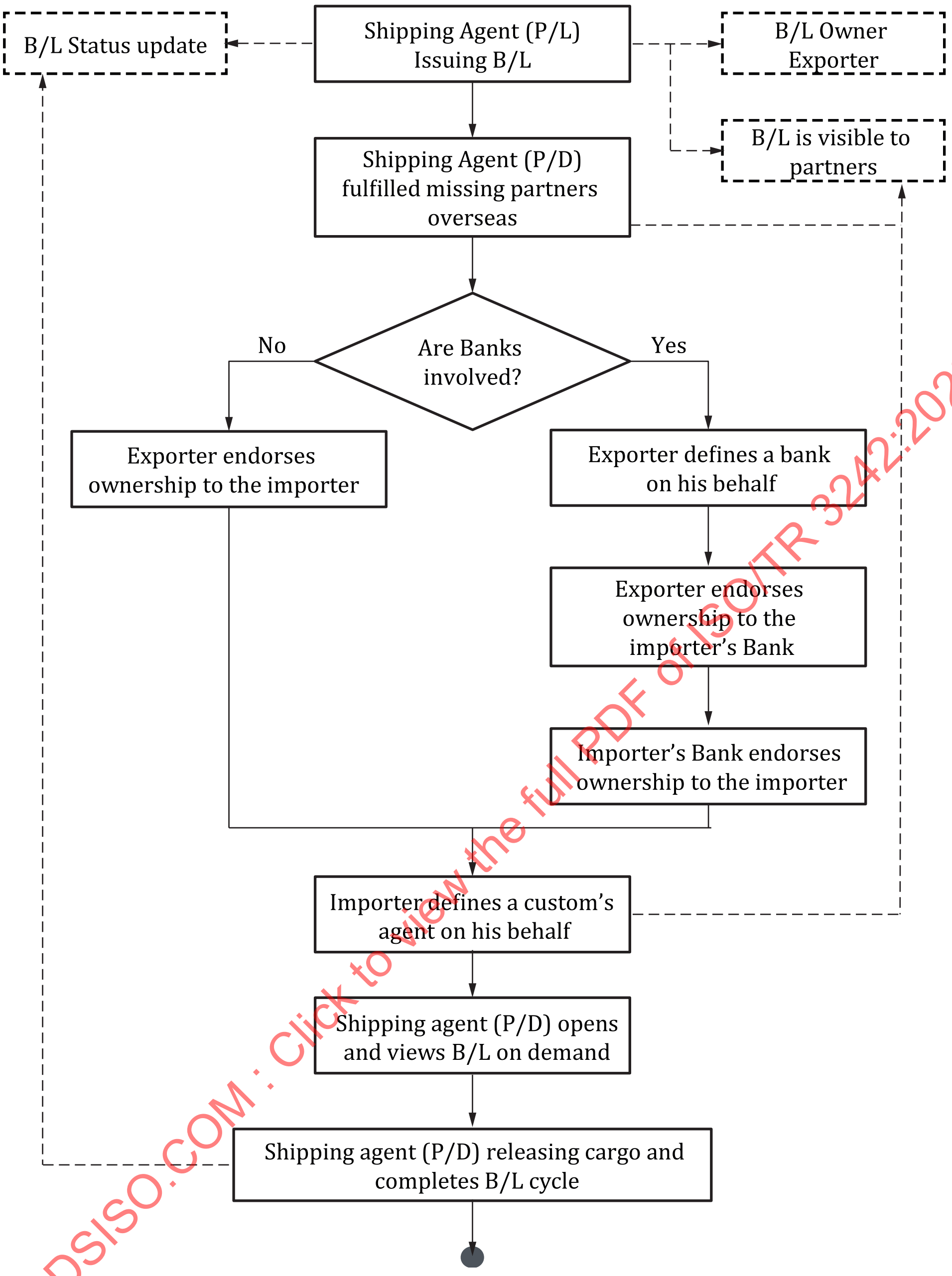

B/L Status update
Shipping Agent (P/L) Issuing B/L
B/L Owner Exporter
B/L is visible to partners
Shipping Agent (P/D) fulfilled missing partners overseas
Are Banks involved?
No
Yes
Exporter endorses ownership to the importer
Exporter defines a bank on his behalf
Exporter endorses ownership to the importer's Bank
Importer's Bank endorses ownership to the importer
Importer defines a custom's agent on his behalf
Shipping agent (P/D) opens and views B/L on demand
Shipping agent (P/D) releasing cargo and completes B/L cycle

Figure 79 — Interaction diagram: Maritime bill of lading (Israel)

Smart Contracts

The business logic of the existing manual workflow was transformed to a blockchain smart contract, for example: only the shipping agent can issue a BoL. The smart contract was developed using Solidity.

Security, privacy and identity management:

The solution is a permissioned blockchain and its infrastructure is based on Microsoft's Azure Blockchain Workbench, an advanced platform for easily building prototype blockchain apps in the cloud.

This platform provides the tools for the Security, privacy and identity management implementation: Authentication, Key storing, SFTP.

Pre and post conditions:

- Prerequisites: Enrolment to the System, Finding relevant cargo shipment that involves participant stakeholders.
- Post-condition: More stakeholders to join the initiative.

Non-functional requirements:

At the pilot phase, the number of transactions is low for that reason, many of the considerations are not relevant.

At the production phase, the requirements for: transactions per second, confirmation time, scalability, reliability, accessibility will be similar to the high requirements existing in all PCSs services today.

10.2.4 Force field analysis

Legal considerations:

When looking to transform a maritime trade business process using blockchain technology, one of the common concerns is if the process implemented with blockchain technology will be recognized by the legal authorities, mostly in the case of a dispute. One of Covid-19 impacts is that there is less resistance to blockchain solutions from government authorities.

Risk:

As part of the cargo release procedure, the technical solution must be reliable operating 24/7 to allow the maritime business to continue.

Other information:

When introducing digital solutions in international maritime trade, the focus to build the ecosystem to use the solution is as important as the technical solution.

A number of similar initiatives emerged and working on interoperability between the solutions is crucial for success.

Further information: International Port Community Systems Association (IPCSA)[45].

10.3 Franchised drugs and pharmaceutical equipment supply-chain management (China)

10.3.1 Categories

Transversal Category

- Public sector information and open data
- 3. Internet of Things

Horizontal Category

- 2. Data Provenance
- 5. Process Optimisation

Vertical Category

- M 7020 Management consultancy activities. (p. 57. ISIC Rev.4)

UN Sustainability Goals

- GOAL 3: Good Health and Well-being
- GOAL 11. Industry, innovation and infrastructure
- GOAL 12: Responsible Consumption and Production

Status

4, in trial or pilot

10.3.2 Summary

Long description

The Bo'ao District traceability and supervision platform for franchised drugs and pharmaceutical equipment supply-chain management was developed with a distributed architecture called Saca EchoTrust which is developed based on Fabric, incorporating foundational or enabling technologies: blockchain and IoT, e- signature, GIS (Geographic Information System) and visualization tools.

The technological enablers of blockchain, IOT and GIS facilitate near real-time traceability and monitoring of the drugs and pharma-equipment from source, logistics, storage and usage to prevent the illegal trading and use of the franchised drugs and pharmaceutical equipment. All critical data flowing through the whole process is securely stored, and is tamper-resistant in permanent, immutable blockchain data storage.

GIS technology is applied to gather on-chain data from different nodes and managed in a unified data standard and traceability coding system to realize the effective supervision of data integrity, tracking alerts and location IDs.

The purpose-built visualized-artefacts management system is used to provide unified information management for key data points and information (e-signature for e-approval, IOT real-time data collection and GIS for geographical data collection).

Business problem or opportunity

Underpin product provenance and authenticity, using E-approval, GIS technology with effective supervision of data immutability and integrity in the management system for franchised drugs and pharmaceutical Equipment.

Contribute in healthcare and scientific research with abundant access to medical data regarding reaction when patients used the drugs and pharmaceutical equipment which can be shared in government and medical institutes to ensure people's health.

Scope

This use case is specially designed for Bo'ao District. The blockchain can be used in healthcare industry. However, it can be promoted widely in primary industry, secondary industry and tertiary industries where data-trace systems are of benefit.

Data trace system aligns with laws and regulations on drugs and pharmaceutical equipment, e.g. State Drug Administration Law, Regulations on the Supervision and Administration of Medical Devices, Supervision and Administration of Inspection of Imported Medical Devices, Personal Information Protection Laws.

Objective

Whole supply chain management and supervision: applying, approving (online, e-approvals), purchasing, customs clearance, transportation (GIS technology) and storage of the pharmaceutical equipment. Pharma data on supply chain is immutable.

Stakeholders

Customs, Provincial sanitary planning commission, Provincial food and drug administration, State food and drug administration, Bonded Warehouse, Provincial government, Medical institutions, Pharmaceutical manufacturer, Transportation companies and Patient.

Predicted outcomes

Functional requirements including e-approval, GIS and immutable on-chain data storage.

Why distributed ledger technology?

Blockchain technology is the technology maintained by multiple stakeholders, using cryptography to ensure data transferred and accessing safety. Stakeholders share data according to mutual agreement. This technology can effectively counteract opportunities for fraud by automating data entry and location and provenance reporting. In supply chain management common threat vectors include data manipulation at entry and later in product lifecycle which in turn allow opportunities for counterfeiting and fraud. This system, designed as it is with multiple stakeholders, offers efficiencies to lower costs, improves data sharing effectiveness and heightens system security as it is baked-in from the outset, not bolted-on to legacy systems to facilitate integration.

