Technical Report

ISO/TR 6277

First edition
2024-02

Blockchain and distributed ledger technologies — Data flow models for blockchain and DLT use cases

Technologies des chaînes de blocs et technologies de registre distribué - Modèles de flux de données pour les chaînes de blocs et les cas d'utilisation de DLT

Reference number
ISO/TR 6277:2024(en)

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

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 consolidates a set of system-level models from ISO 23257:2022 and ISO/TR 3242:2022 to give a data-flow-centric description framework for blockchain and distributed ledger technology (DLT) use cases. The framework enables a data flow analysis approach for blockchain and DLT use cases which has been defined in ISO 23257:2022, successfully applied across all use cases in ISO/TR 3242:2022 and extended in this document to display more detailed information on data flows.

The robust descriptive capabilities provided by this framework can help to improve blockchain and DLT application design and enhance interoperability. It can be beneficial for:

- clear understanding of data types and data flows in distributed ledger systems that allows for better-designed, fit-for-purpose systems;
- better governance and risk management;
- a sound basis for interoperability modelling for the use cases that require data exchange in hybrid or orchestrated systems environment.

Understanding data flows can be a necessary foundation for DLT users to ensure data privacy and data confidentiality in DLT use cases, or a decision-making basis when implementing technology selection or scheme assessment. From this perspective, data flow analysis is especially essential to scenarios which frequently involve data flows among stakeholders or devices. To illustrate the features of data flows in DLT use cases with above characteristics, this document provides three uses cases which apply the description framework to unfold data flows among devices, data flows along with business process, as well as data flows between physical and virtual spaces. These use cases can also provide an insight into the role of data flow analysis in balancing business value maximization and risk controls.

This document is organized as follows:

- Clause 5 presents an overview of DLT data flows, including data flow categories, data categories, roles/subroles and considerations related to data flow.
- Clause 6 and Clause 7 provide analysis of typical intra-system and inter-system data flows for DLT systems.
- Clause 8 provides three DLT use cases based on a descriptive and visualization template focusing on data flows.

Blockchain and distributed ledger technologies — Data flow models for blockchain and DLT use cases

1 Scope

This document uses a set of models that describe the flows of different types of data between distributed ledger technologies (DLT) and related systems, as well as between different DLT nodes.

It provides a descriptive analysis of data flows in the development of use cases, as well as the basis for understanding the characteristics of DLT data flows, to support DLT application design and system analysis.

The models referenced are in accordance with ISO 23257:2022 and the use case analysis approach provided in ISO/TR 3242:2022.

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*

ISO 23257, *Blockchain and distributed ledger technologies — Reference architecture*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739, ISO 23257 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
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

Note 2 to entry: Self-service provisioning refers to the provisioning of resources provided to cloud services performed by cloud service customers through automated means.

[SOURCE: ISO/IEC 22123-1:2023, 3.1.1]

3.2
data category
class of data items that are closely related from a formal or semantic point of view

[SOURCE: ISO 30042:2019, 3.8, modified — Example and Notes to entry deleted.]

3.3
data flow
sequence in which data transfer, use, and transformation are performed during the execution of a computer program

[SOURCE: ISO 23257:2022, 3.5]

3.4
decentralized identifier
DID
identifier that is issued and managed in a decentralized system and designed to be unique within a context

Note 1 to entry: Decentralized identifiers are used in systems that do not rely on central registration authorities.

[SOURCE: ISO 22739:2024, 3.18]

3.5
derived data
data created as a result of processing that involves steps other than or in addition to direct retrieval and validation of information from data functions

[SOURCE: ISO/IEC 20926:2009, 3.17]

3.6
DLT account
distributed ledger technology account
representation of an entity participating in a transaction in a DLT system

[SOURCE: ISO 22739:2024, 3.26]

3.7
edge
boundary between pertinent digital and physical entities delineated by networked sensors and actuators

Note 1 to entry: Pertinent digital entities means that the digital entities which need to be considered can vary depending on the system under consideration and the context in which those entities are used.

