
**Blockchain and distributed ledger
technologies – Use cases**

Copyright document for WG on Baseline security requirements
No reproduction or circulation



Copyright document for WG on Baseline security requirements
No reproduction or circulation



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Page

Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Use case processes	1
5 Template development	2
5.1 General	2
5.2 Functional Requirements	3
5.3 System architecture	3
5.4 Data Flows	4
5.5 Use Case Models	5
5.6 Categories	6
5.7 Category: Transversal	6
5.8 Category: Horizontal	7
5.9 Category: Vertical	7
5.10 Category: sustainable development goals	8
5.11 Category: status of use case	8
5.12 Category: Other use case classifications	9
6 Use case list and abstracts	10
6.1 Data Provenance	10
6.2 Fintech use cases	14
6.3 Supply Chain cases	18
6.4 Smart Energy use cases	22
7 Use case overview and insights by category	24
7.1 General	24
7.2 Insights - transversal categories	25
7.3 Insights - horizontal categories	26
7.4 Insights - vertical category	27
7.5 Insights - status	28
7.6 Sustainable development goals (SDGs)	29
7.7 Insights - blockchain implementation types	30
7.8 Insights - open source	31
8 Use cases: Data Provenance	32
8.1 Data Accountability (European Union)	32
8.1.1 Categories	32
8.1.2 Summary	33
8.1.3 User requirements	34
8.1.4 Force field analysis	39
8.2 Property Record Management System (PRMS) (India)	40
8.2.1 Categories	40
8.2.2 Summary	40
8.2.3 User requirements	43
8.2.4 Force field analysis	47
8.3 Student records management system (SRMS) India	47
8.3.1 Categories	47
8.3.2 Summary	48
8.3.3 User requirements	49
8.3.4 Force field analysis	53
8.4 Education certificates provenance (Singapore)	54
8.4.1 Categories	54

8.4.2	Summary	55
8.4.3	User requirements	57
8.4.4	Force field analysis	61
8.5	Content timestamp verification (Netherlands)	62
8.5.1	Categories	62
8.5.2	Summary	62
8.5.3	User requirements	64
8.5.4	Force field analysis	66
8.6	Self-sovereign ID (SSI) (Cyprus)	67
8.6.1	Categories	67
8.6.2	Summary	68
8.6.3	User requirements	70
8.6.4	Force field analysis	77
9	Use cases: Fintech	78
9.1	Accounts receivable financing system (China)	78
9.1.1	Categories	78
9.1.2	Summary	78
9.1.3	User requirements	80
9.1.4	Force field analysis	83
9.2	Interbank loan reconciliation and settlement (China)	83
9.2.1	Categories	83
9.2.2	Summary	84
9.2.3	User requirements	84
9.2.4	Force field analysis	87
9.3	Organized CHIT funds (India)	88
9.3.1	Categories	88
9.3.2	Summary	88
9.3.3	User requirements	90
9.3.4	Force field analysis	94
9.4	Transparent securitisation (Italy)	95
9.4.1	Categories	95
9.4.2	Summary	96
9.4.3	User requirements	97
9.4.4	Force field analysis	102
9.5	Pension process optimisation (China)	104
9.5.1	Categories	104
9.5.2	Summary	104
9.5.3	User requirements	105
9.5.4	Force field analysis	110
9.6	Decentralised Charity Platform (the Republic of Korea)	110
9.6.1	Categories	110
9.6.2	Summary	111
9.6.3	User requirements	113
9.6.4	Force field analysis	116
10	Use cases: Supply Chain	117
10.1	International trade transparency (Singapore)	117
10.1.1	Categories	117
10.1.2	Summary	118
10.1.3	User requirements	119
10.1.4	Force field analysis	123
10.2	Maritime Bill of Lading (Israel)	124
10.2.1	Categories	124
10.2.2	Summary	124
10.2.3	User requirements	126
10.2.4	Force field analysis	130
10.3	Franchised drugs and pharmaceutical equipment supply-chain management (China)	130

10.3.1	Categories	130
10.3.2	Summary	131
10.3.3	User requirements	132
10.3.4	Force field analysis	135
10.4	Anti-counterfeit solution for pharma industry (India)	136
10.4.1	Categories	136
10.4.2	Summary	136
10.4.3	User requirements	138
10.4.4	Force field analysis	142
10.5	IGP provenance traceability (Italy)	142
10.5.1	Categories	142
10.5.2	Summary	143
10.5.3	User requirements	145
10.5.4	Force field analysis	149
10.6	Universal Farm Compliance (Ireland)	149
10.6.1	Categories	149
10.6.2	Summary	150
10.6.3	User requirements	151
10.6.4	Force field analysis	156
10.7	International waste transportation management system (Netherlands)	156
10.7.1	Categories	156
10.7.2	Summary	157
10.7.3	User requirements	158
10.7.4	Force field analysis	164
11	Use cases: Smart Energy	165
11.1	Cooperative energy trading (Ireland)	165
11.1.1	Categories	165
11.1.2	Summary	165
11.1.3	User requirements	167
11.1.4	Force field analysis	170
11.2	Energy Trading with Transactive Energy Grids (India)	171
11.2.1	Categories	171
11.2.2	Summary	172
11.2.3	User requirements	173
11.2.4	Force field analysis	178
11.3	Renewable energy consumer grids (Spain)	178
11.3.1	Categories	178
11.3.2	Summary	179
11.3.3	User requirements	180
11.3.4	Force field analysis	184
	Annex A Use case exemplar	186
	Bibliography	188

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.

Copyright document for WG on Baseline security requirements
No reproduction or circulation

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.