10.3.3 User requirements

Functional requirements

- Medical institutions: to give the patients proper treatment plan, if imported drugs and pharmaceutical equipment are needed. Apply for the imported application on the system; use the received drugs and equipment according to the treatment plan; monitor patients' reaction;
- State or Provincial drug administration: Approve the application and monitor manage the whole process.
- Medical agent: purchase imported drugs and equipment after approval;
- Customs: manage and monitor importation and exportation.
- Bonded warehouse: To storage drugs and equipment when needed;
- Logistics: transportation for the imported drugs and equipment.

Visualizations: Figures 80 to 84

- **Reference architecture**

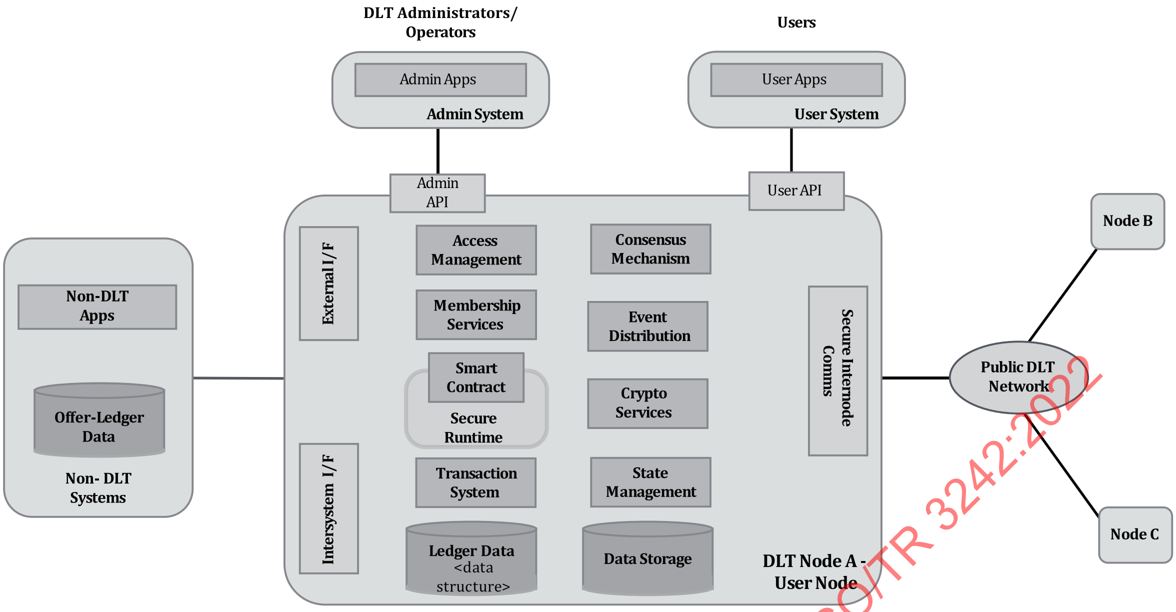


Figure 80 — Systems view architecture: Franchised pharma supply chain management (China)

— **Data flow model**

Data flow analysis – data categories data

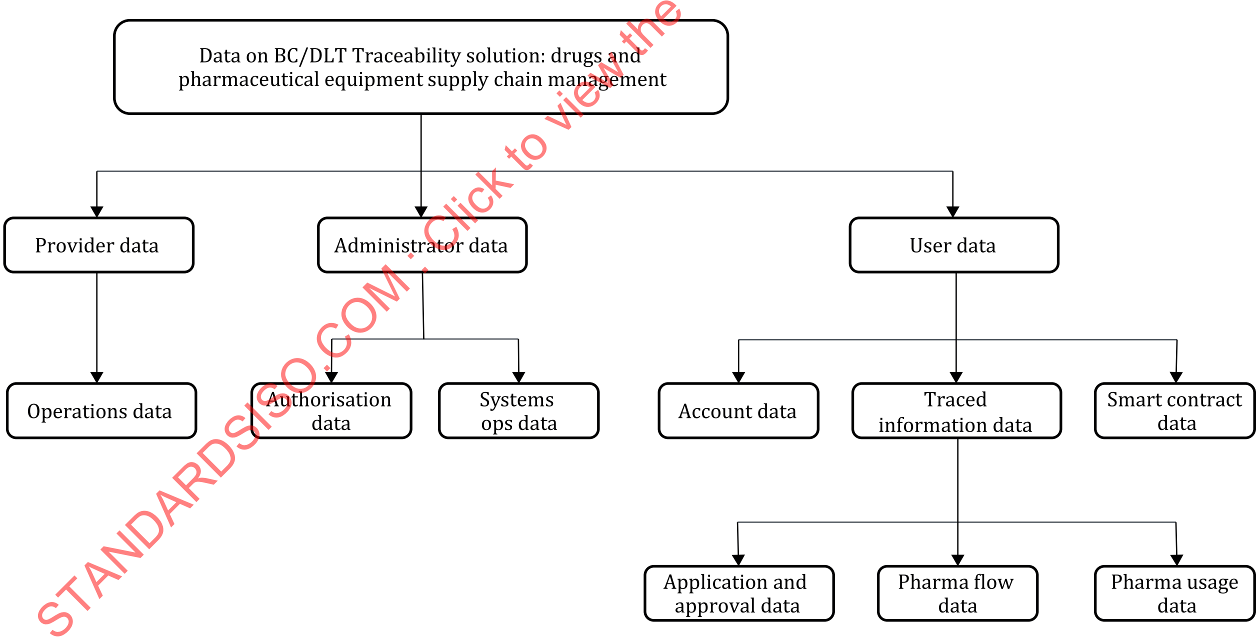


Figure 81 — Data flow and stakeholder roles: Franchised pharma supply chain management (China)

Data flow analysis

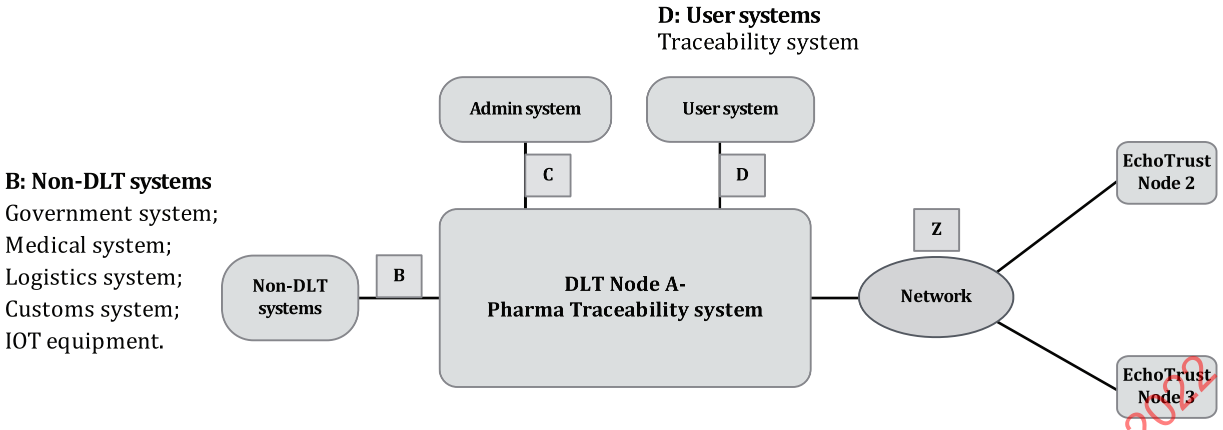


Figure 82 — Data flow analysis: Franchised pharma supply chain management (China)

— **Behavioural UML**

Use case diagram and sequence diagram

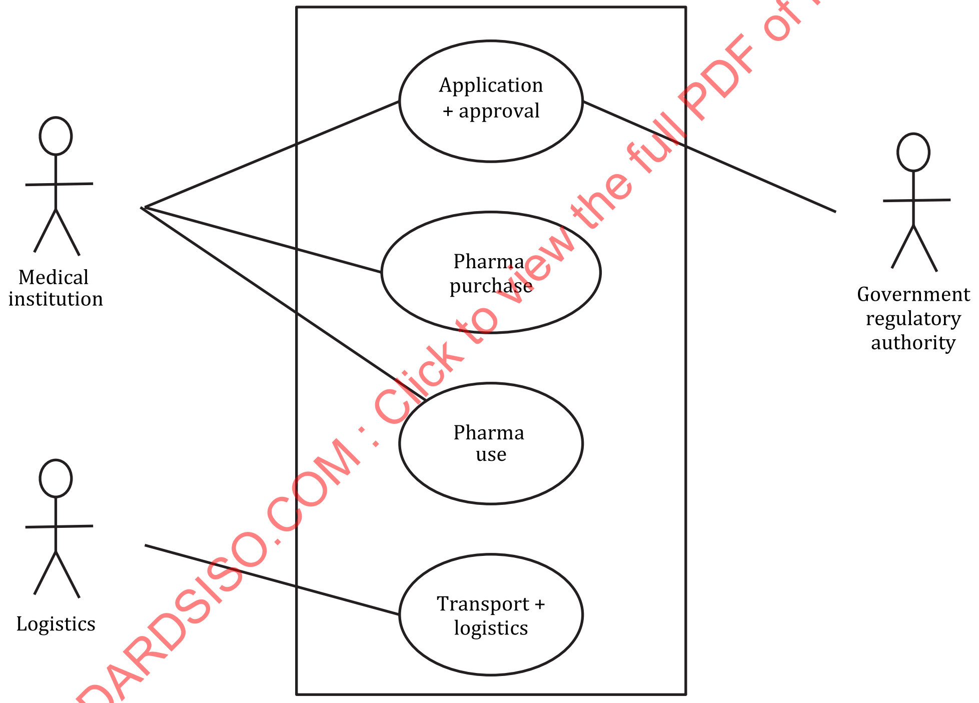


Figure 83 — Use case diagram: Franchised pharma supply chain management (China)