[SOURCE: ISO/IEC TR 23188:2020. 3.1.2]

3.8
end user identifiable information
EUII
derived data associated with a user that is captured or generated from the use of the service by that user

Note 1 to entry: Data that is linked to the user but is not DLT user data.

Note 2 to entry: End user identifiable information includes connectivity data, usage data.

[SOURCE: ISO/IEC 19944-1:2020, 3.1.2, modified — Notes 1 and 2 to entry added.]

3.9
role
set of activities that serves a common purpose

[SOURCE: ISO/IEC 22123-1:2023, 3.1.10]

3.10
peer-to-peer
P2P
relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central entity

[SOURCE: ISO 22739:2024, 3.70]

3.11
smart contract
computer program stored in a distributed ledger technology system wherein the outcome of any execution of the program is recorded on the distributed ledger

Note 1 to entry: A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction.

[SOURCE: ISO 22739:2024, 3.88]

3.12
sub-role
subset of the activities of a given role

[SOURCE: ISO/IEC 22123-1:2023, 3.3.11]

3.13
transaction record
record documenting a transaction of any type

Note 1 to entry: Transaction records can be included in, or referred to, in a ledger record.

Note 2 to entry: Transaction records can include the result of a transaction.

[SOURCE: ISO 22739:2024, 3.95]

4 Abbreviated terms

API	Application programming interface
DID	Decentralized identifier
DLT	Distributed ledger technology
ICT	Information and communications technology
IoT	Internet of things
n.e.c.	Not elsewhere classified
PIA	Privacy impact assessment
PII	Personal identifiable information
PoC	Proof of concept
SDG	Sustainable development goal
SME	Small and medium-sized enterprise
VC	Verifiable credential

5 Overview of data flow for DLT

5.1 General

The impetus for introducing DLT-specific data flow models is to support technical and business process analysis. The models mentioned in this document are in accordance with ISO 23257:2022 and applied across all use cases in ISO/TR 3242:2022 combined with the behavioural UML models. The focus on the approach in this document is exploring diverse ways of applying it to data flow analysis on DLT use cases. The approach taken in this document derives from architectural approaches in cloud computing and service-oriented design. If a service model is a collection of components that represents a business service, a data flow model that is described across component-based view of a system can help bring clarity to both technical and business objectives in system design.

It can be seen in ISO/TR 3242:2022 and elsewhere that applications and systems deploy blockchain and DLT to provide robust and purposeful system transparency in highly distributed, multi-party systems, on cloud-based execution environments. The data flow models reviewed here can be used in tandem with service-modelling approaches to gain greater insight into system functionality and business process performance.

5.2 Categories of data flows

ISO 23257:2022 and ISO/TR 3242:2022 identify five fundamental data flows relative to DLT systems:

- Data flow N: data flowing within and between the nodes of the DLT system.
- Data flow A: data flowing between separate DLT systems when they interoperate.
- Data flow B: data flowing between a DLT system and non-DLT systems connected to it.
- Data flow C: data flowing between administration applications and a DLT system.
- Data flow D: data flowing between user applications and a DLT system.

NOTE ISO 23257:2022 defines Data flow Z as data flowing among the nodes of the DLT system. ISO/TR 3242:2022 includes data flow within the nodes of the DLT system and defines Data flow Z as data flowing within and between the nodes of the DLT system. This document adopts the definition in ISO/TR 3242:2022 and uses the code N instead of Z to avoid confusion.

5.3 Data categories

This document identifies data categories in the DLT ecosystems, to help understanding DLT data flows and support transparency about DLT data. A data taxonomy is also useful for the conversation about data between different roles/sub-roles. This document provides the following four sets of data categories:

- data categories from data storage perspective;
- data categories from data sources;
- identifier data categories;
- other data categories.

5.3.1 Data categories from data storage perspective

5.3.1.1 General

In order to balance the advantages and performance of DLT systems, off-ledger data storage has increasingly become a common auxiliary way of data storage in DLT system, especially in the DLT applications involving large amount of DLT user data.

The main concern for on-ledger data and off-ledger data is the difference of scope of data processing and use. In most cases, processing and use of off-ledger data have no much difference with data in other types of IT systems, however, it is usually impossible to delete on-ledger data, which makes it more crucial to provide specific ways of ensuring transparency and privacy protection.