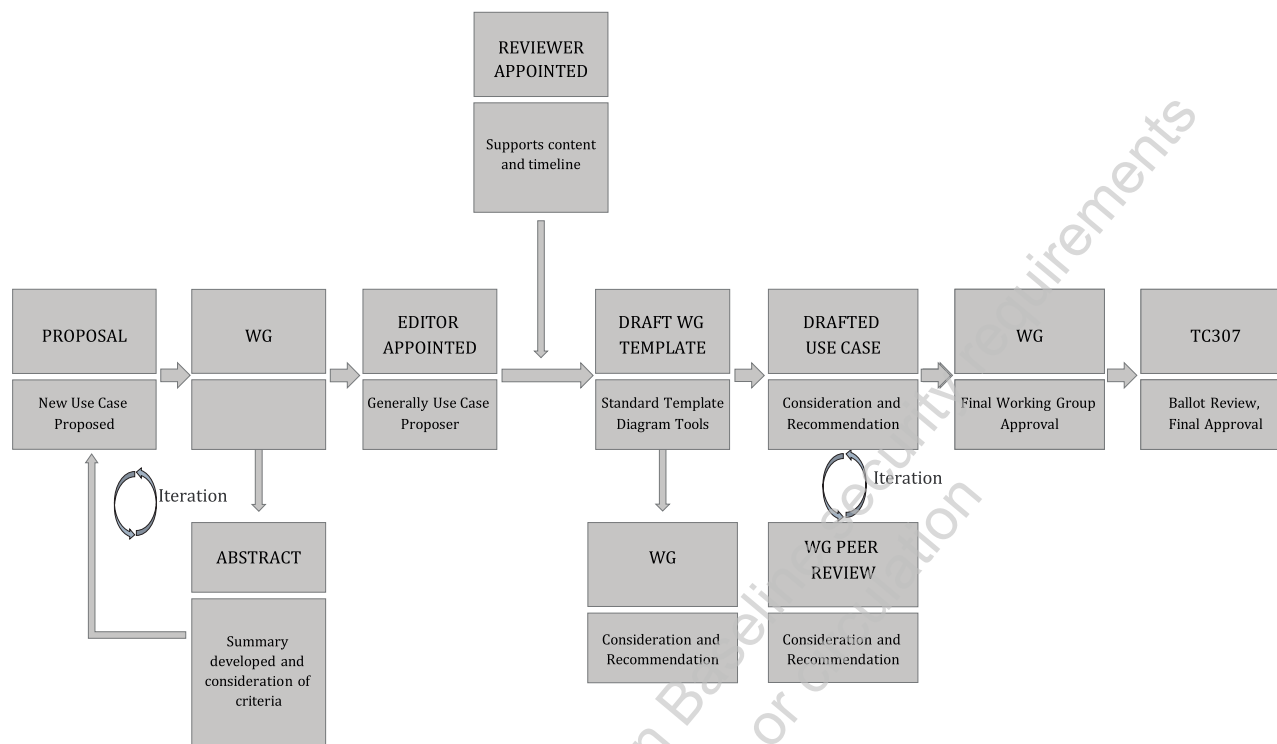


Figure 1 — Use case process and review flow

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.

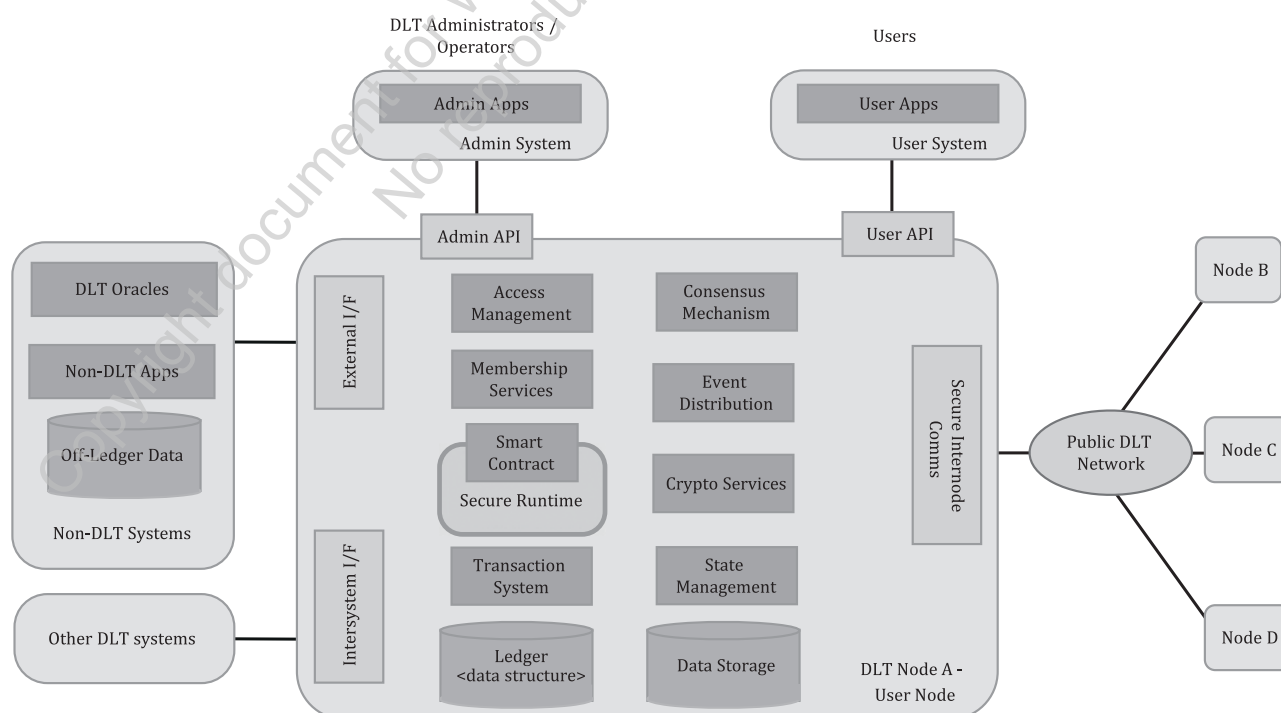


Figure 2 — Reference Architecture System View (ISO 23257 [3])

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.

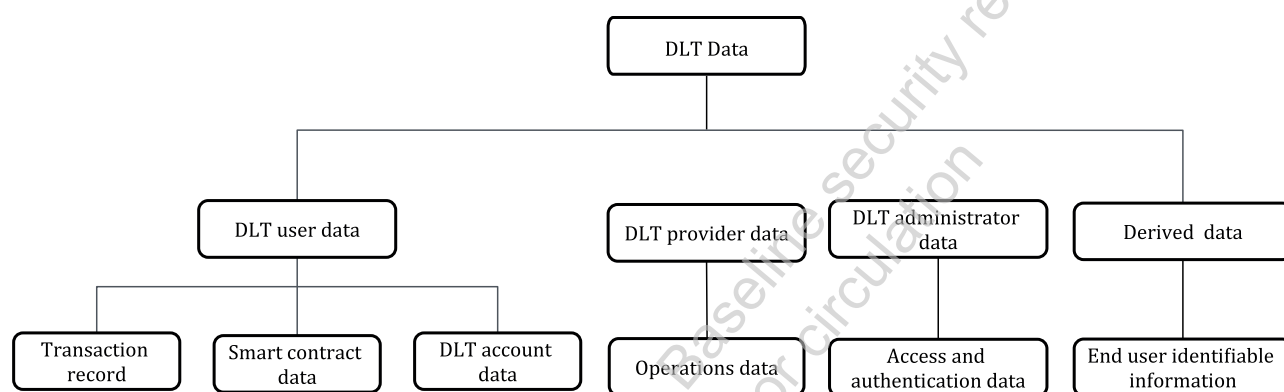


Figure 3 — Data categories from the data source perspective

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.

- Specify the role of each stakeholder in facilitating the data flow.
- Identify the type of data flow (See categories A to D and Z below)
- 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.

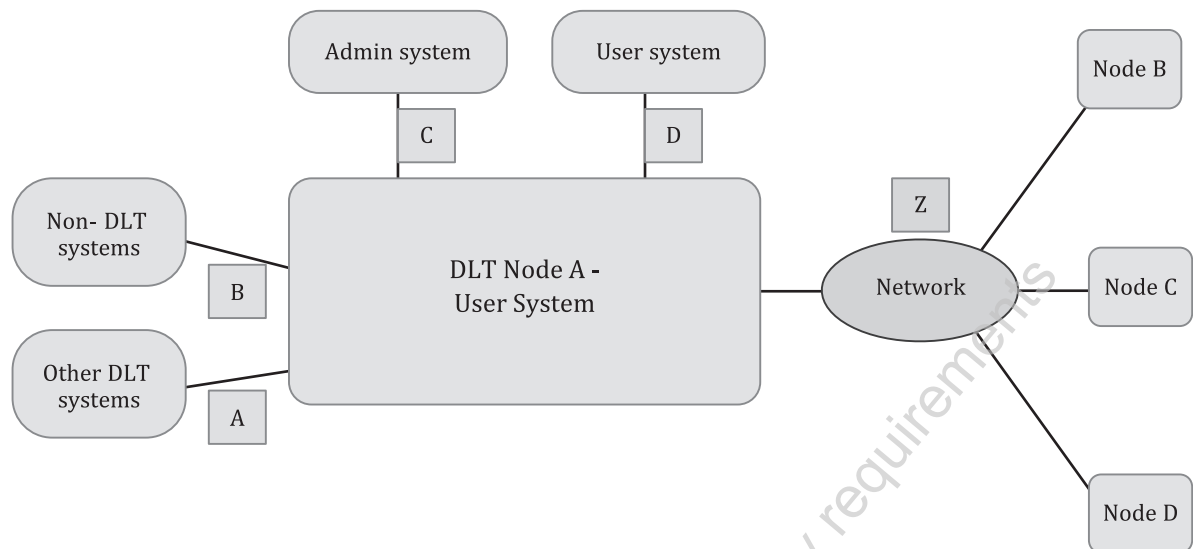


Figure 4 — DLT Data Flow diagram

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.