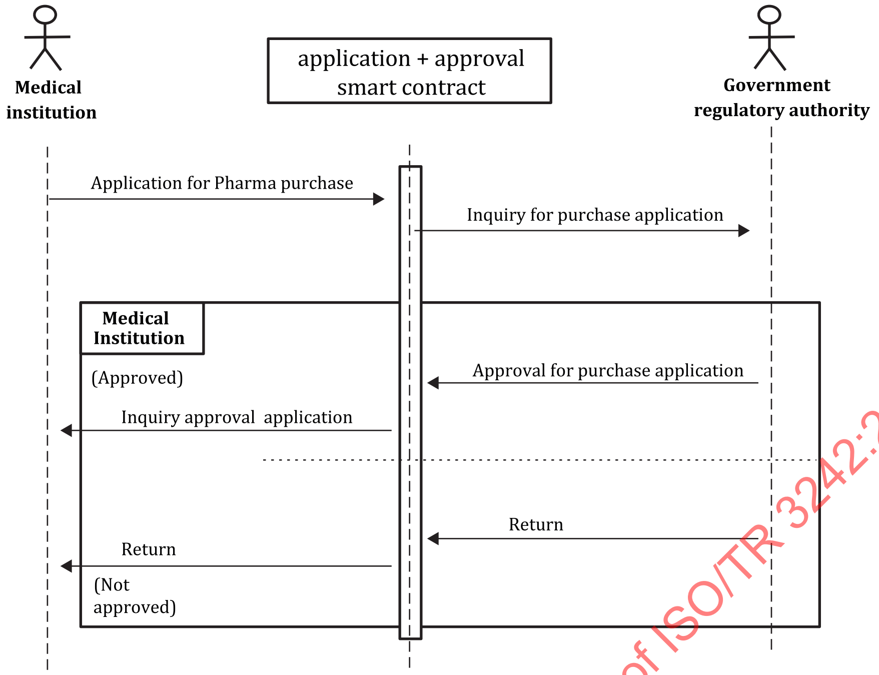

Medical institution
application + approval smart contract
Government regulatory authority
Application for Pharma purchase
Inquiry for purchase application
Medical Institution
(Approved)
Approval for purchase application
Inquiry approval application
Return
Return
(Not approved)

Figure 84 — Sequence diagram: Franchised pharma supply chain management (China)

Security, privacy and identity management:

This solution is secured by:

- electronic signature
- anti-counterfeiting of electronic approvals
- simultaneous distribution of electronic approvals

Coding standard based on the combination of international GS1 standard and China's coding standard, including Unique coding system standard, Significant Product Tracing code, the State Pharma electricity Monitoring code, and the Committee's Pharma coding rules.

Pre and post conditions:

- Pre-condition: The connectivity of IOT and internet is stable to ensure tracing data are updated in real-time.
- Post-condition: Data traceability are recorded on blockchain.

Non-functional requirements:

- Performance - the page responds in 1 second.
- Usability - Blockchain systems are user-friendly for all stakeholders to use.
- Scalability - if needed, significant nodes such as government stakeholders will be added in networks, while non-significant nodes will only be deployed for user end.

10.3.4 Force field analysis

Legal considerations:

Data trace system aligns with laws and regulations on drugs and pharmaceutical equipment, e.g. State Drug Administration Law, Regulations on the Supervision and Administration of Medical Devices, Supervision and Administration of Inspection of Imported Medical Devices, Personal Information Protection Laws.

Risk:

With both blockchain technology and IOT technology, imported Drugs and pharmaceutical Equipment authenticity can be ensured and traced. However, counterfeiting Drugs and Pharmaceutical Equipment can bring huge profits, data authenticity still has inherent risks. To manage this risk, BC/DLT Traceability Solution of Drugs and Pharmaceutical Equipment Supply-chain Management has clear approval and manage parties, to record videos with multiple people to ensure data authenticity, to mitigate the risk.

Other information:

Further information: Neusoft Cloud Technology Co., Ltd[46].

10.4 Anti-counterfeit solution for pharma industry (India)

10.4.1 Categories

Transversal Category:

- 1. Cloud computing
- 2. Public sector information and open data
- 3. Internet of Things
- 5. Electronic identification, trust services, e-signatures

Horizontal Category

- 1. Identity Management
- 2. Data Provenance
- 5. Process Optimisation
- 6. Automation

Vertical Category

- ISIC Section, division, group and class = M 7020
- Management consultancy activities. (p. 57. ISIC Rev.4)

UN Sustainability Goals

- GOAL 3: Good Health and Well-being
- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 12: Responsible Consumption and Production

Status

List text. 4, in trial or pilot

10.4.2 Summary

Long description

The platform offers 4 components:

- Mobile application or SDK: used by anyone to scan a medicine to check authenticity and provenance. It leverages the anomaly detection capabilities of the underlying platform. SDK allows integration with the platform. Alternately, users can utilize scanning/reading applications able to scan and decode data carriers (e.g. barcodes) which are in accordant with GS1 Standards.
- In-pharmacy POS Scanner: convenient for the user to scan and learn about product authenticity. Additional integration with the pharmacy billing system ensures that only validated medicines are billed.
- RealMeds platform: offers all the features related to track & trace and anti- counterfeiting and offers easy APIs for integration with any existing drug manufacturing or label printing workflow. Its real-time events can be used to receive real-time notifications when a counterfeit drug was detected. The platform applies an elaborate and extensible counterfeit detection, including, checking the DCA (Drug Control Administration) databases (e.g. NSQ, Banned Drugs)
- Dashboard: offers dashboard for public, government drug control authorities, and
- manufacturers/brand owners. The dashboard provides insight into the user specific KPIs such as heatmap of counterfeit events origin, what medicines are sold where, who are the top manufacturers/medicines fake industry is targeting, etc.

Business problem or opportunity

The pharmaceutical supply chain is, digitally, very fragmented, which creates a gap that is leveraged to introduce fake drugs. New business models - e.g. online pharmacies (aggregators) require advanced digital compliance to facilitate automated product verification and end-to-end traceability.

Scope

The objective of the platform is to provide end-to-end track & traceability with elaborate anti-counterfeiting checks to ensure that medicines are authentic and are safety compliant throughout the whole product lifecycle. The platform can also be used at point of administering and at POS in-store/online.

Objective

For all the medicines being tracked on RealMeds, the platform ensures single ownership at any instance and no one can inject a fake/duplicate record for a product item on the network.

Stakeholders

Patients, caregivers, pharma: retailers, logistics and manufacturers.

Predicted outcomes

A reduction in drug counterfeiting where medicines are tracked, and ownership transfer is carried out on the platform.

Why distributed ledger technology?

Enhanced data security with DLTs in-built data encryption and anonymity. Immutable transaction log of scanned history so that anyone seeing the provenance data can trust the system because they know that no one can change the ledger data.

With high data protection support and trustful nature, it is easier for the drug manufacturers to extend the counterfeit check by storing their spectroscopy fingerprint data. This will ensure that substandard drugs are detected more efficiently.

Distributed nature of the ledger allows a single view of the underlying data with fine-grained ACLs. This makes data sharing very efficient and simplifies the application architecture.

This reduces the cost of ownership, significantly. With RealMeds as a hosted cloud platform with simple APIs, it is within the reach of all size manufacturers. Every manufacturer can join the network and protect their brand from counterfeiting.

10.4.3 User requirements

Functional requirements

A manufacturer or its system requests a serial number be issued by RealMeds and encoded into a GS1 accordant data carrier, such as GS1 QR Code or GS1 DataMatrix, to be used in the manufacturer's primary, secondary or tertiary packaging.

- In the case of an anti-cancer medicine that is packaged in a bottle and the manufacturer requests a label from RealMeds for its secondary packaging.
- The label is then printed on the package using a GS1 compliant printer.
- The manufacturer scans the code on the label and initiates the tracking and traceability of the medicine.
- Depending upon the tracking requirement, the manufacturer can also keep a RealMeds location tracker inside the package.
- As the medicine moves in the supply chain, the tracker continuously feeds the temperature, humidity and location data to the platform, which keeps track of it to ensure that the medicine is invalidated if any of these parameters invalidate the rules configured in the platform, e.g. if a medicine is supposed to be within 2 degrees centigrade to 8 degrees centigrade but during the shipment it had stayed beyond 8 degrees for a certain time, the platform will invalidate that medicine so that it cannot be purchased/administered.
- The medicine, finally, reaches a pharmacy shop where a consumer comes to purchase it.
- The consumer can scan and validate the medicine using the POS scanner, before purchase, and depending on the result, can choose to purchase the medicine.

Visualizations: Figures 85 to 89

- **Reference architecture**

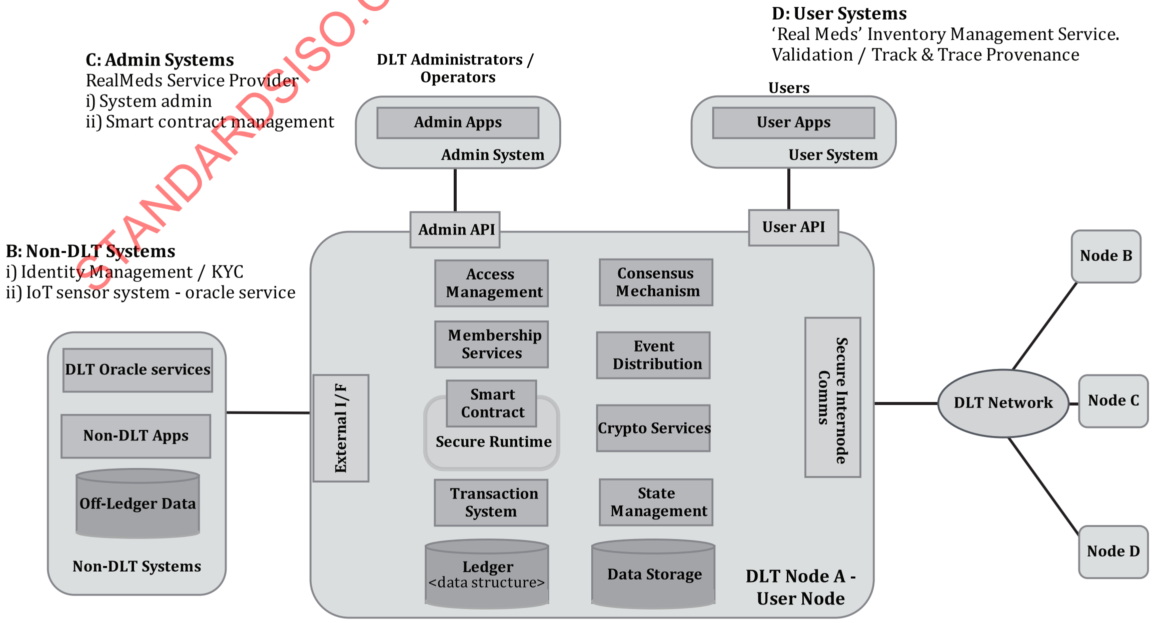


Figure 85 — Systems view architecture: Anti-counterfeit solution for pharma industry (India)

— Data flow model

Data flow analysis

Data flows triggered by the data-related operations of each stakeholder:

i) Specify the role of each stakeholder in facilitating the data flow: **Patient, Caregiver, Manufacturer, Supply chain participants, Drug control authority, Service Provider (RealMeds).**
ii) Identify the type of data flow (See categories A-Z below)

A: between 2 separate DLT systems when they interoperate
B: between a DLT system and non-DLT systems connected to it
C: between administration applications and a DLT system
D: between user applications and a DLT system
Z: within and between the nodes of the DLT system

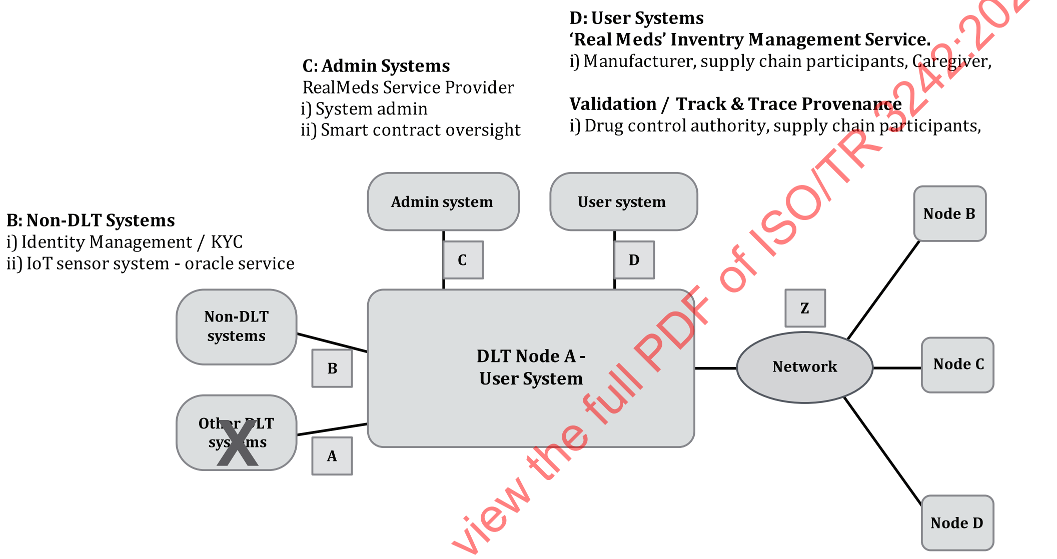

D: User Systems
'Real Meds' Inventry Management Service.
i) Manufacturer, supply chain participants, Caregiver,
Validation / Track & Trace Provenance
i) Drug control authority, supply chain participants,
C: Admin Systems
RealMeds Service Provider
i) System admin
ii) Smart contract oversight
B: Non-DLT Systems
i) Identity Management / KYC
ii) IoT sensor system - oracle service
Admin system
User system
C
D
Node B
Non-DLT systems
Z
B
DLT Node A - User System
Network
Node C
Other DLT systems
X
A
Node D

Figure 86 — Data flow analysis: Anti-counterfeit solution for pharma industry (India)

Data flow and interaction analysis

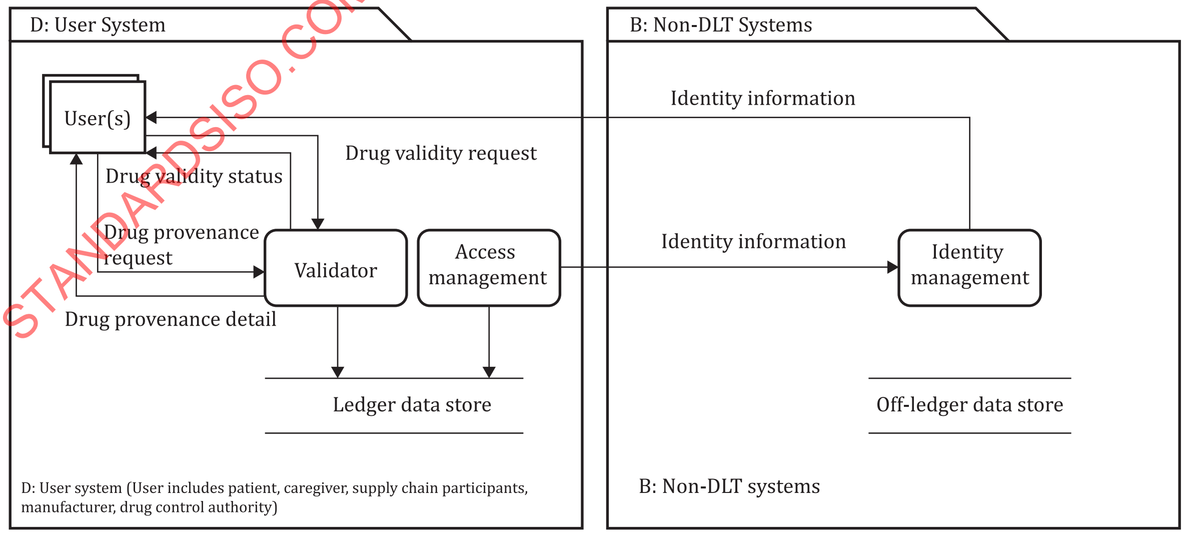


Figure 87 — Interaction diagram: Anti-counterfeit solution for pharma industry (India)

— Behavioural UML

Use case diagram

Track and traceability anti-counterfeit solution for pharma industry

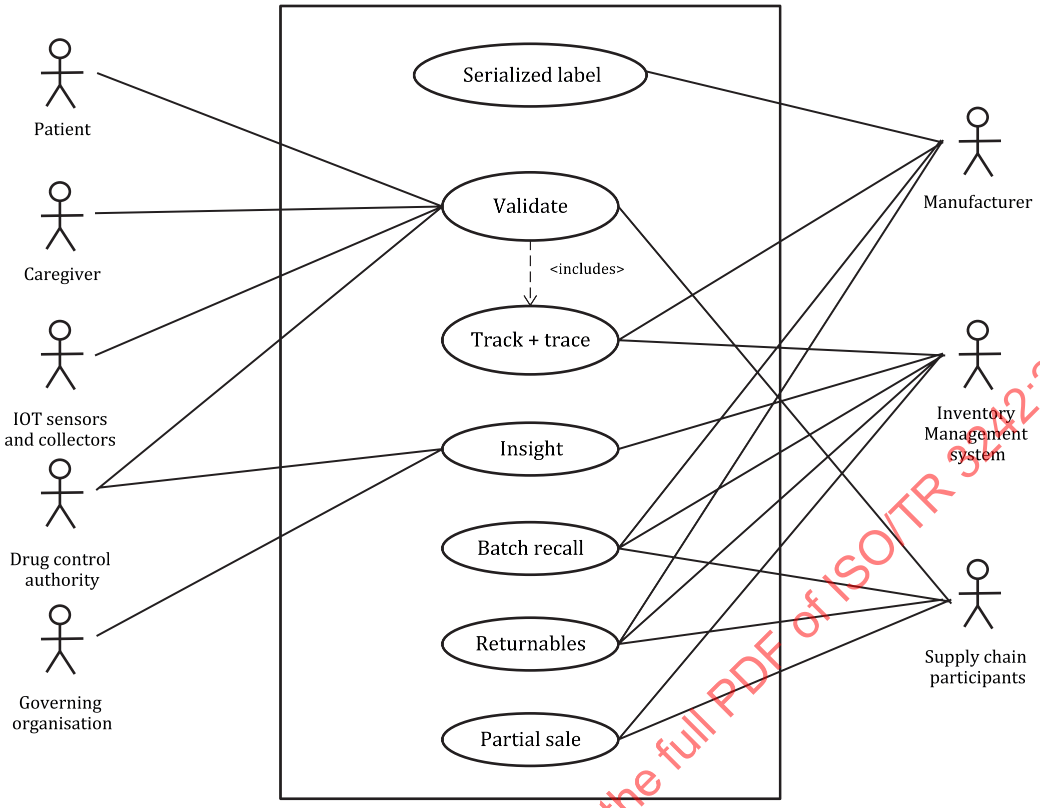


Figure 88 — Use case diagram: Anti-counterfeit solution for pharma industry (India)