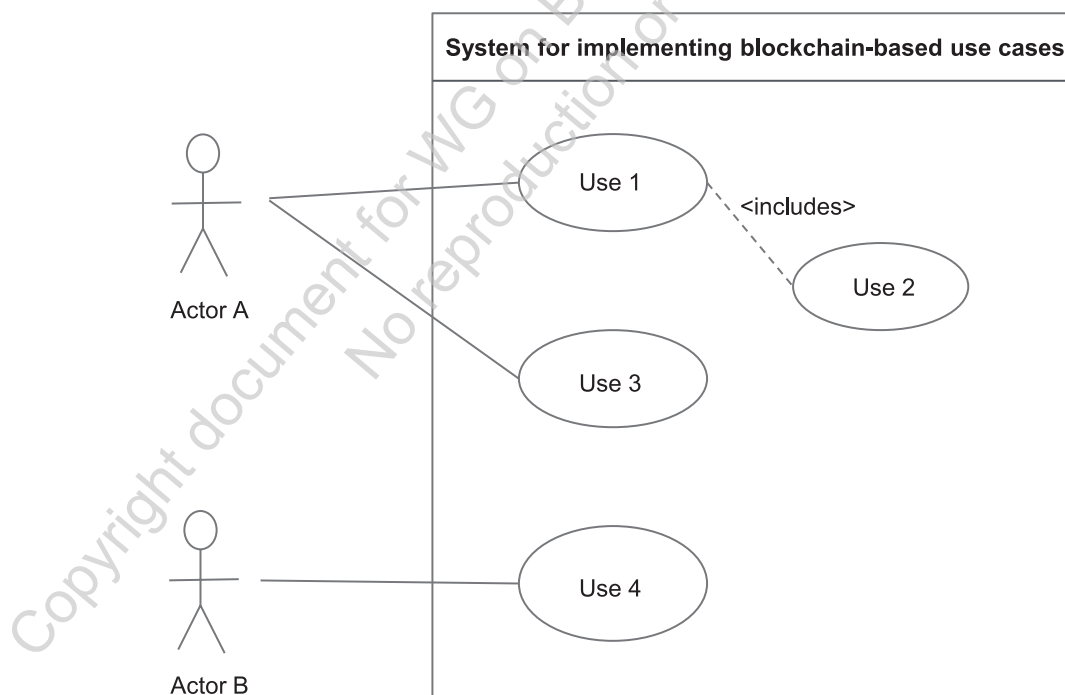


Figure 5 — Simple use case diagram

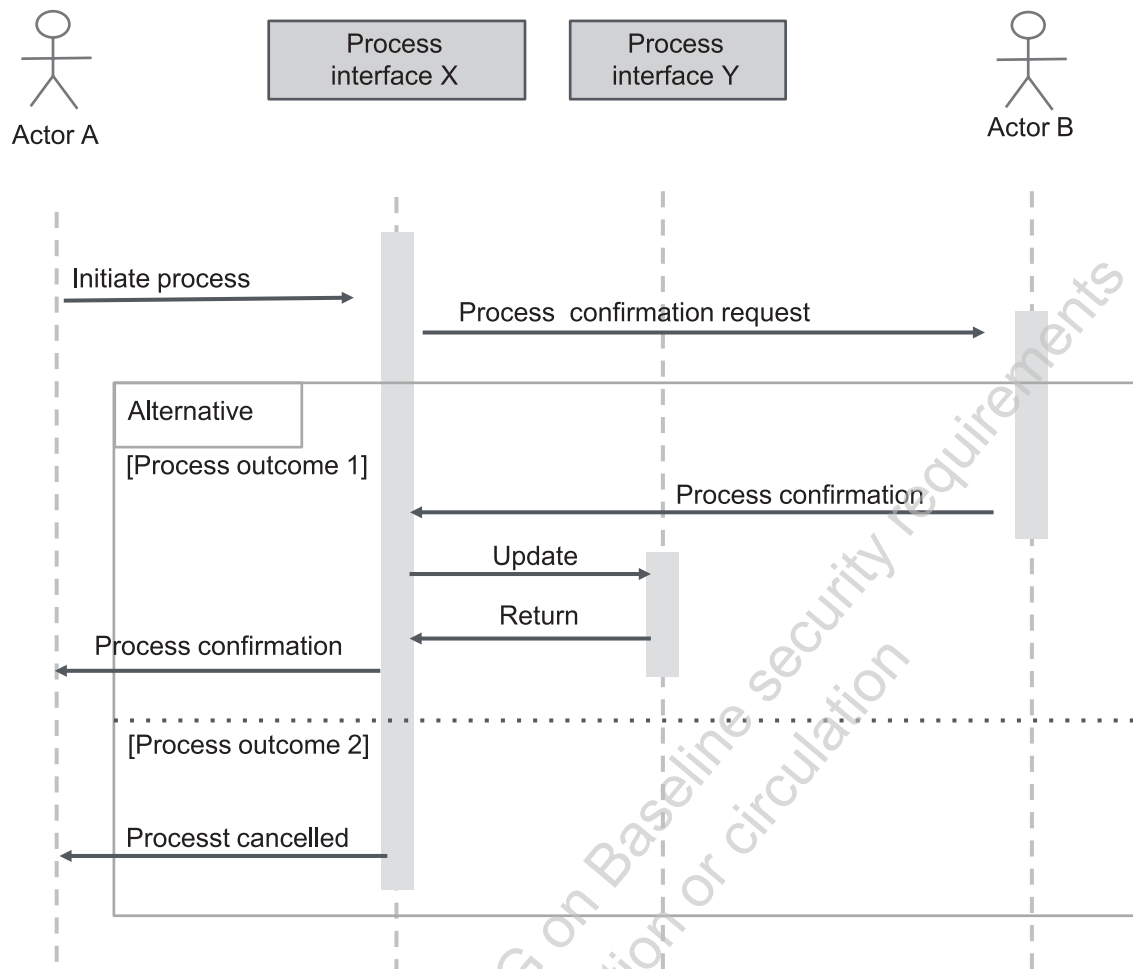


Figure 6 — Example sequence diagram

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 difficulty 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 lakh¹⁾ crores²⁾ 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