Sequence diagram

Mobile App Access Use Case Diagram: Track and traceability anti-counterfeit solution for pharma industry

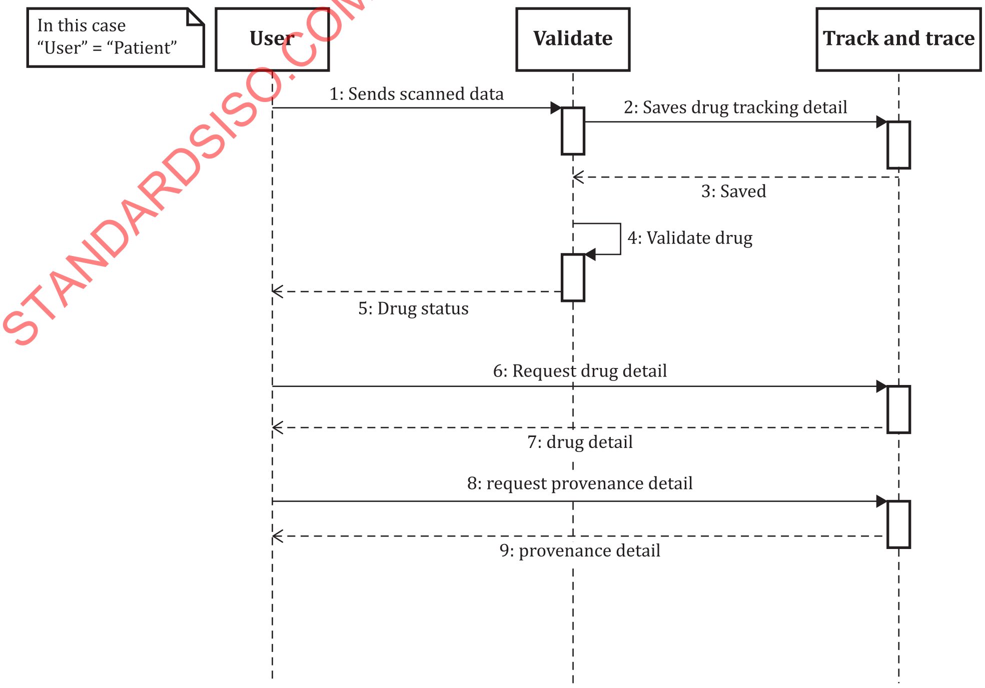


Figure 89 — Sequence diagram: Anti-counterfeit solution for pharma industry (India)

Smart contracts:

Platform uses smart contracts to:

- Validate a participant.
- Validate a label data read by a scanner or a mobile application for its compliance with configured label formats - e.g. GS1 complaint.
- Ensure that the temperature, humidity and location data is received from authorised devices and sensors.
- Validate medicine parameters, temperature, humidity and location data against configured rules - e.g. expiry date, allowed temperature threshold, geo-fencing, etc.
- Ensure the single ownership of a medicine.
- Additionally, validate the composition of a medicine by referring to its spectroscopy fingerprinting.

Security, privacy and identity management:

Permissioned Blockchain network.

Only registered medicines are tracked, and only registered participants can be part of the network. This ensures that the system is protected from unauthorized participants. However, anyone can scan and validate a medicine on the network. All transactions and data are protected using the user permissions and ACLs (access control list).

The platform leverages the Blockchain security to store data and transactions.

- Every data exchange between all the systems (as shown in the data flow diagram) is encrypted.
- KYC (Know Your Customer) mechanism is followed to ensure the registration of right participant on the network.

All transactions on the network can be linked to a user. However, no personally identifiable data is stored on the network. This makes it easier to comply with country specific data policies e.g. GDPR.

Pre and post conditions:

Pre -conditions:

- Manufacturers identify the physical items they intend to track in the supply chain with unique serial numbers.
- The manufacturer utilizes printing and verification systems for data carrier symbols accordant to GS1 Standard
- The manufacturer's label generating system is integrated with RealMeds API
- Every participant has RealMeds or scanning/reading applications able to scan and decode data carriers (e.g. barcodes) which are accordant with GS1 Standards to scan a medicine
- For live tracking of Temperature, Humidity and Location, the monitoring device is registered with RealMeds Blockchain to avoid security issues.

Post-conditions

- Interactive supply chain: notification of events of interest - e.g. someone seeking to purchase/administer an expired medicine - can be notified in real-time.

Non-functional requirements:

Interoperability is a key feature of the system. It will drive adoption and acceptance. The requirement for interoperability can add complexity, which could be solved with the unified view of system data afforded by the distributed node-based DLT network.

Following standards is the basis for interoperability. All the labels are generated as per GS1 standard. Data exchange between different systems is facilitated using EPCIS standard and API interfaces use REST/JSON to enable integrations. Support for additional interfaces, such as SOAP/XML, cXML, etc. exist for integration with legacy systems.

10.4.4 Force field analysis

Legal considerations:

GS1 - a global supply chain standard GDPR - data privacy laws apply within EU

Compliance with pharmaceutical industry-related regulations

Risk:

Business Risk: Need to address manufactures' concerns about their data privacy and security objectively by repeated demonstration to build confidence in them, so that they are open to store the composition data for identification of substandard drugs. Need of manufacturers to understand the benefit to their quality checks and thus they can avoid various legal, regulatory and operational issues later.

Referenced standards:

Following major standards & guidelines were used to build the platform:

ISO/IEC 19987[47]

ISO/IEC 19988[48]

DGFT DAVA Guidelines & Schema - Government of India[49]

GS1 Global Traceability Standard - Release 2.0[50]

EPC Information Services (EPCIS) - Version 1.1 - GS1 Standard[51]

21 CFR Part 11 - FDA - Pharmaceutical CGMPs[52]

AIDC Healthcare Implementation Guideline - Release 3.0.1 - GS1[53]

GS1 Logistic Label Guideline - Release 1.3[20]

Other information:

Further information: RealMeds - Blockchain, AI and IoT based comprehensive track & traceability and anti-counterfeiting PaaS for drugs. Pharmaceuticals Counterfeiting[54].

10.5 IGP provenance traceability (Italy)

10.5.1 Categories

Transversal Category

- 1. Cloud computing
- 2. Public sector information and open data
- 3. Internet of Things
- 5. Electronic identification, trust services, e-signatures

- 6. e-Privacy

Horizontal Category

- 2. Data Provenance
- 3. Governance and DAOs
- 5. Process Optimisation

Vertical Category

- Classification: A-0123
- Section A - Agriculture, forestry and fishing
- Division 01 - Crop and animal production, hunting and related service activities
- Group 012 - Growing of perennial crops
- Class 0123 - Growing of citrus fruits

UN Sustainability Goals

- GOAL 9: Industry, Innovation and Infrastructure
- GOAL 17: Partnerships to achieve the Goal

Status

- 5. in production/live implementation

10.5.2 Summary

Long description

Italy is the top producer in Europe of products with 'denomination of origin' certification. In recent years, the trade in counterfeit products has grown exponentially and represents a significant threat to economic growth, undermining the implementation of good management practices and diminishing the authenticity of 'Made in Italy' products on the foreign market.

The Red Orange Upgrading Green Economy (ROUGE) makes it possible to guarantee fruit of excellence thanks to a technological label that tells the origin, identity and characteristics of the product.

ROUGE was conceived by AlmavivA with the Consorzio IGP Arancia Rossa with a vision to offer product and consumer protection services to member companies.

ROUGE runs on the top of the blockchain architecture. The solution ensures that maximum value is extracted from even heterogeneous blockchain ecosystems by establishing interoperability and communication criteria.

Business problem or opportunity

- Creating an organized and efficient ecosystem along the Supply Chain, from farmers to consumers.
- Protecting, valorisating and promoting true Made in Italy products all over the world.
- Enabling an end-to-end supply chain traceability in the food sector which implies robust transparency and security to all kind of actors involved within it.

Scope

ROUGE is a national and international product, it can be applied in the Food Supply Chain Sector. Italian law no.12/19 dated 11 January 2019 (the "Law") came into force on 13 February 2019 and cemented the legal enforceability of electronic timestamping performed through blockchain technologies.

As part of a national reform pertaining to the simplification of administrative formalities for companies, the Law explicitly states in its Article 8 ter, 3° that "storage of a computerized document through the use of technologies passed on distributed ledger creates the same legal effect as 'electronic time stamp'", as defined in the European Regulation no. 910/2014 on electronic identification and trust services for electronic transactions dated 23 July 2014 ("eIDAS").