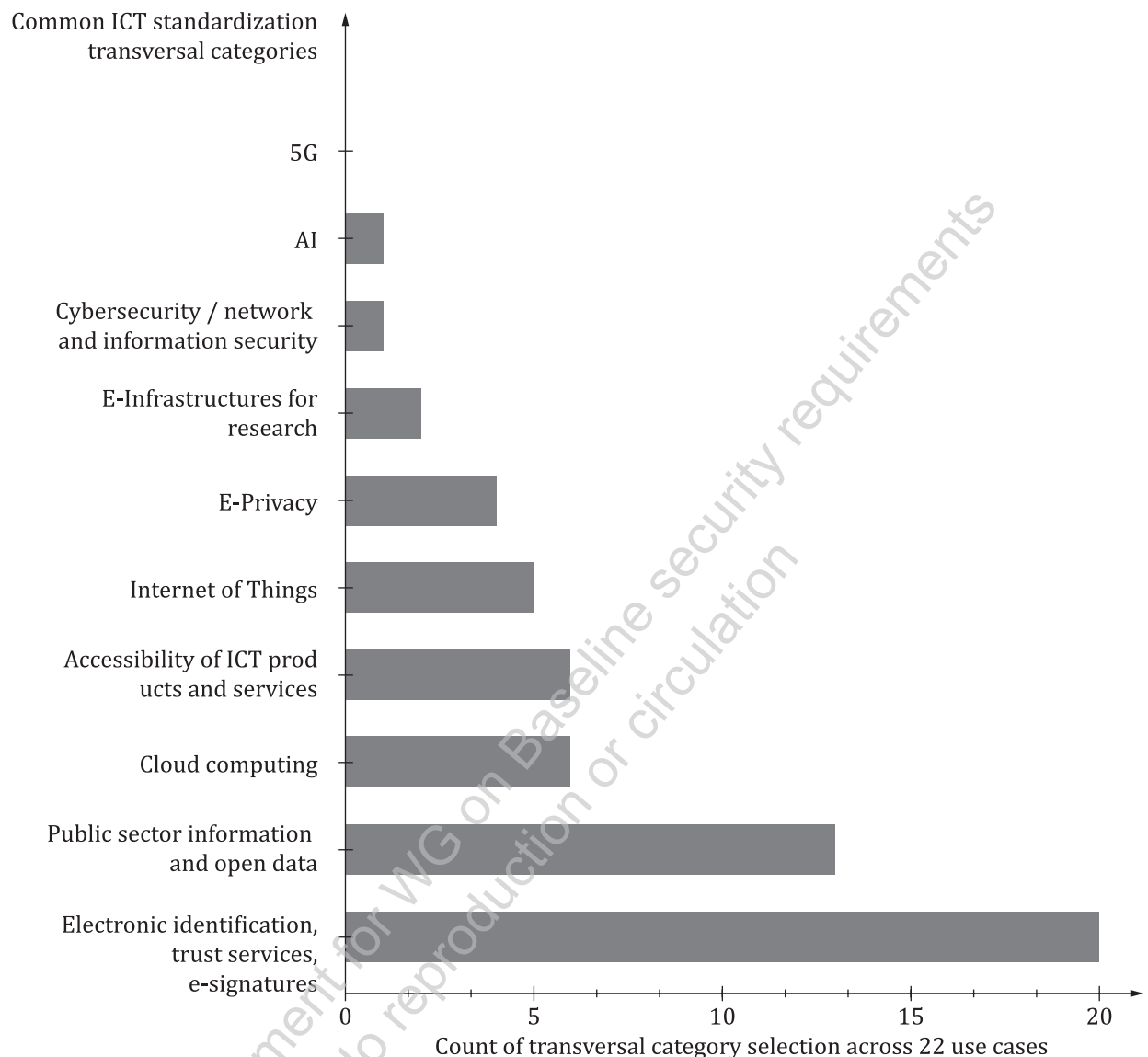


Figure 7 — Transversal category overview

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

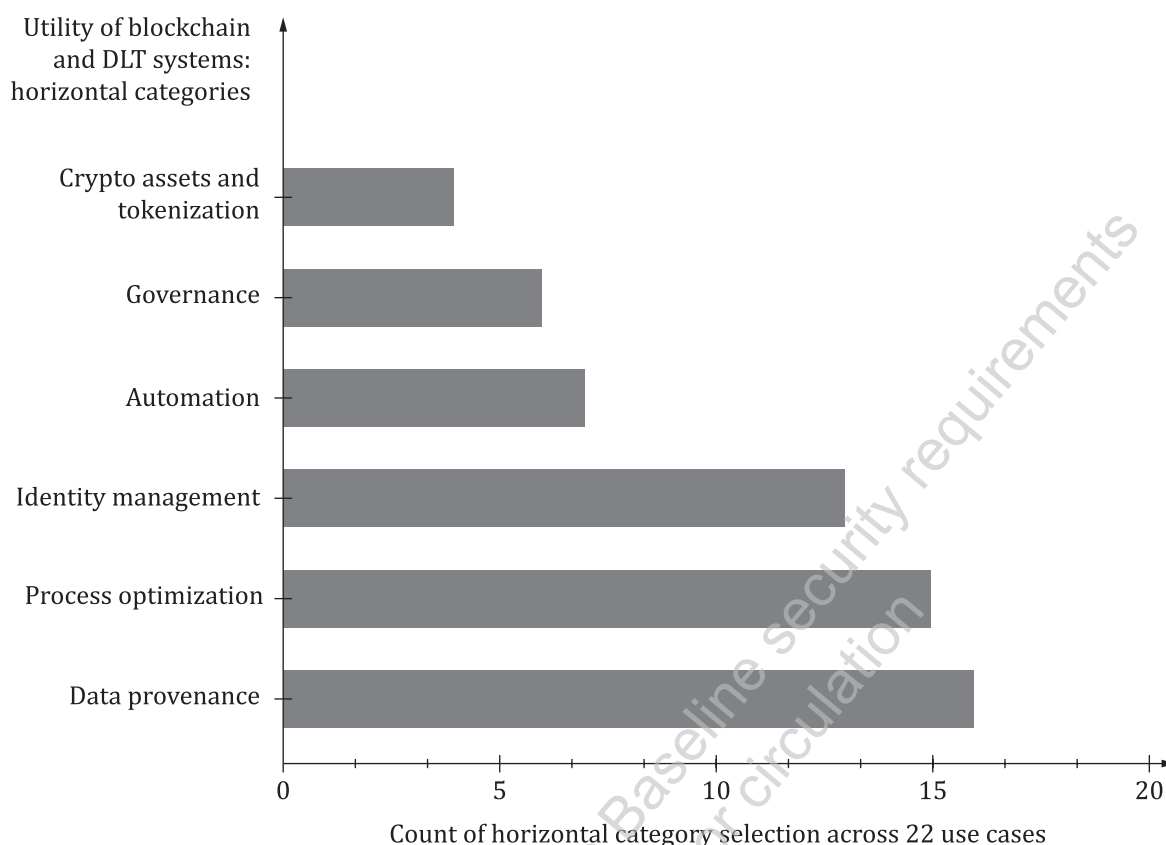


Figure 8 — Horizontal category overview

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

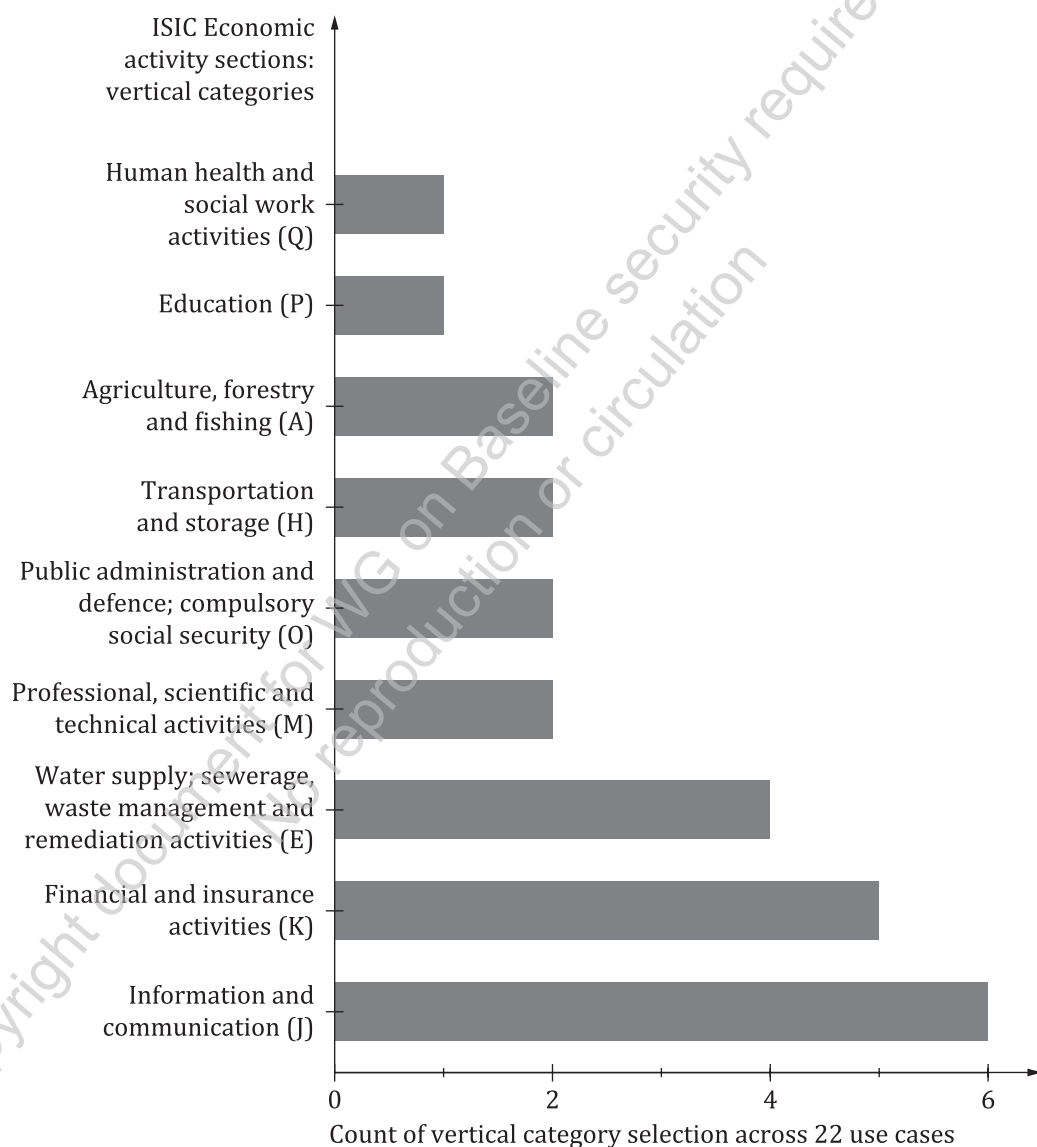


Figure 9 — Vertical category overview

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

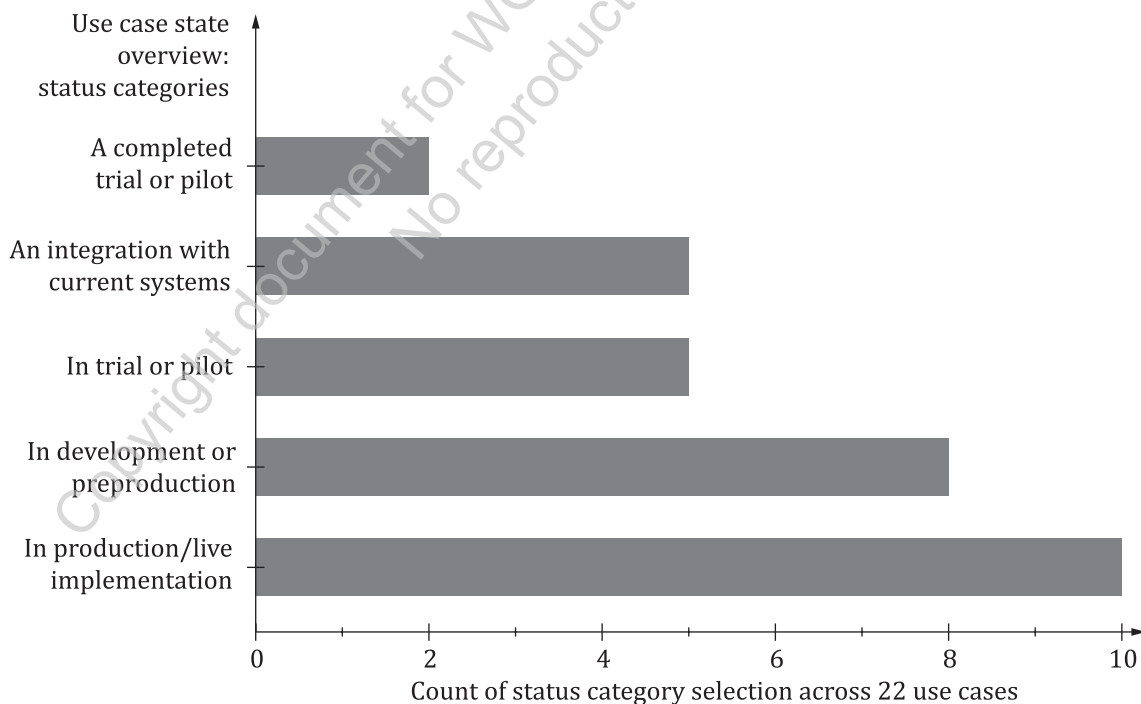


Figure 10 — Status category overview

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)