Objectives

Improve food safety and transparency, consumer trust, Data Quality & Trusted Data Governance, mitigate recall costs and impacts.

Increasing communication through the Supply Chain allowing partners to share joint goals and feedback to improve more chances of success and build trust.

Establishing timelines and mechanisms for transferring updates on progress, holding accountability when progress is lacking.

Stakeholders

- ROUGE was conceived by AlmavivA with the Consorzio IGP Arancia Rossa with a vision to offer product and consumer protection services to member companies. The project brings together four important entities:
- CREA, the research centre that collects food production data; University of Catania that creates economic models with respect to the data collected in the field to support production decisions;
- Consorzio IGP Arancia Rossa that, thanks to these tools, can verify the origin of products and trace their path; AlmavivA as a technological partner.

Key Actors:

- Farmers
- Retailers
- Distributors
- Consumers
- Agricultural Service Providers
- Governments

Predicted outcomes

Tracing a production chain for the German market with the initial participation of at least 4 producers from the Consorzio Arancia Rossa IGP di Sicilia, 1 processing company, 1 distribution company, a certification entity and a large-scale retail trade.

The ROUGE project chain is further extended through the commercial agreement between Arance Rosse IGP, Beske China and Adm-EA Consulting to seize opportunities on global markets.

Why distributed ledger technology?

Blockchain promotes transparency and helps streamline the process of sharing information: each actor provides data and real-time updates about products and views the same set of data on a product's lifecycle, improving transparency, accountability and trust.

This provides confidence that the data has not been tampered with or altered inappropriately and allows also a more direct visibility on whether contracts and agreements are adhered to and properly documented.

Blockchain enables interoperability between the various traceability solutions without the need to replace the applications or moving onto a single solution for all entities on the supply chain. This is very important when there are multiple entities, partners, locations, and facilities on a supply chain that do not need or want to directly integrate with each other or be impacted by another entity's technology and/or business decisions.

The ROUGE system facilitates a better production control, avoiding under or overproduction. Suppliers can build a better delivery time for their store, customer satisfaction is improved and retailers can engage customers by providing access to specific information.

10.5.3 User requirements

Functional requirements

All actors actively involved in entering supply chain data are subject to:

- Being registered within the ecosystem.
- Inserting the data of interest in compliance with the specifications drawn up by the protection consortium.
- Ensuring that each individual product has a unique identifier (UID) and is equipped with NFC or QR CODE tags.
- Creating a supply chain history through which the final consumer will have the possibility to verify the traceability of the purchased product.

Visualizations: Figures 90-94

- **Reference architecture**

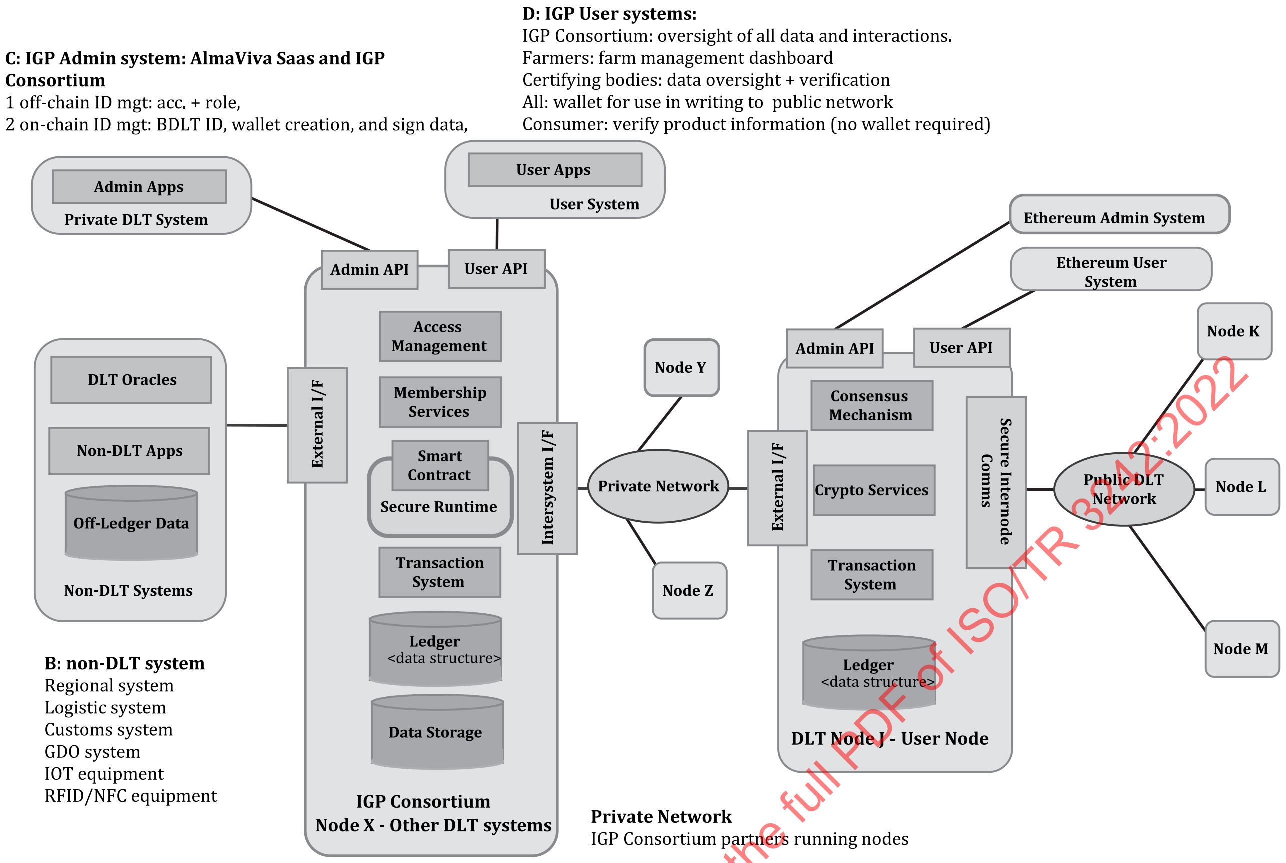


Figure 90 — Systems view architecture: IGP provenance traceability (Italy)

- **Data flow model**

Data flow Analysis

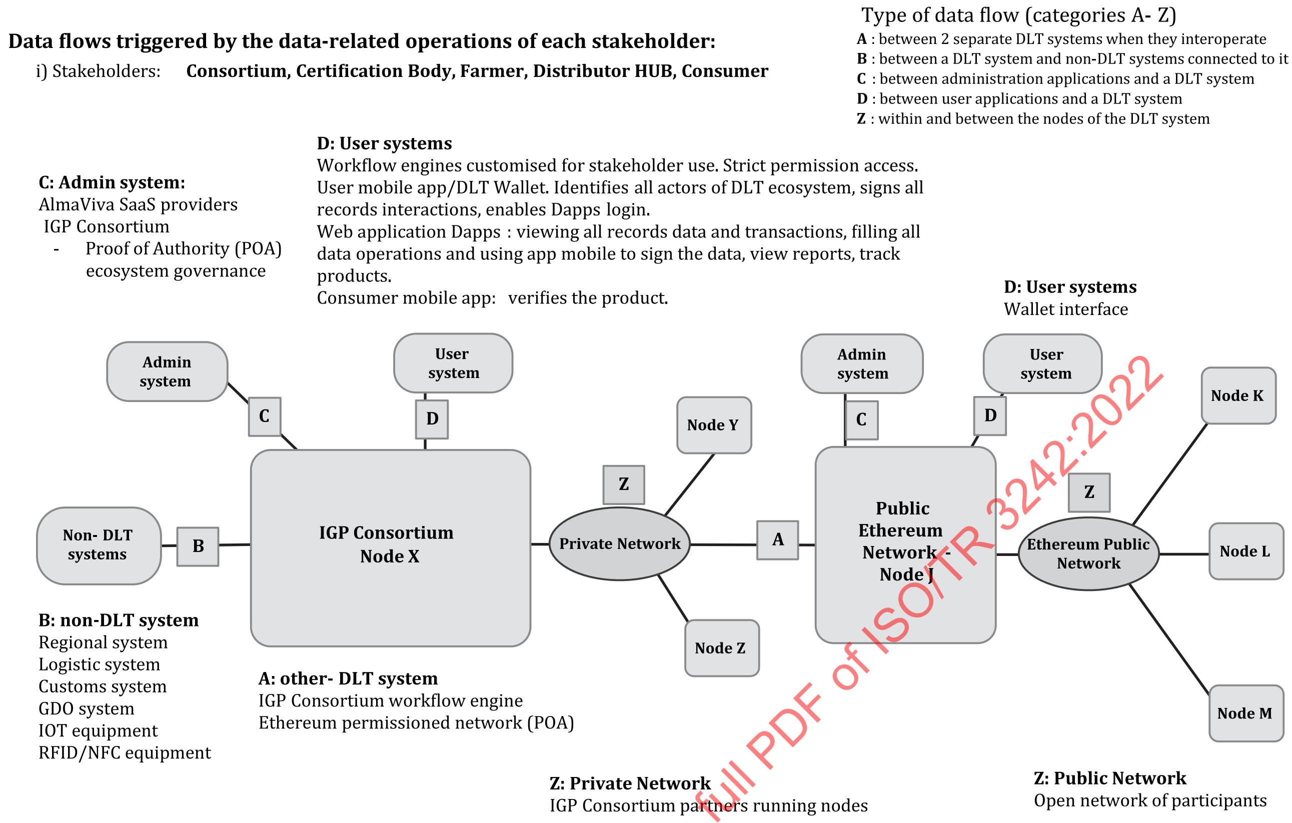
The blockchain solution is based on the interaction between the Consortium's portal, which shows data from the various production sources, and an App that provides information thanks to a geolocation system integrated with the Tag label affixed on the boxes of oranges.