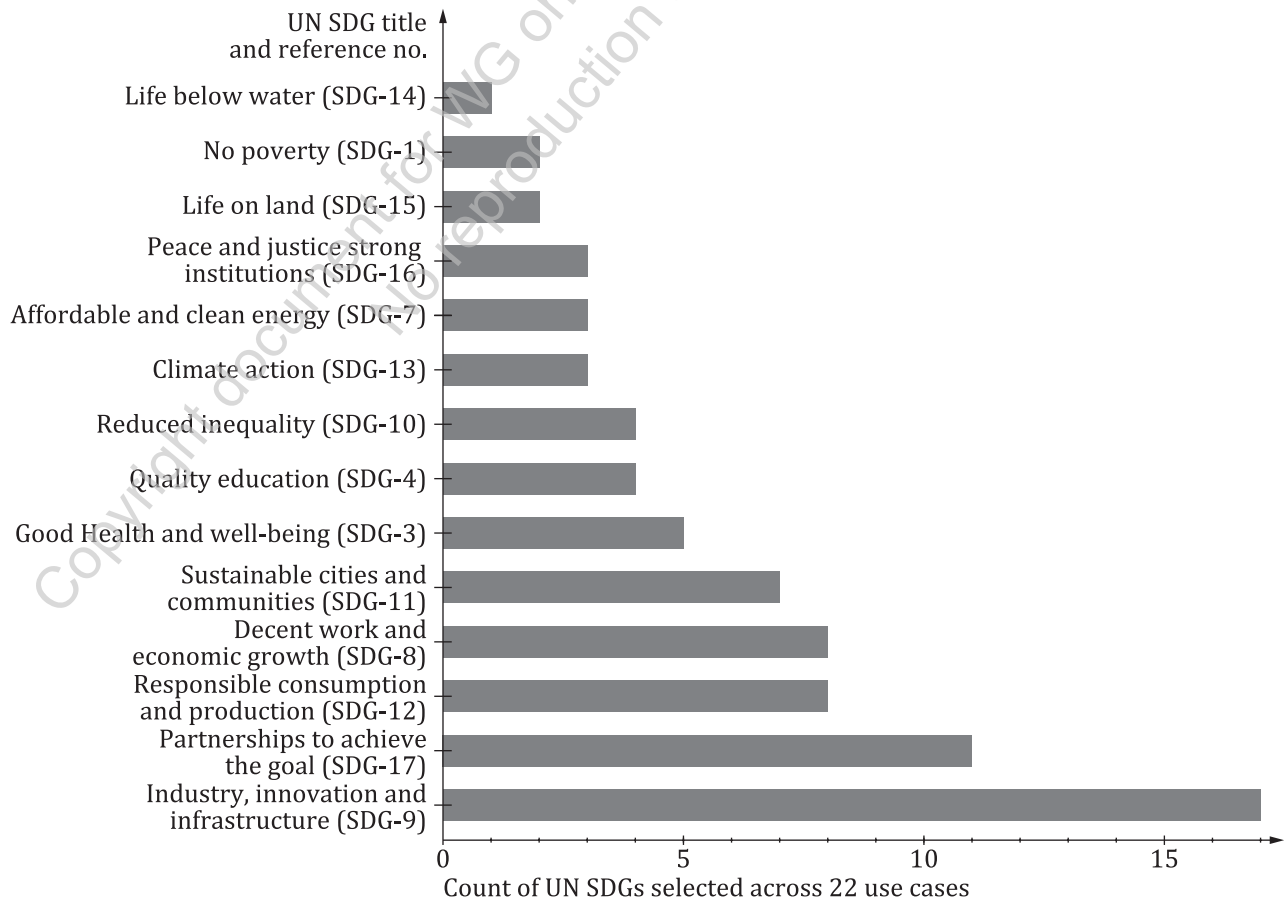


Figure 11 — Sustainable development goals category overview

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 %).

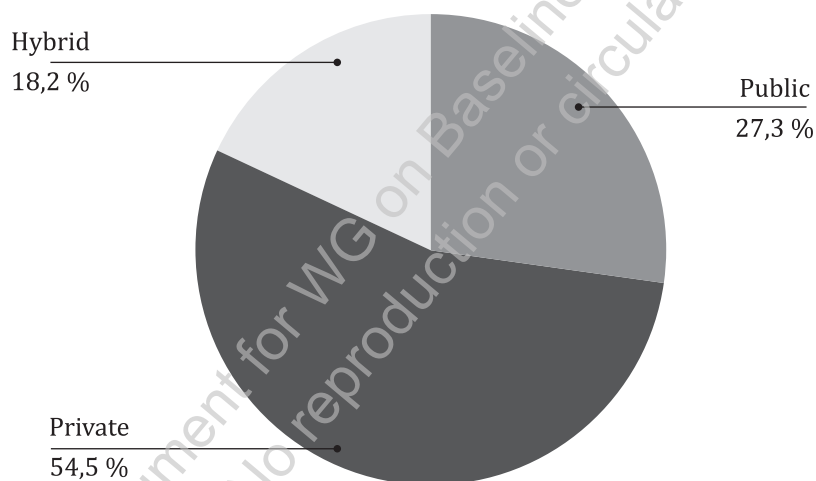


Figure 12 — Blockchain implementation type

Blockchain implementation platforms

[Figure 13](#) shows a count the blockchain implementations referenced in this document.

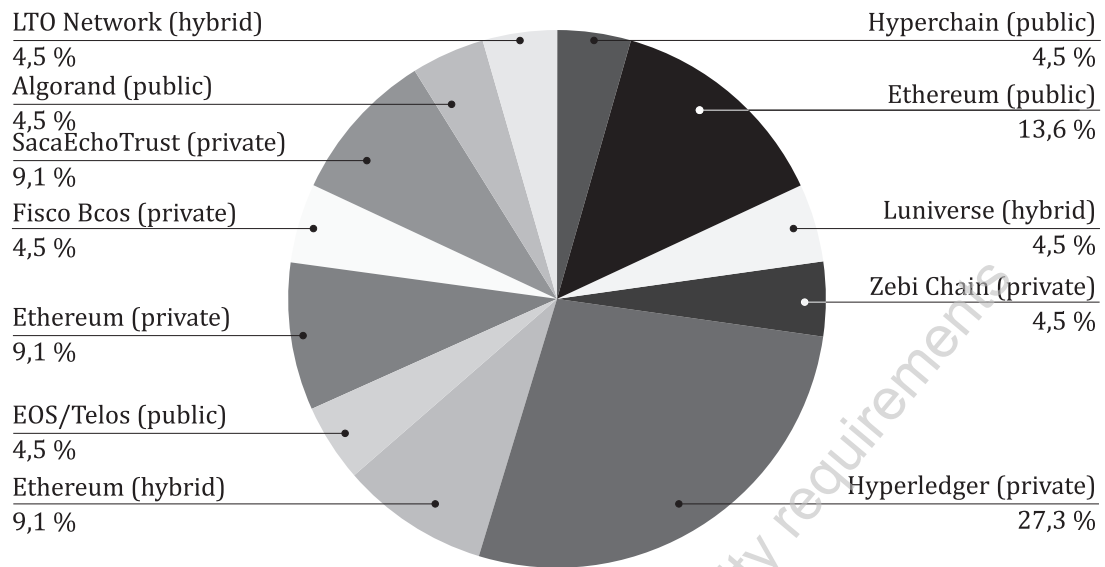


Figure 13 — Blockchain implementation platforms

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.

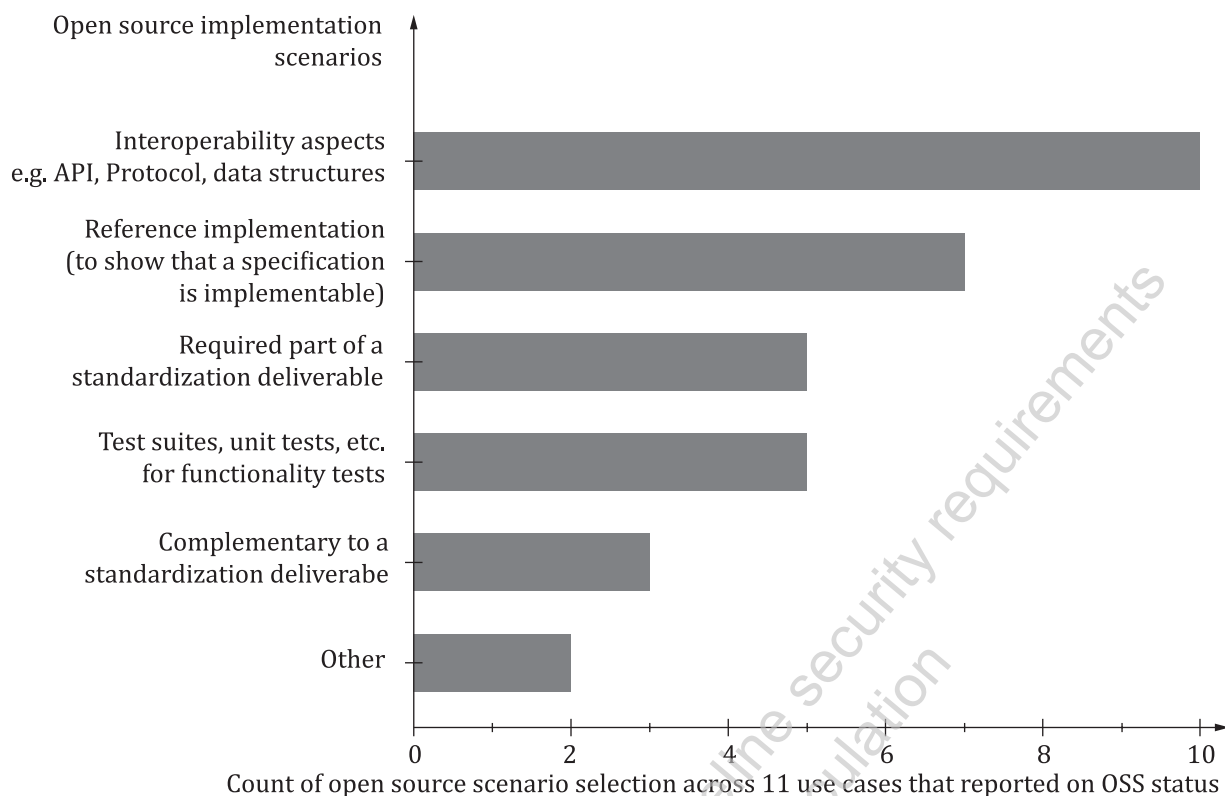


Figure 14 — Open source scenarios

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**

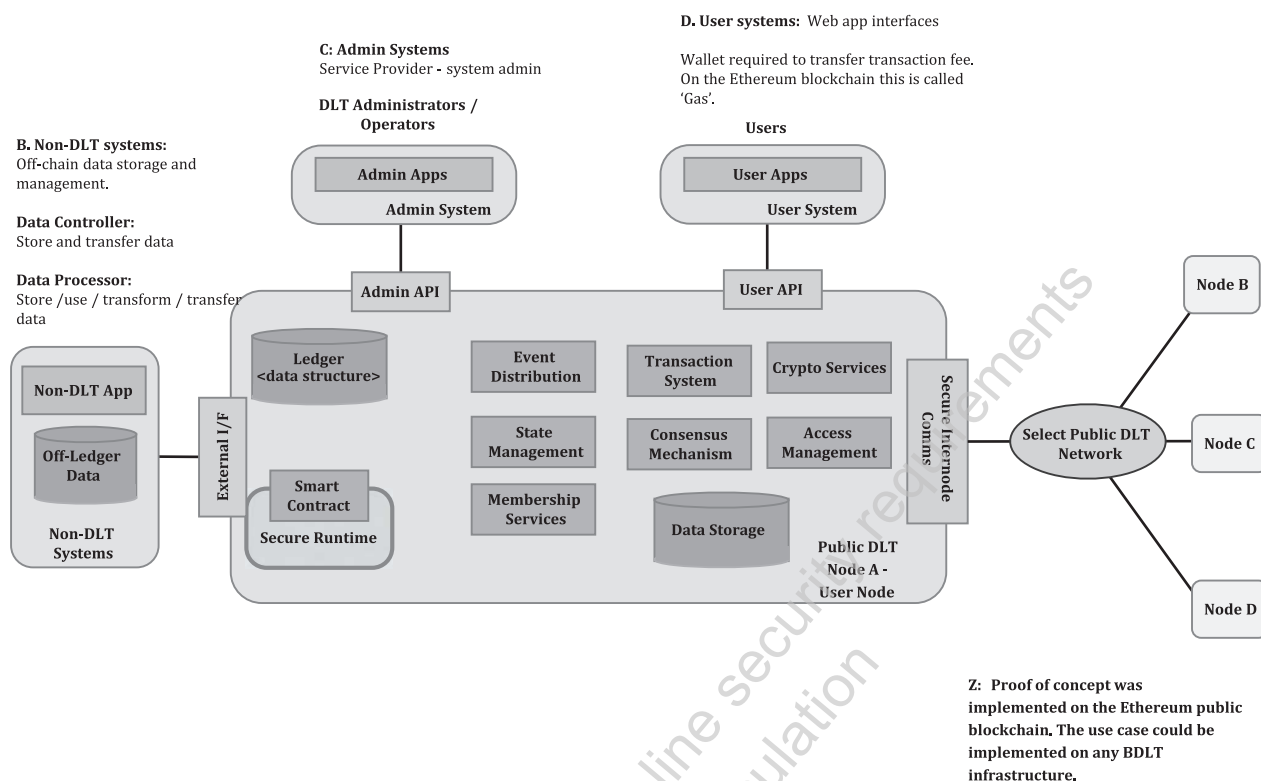


Figure 15 — System view architecture: Data accountability (EC)

— 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

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

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

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

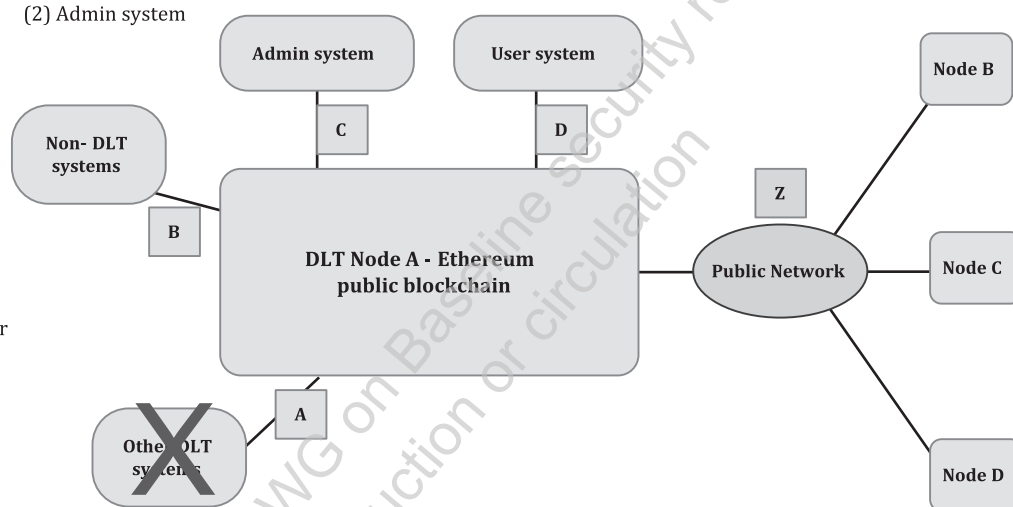


Figure 16 — Data flow analysis: Data accountability (EC)