Through this TAG/NFC, the App allows monitoring of the: production field, date of harvest, storage and distribution methods.

The hi-tech label connected to the blockchain system guarantees the certain recognition of the data, based on information from the public administration and companies linked to the Consortium, and the correct link with the certified and unchangeable history of the product.

The solution has been implemented using Ethereum and Ethereum Mainnet with all the benefits of a private network combined to the reliability of a public one. It enables the participation of both 'private' nodes (other private companies or consortia) and 'public' nodes.

A Stack MEAN (MongoDB, Angular, Express, NodeJS) has been used for the delivery of web applications, all components use Open Source code.



Data flows triggered by the data-related operations of each stakeholder:

i) Stakeholders: **Consortium, Certification Body, Farmer, Distributor HUB, Consumer**

Type of data flow (categories A- Z)

A : between 2 separate DLT systems when they interoperate
B : between a DLT system and non-DLT systems connected to it
C : between administration applications and a DLT system
D : between user applications and a DLT system
Z : within and between the nodes of the DLT system

C: Admin system:
AlmaViva SaaS providers
IGP Consortium
- Proof of Authority (POA) ecosystem governance

D: User systems
Workflow engines customised for stakeholder use. Strict permission access.
User mobile app/DLT Wallet. Identifies all actors of DLT ecosystem, signs all records interactions, enables Dapps login.
Web application Dapps : viewing all records data and transactions, filling all data operations and using app mobile to sign the data, view reports, track products.
Consumer mobile app: verifies the product.

D: User systems
Wallet interface

B: non-DLT system
Regional system
Logistic system
Customs system
GDO system
IOT equipment
RFID/NFC equipment

A: other- DLT system
IGP Consortium workflow engine
Ethereum permissioned network (POA)

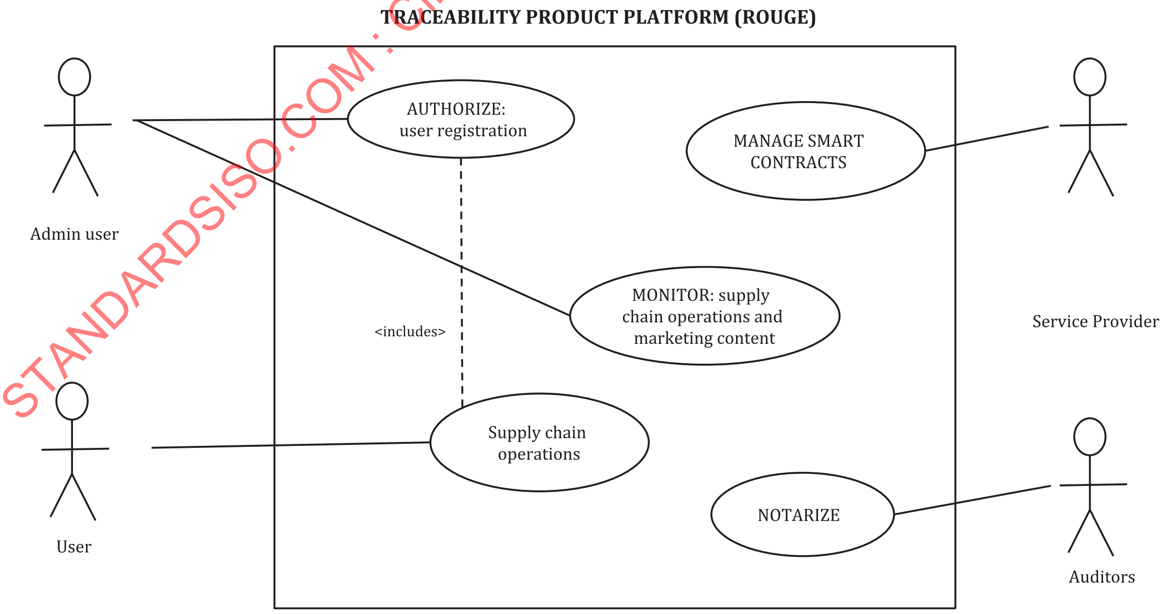
Z: Private Network
IGP Consortium partners running nodes

Z: Public Network
Open network of participants

Figure 91 — Data flow analysis: IGP provenance traceability (Italy)

— Behavioural UML

Use case diagram



TRACEABILITY PRODUCT PLATFORM (ROUGE)
Admin user
AUTHORIZE: user registration
MANAGE SMART CONTRACTS
MONITOR: supply chain operations and marketing content
<includes>
Supply chain operations
NOTARIZE
User
Service Provider
Auditors

Figure 92 — Use case diagram: IGP provenance traceability (Italy)

Interaction diagram

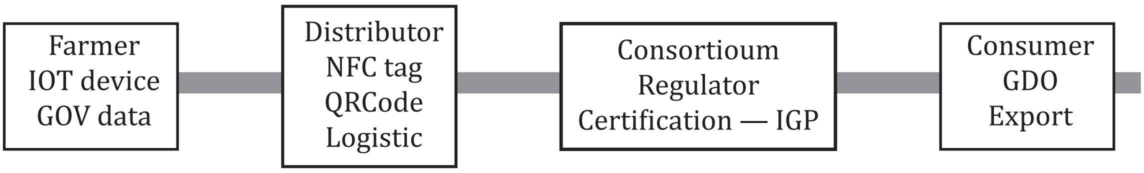


Figure 93 — Interaction diagram: IGP provenance traceability (Italy)

Sequence diagram

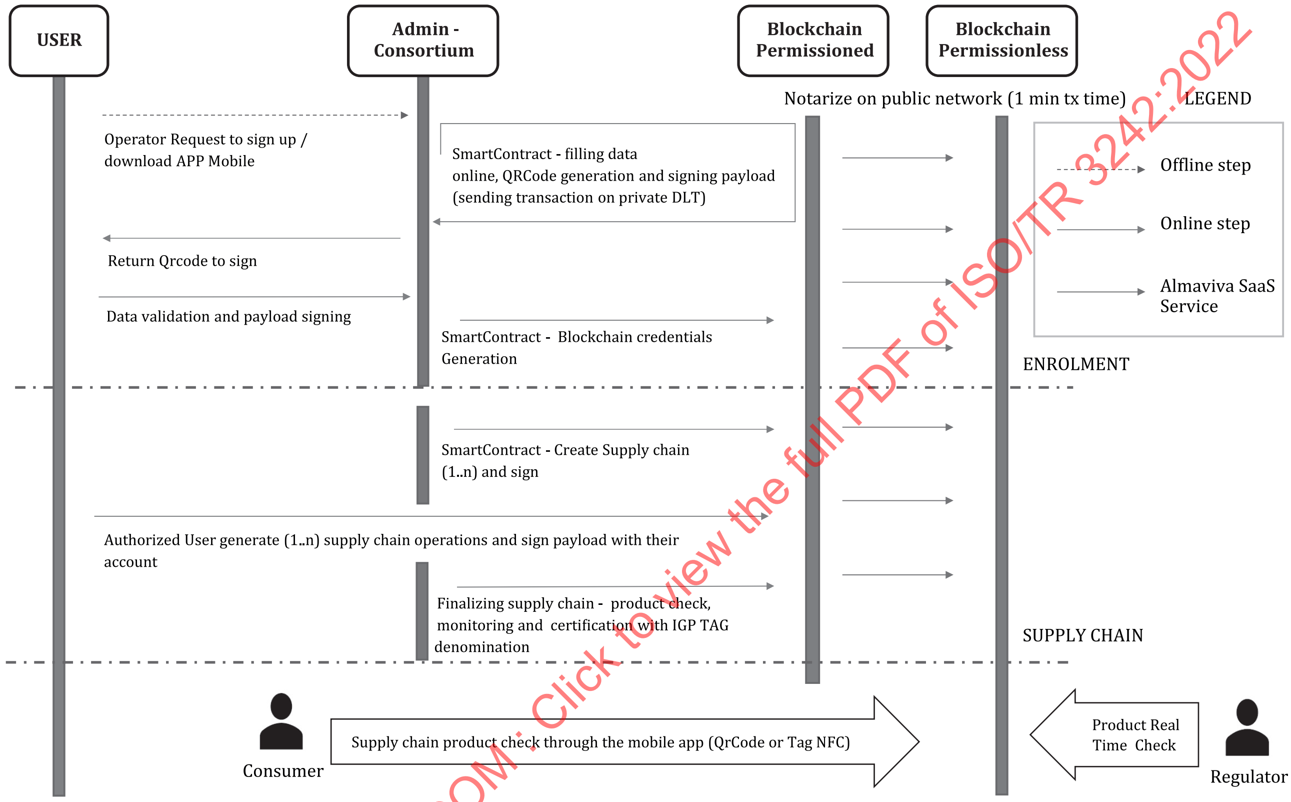

USER
Admin - Consortium
Blockchain Permissioned
Blockchain Permissionless
Notarize on public network (1 min tx time)
LEGEND
Offline step
Online step
Almaviva SaaS Service
Operator Request to sign up / download APP Mobile
SmartContract - filling data online, QRCode generation and signing payload (sending transaction on private DLT)
Return Qrcode to sign
Data validation and payload signing
SmartContract - Blockchain credentials Generation
ENROLMENT
SmartContract - Create Supply chain (1..n) and sign
Authorized User generate (1..n) supply chain operations and sign payload with their account
Finalizing supply chain - product check, monitoring and certification with IGP TAG denomination
SUPPLY CHAIN
Consumer
Supply chain product check through the mobile app (QrCode or Tag NFC)
Product Real Time Check
Regulator

Figure 94 — Sequence diagram: IGP provenance traceability (Italy)

Security, privacy and identity management:

Smart Contracts records the operations that every single actor in the supply chain enters and signs with its own wallet.