— 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

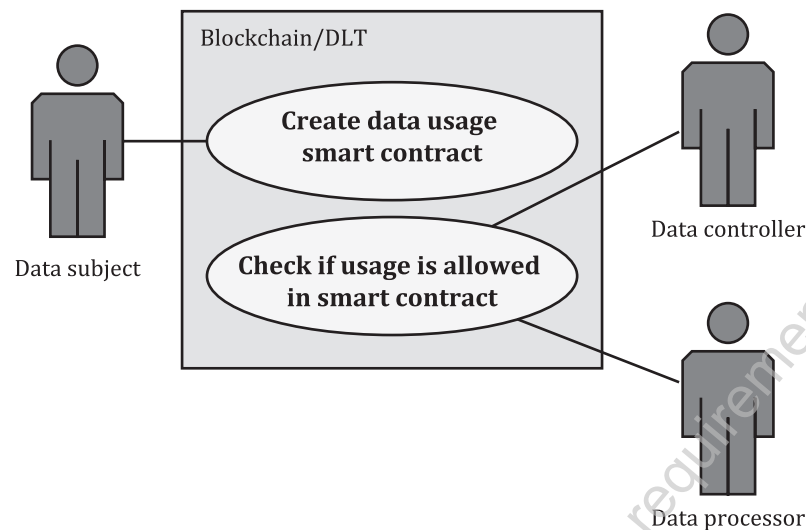


Figure 17 — Use case diagram: Data accountability (EC)

Use case interaction diagram

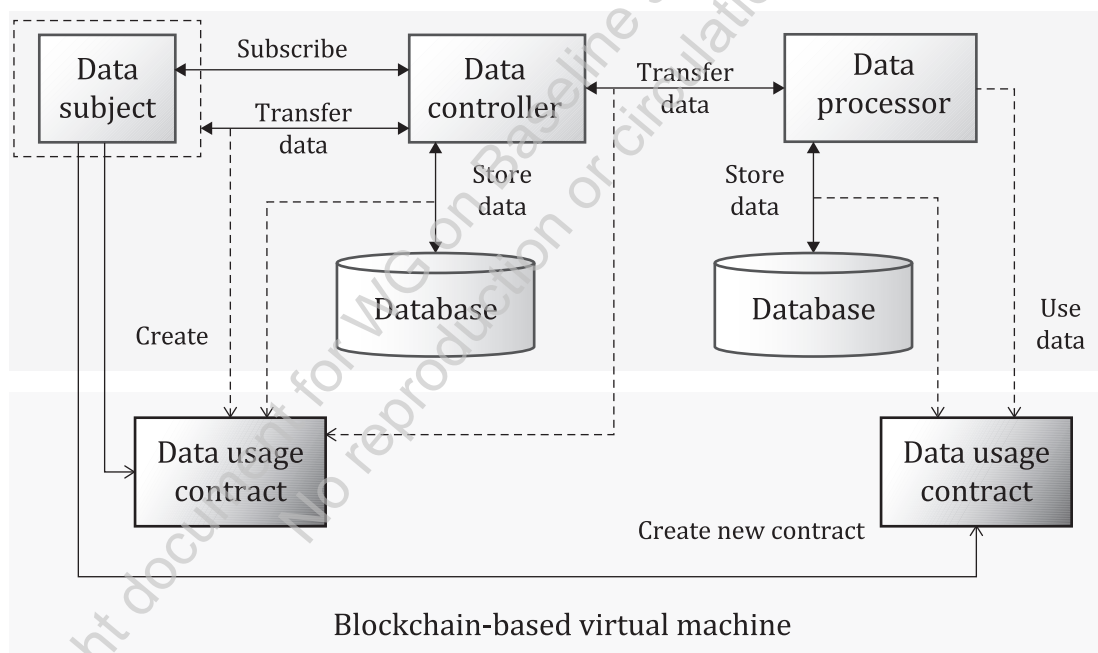


Figure 18 — Interaction diagram: Data accountability (EC)

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.

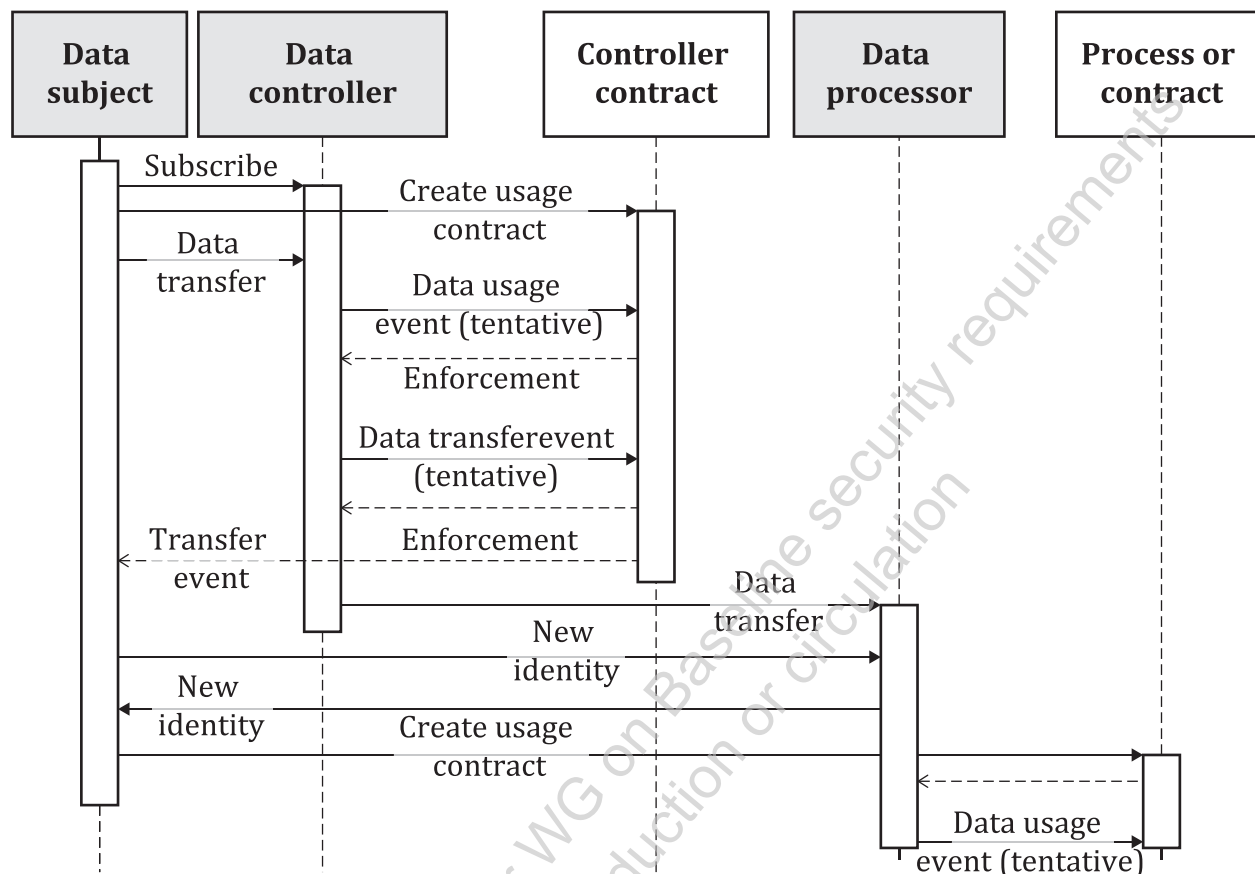


Figure 19 — Sequence diagram: Data accountability (EC)

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.