It also performs the census association of the actors with the release of a unique identity and configures for each actor a defined role to control the level of visibility it can have on the platform data.

Finally, it uniquely associates the NFC Tag transponder with a blockchain ID.

Pre and post conditions:

Identity management is guaranteed through the creation of a wallet for each actor, the private key is saved on the individual device of the actor and the privacy of the data is guaranteed by cryptography algorithms.

Non-functional requirements:

Pre-Requirement: The availability of the blockchain ecosystem of the Consorzio Arancia Rossa di Sicilia during the whole period of harvesting, production and marketing of the product.

10.5.4 Force field analysis

Legal considerations:

Italy was the first European country to recognize, within a decree "regulatory reference" at the legal level, DLT technology and smart contracts.

There are no particular legal risks from this point of view nor for privacy data as there is no disclosure of sensitive data.

The proposed solution also solved the legal aspect regarding cryptocurrency financial reporting and budgeting linked to the notarization of the status of the private blockchain network on the public blockchain, using the advice of experts and lawyers.

Risk:

No particular technical risks are expected as the ecosystem is completely open and any other DLT platform can be integrated.

A potential risk is the possibility that some actors do not want to participate in a traced supply chain with the exclusion of some members.

Other information:

Further information: Consorzio di Tutela Arancia Rossa di Sicilia IGP[12].

10.6 Universal Farm Compliance (Ireland)

10.6.1 Categories

Transversal Category

- 1. Cloud computing
- 2. Public sector information and open data
- 5. Electronic identification, trust services, e-signatures
- 8. Accessibility of ICT products and services

Horizontal Category

- 1. Identity Management
- 2. Data Provenance
- 5. Process Optimisation

Vertical Category

- Section O - Public Administration
- Division 84 - Public administration and defence; compulsory social security
- Group 841 - Administration of the State and the economic and social policy of the community Class 8413 - Regulation of and contribution to more efficient operation of businesses
- (p. 59, ISIC Rev. 4)

UN Sustainability Goals

- GOAL 9: Industry, Innovation and Infrastructure GOAL 11: Sustainable Cities and Communities GOAL 12: Responsible Consumption and Production GOAL 15: Life on Land

- GOAL 17: Partnerships to achieve the Goal

Status

3. in development or pre-production

10.6.2 Summary

Long description

Universal Farm Compliance facilitates a trusted, transparent, connected agriculture produced food compliance system enabled by EU blockchain infrastructure and supported by national public bodies.

- SaaS + mobile services to facilitate universal farm-compliance.
- leverage distributed technologies and decentralised governance frameworks to allow farmers ownership and publishing rights over their compliance data,
- facilitate public bodies to issue compliance + audit workflows for real-time farm reporting,
- certify + attest to valid compliance and share digital proofs-of-attainment to enhance data integrity and reputation,
- optimise and automate compliance workflows and,
- increase transparency and trust in the food value chain across the Single Digital Marketplace.

Business problem or opportunity

Incentivise and facilitate digitising farm data at source for farm management and compliance purposes. The approach saves time and money and has potential to introduce access to new revenue streams to farmers using the system.

Scope

This use case applies to the agriculture sector within the EU, bound by common regulatory environments.

E.g. Common Agricultural Policy 2020 with a marked focus on environmental targets: control of Nitrogen, GHG emissions and water management as well as a drive towards increasing food supply transparency.

It is enabled by infrastructure made available through Connecting Europe Facility (CEF) and EU Blockchain Service Infrastructure (EBSI v1.0 Infrastructure Specification)[56]

Objective

Create a channel for secure, real-time farm compliance reporting via mobile farm data collected by approved users on the fly.

Stakeholders

Farm compliance authorities, farmers, landowners, Department of Agriculture, agriculture produced food businesses.

Predicted outcomes

An empowering decentralised farmer-first data governance model that underpins a real-time farm compliance reporting framework.

Why distributed ledger technology?

Trust, provenance and process automation:

Leveraging infrastructure and resources available through Connecting Europe Facility (CEF) and EU Blockchain Service Infrastructure (EBSI v1.0 Infrastructure Specification) this use case aims to:

- redesign the interface between public sector and farming communities,
- to build new models of engagement that bring the benefits of emerging technologies to field data digitisation,
- address farm data ownership concerns and create efficiencies in farm compliance processes.

10.6.3 User requirements

Functional requirements

- Farm compliance authorities: set, monitor and certify opt-in compliance workflows for farmers;
- Farmers and landowners: digitise farm data at source and tag according to task- schedule and workflow;
- Dept. of Agriculture: Wide ranging farm ecosystem oversight for research and planning purposes;
- Agriculture produced food businesses: verify certification - enhancing food chain transparency.

Universal Farm Compliance requires the management of multiple digital identity within a single use case; with requirements to:

- identify registered farm operators,
- identify farm operative roles,
- identify farming tasks and task status,
- identify named workflows in order that a named individual can submit task completion reports, within named compliance workflows, to appropriate compliance authorities.

Visualizations: Figures 95 to 98

- **Reference architecture**

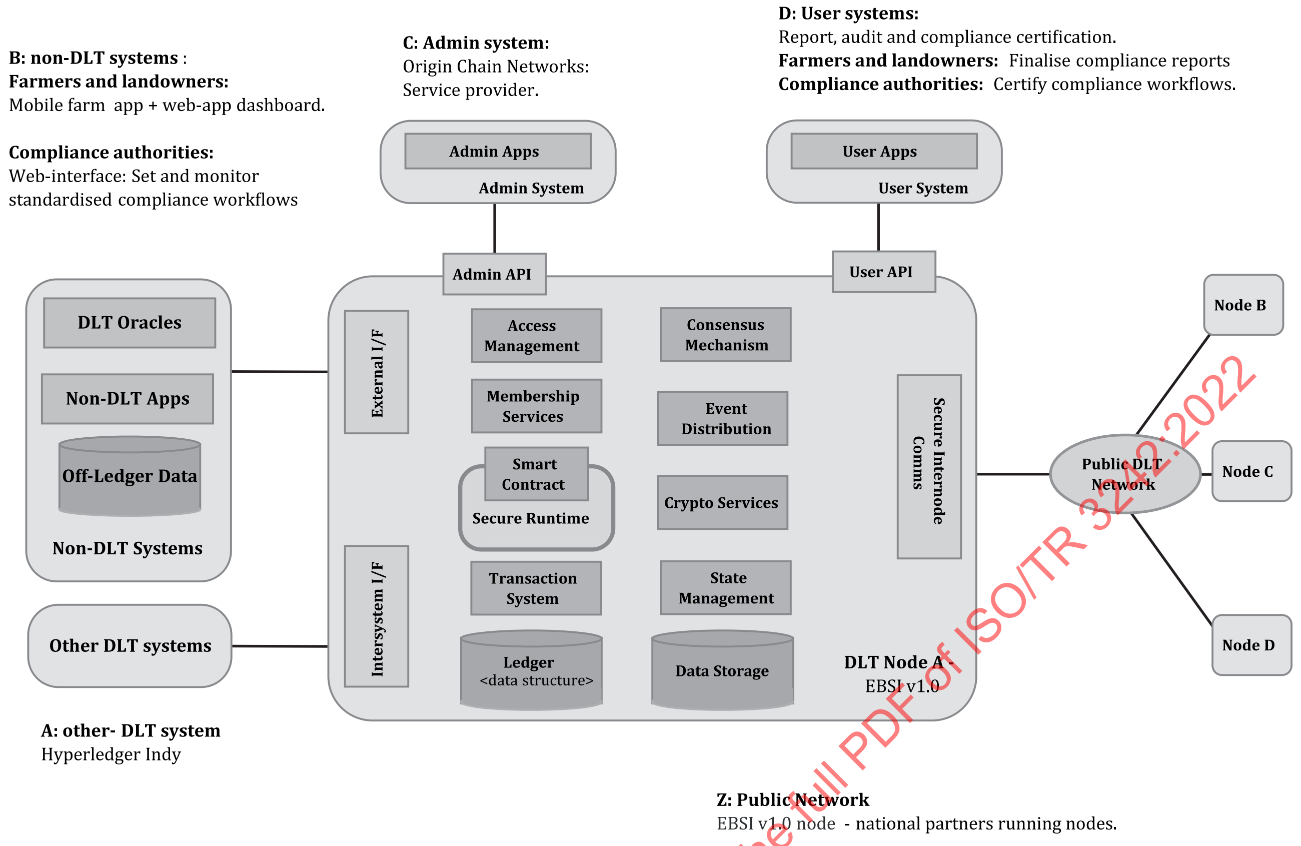


Figure 95 — Systems view architecture: Universal farm compliance (Ireland)

— Data flow model