5.3.1.2 On-ledger data

On-ledger data are data stored inside a DLT system, which includes small amounts of data from DLT users. Due to the size-limit of DLT ledger, on-ledger data can also include hashes related to off-ledger data from DLT users.

5.3.1.3 Off-ledger data

For large amounts of data from DLT users, or personal identifiable information (PII) which might need to be deleted or updated by the PII principal, it is common practice to store the data on a cloud on the user's infrastructure or a public storage provided by a third party or network. Off-ledger data also includes data from the DLT provider data and data derived when a DLT application is used.

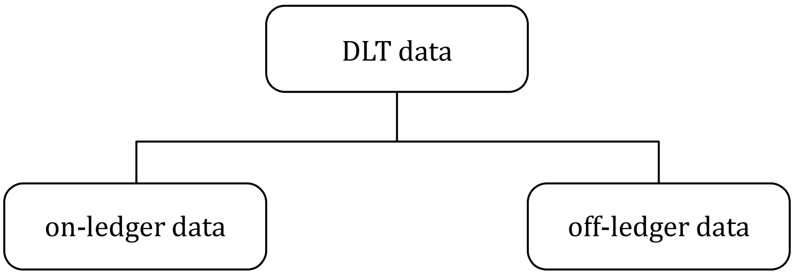


Figure 1 — Data categories from storage perspective

5.3.2 Data categories from data sources perspective

5.3.2.1 General

ISO 23257:2022 defines six DLT roles, including DLT developers, DLT administrators, DLT users, DLT providers, DLT governors and DLT auditors. Among these DLT roles, DLT administrators, DLT users and DLT providers are most closely related to DLT data. In order to support different stakeholders to carry out data-related activities, or to formulate data-related policies, this document identifies seven data categories which are associated to different DLT roles (see Figure 2).

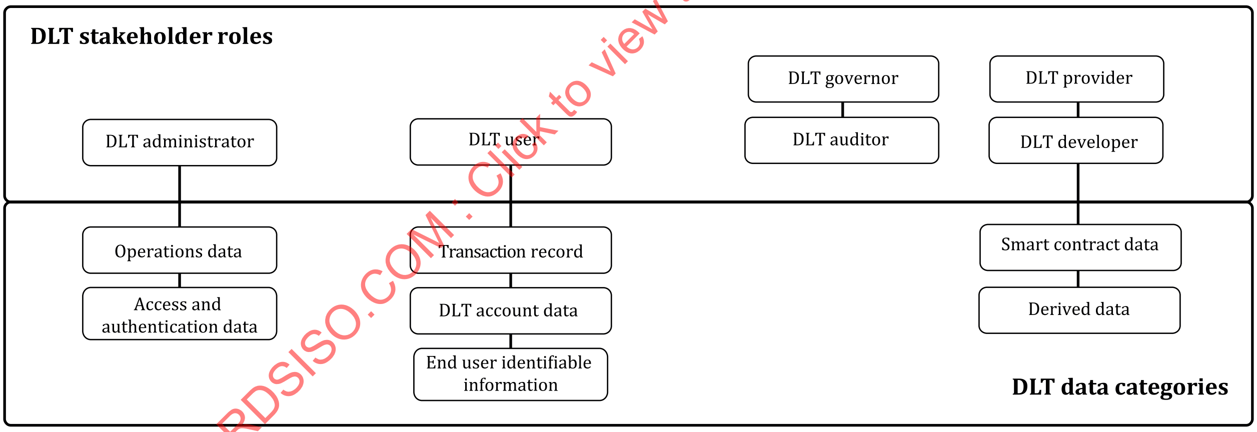


Figure 2 — DLT stakeholder roles and related DLT data categories (reproduced from ISO 23257:2022)

5.3.2.1.1 Transaction record

Transaction record can be financial transaction data, or generalized transaction data such as genome data, voter record, transport data, product production data. Transaction records might be on-ledger data or off-ledger data with related hashes stored on ledger. Transaction record is generated when a DLT user uses a DLT system to record a transaction.

5.3.2.1.2 DLT account data

A smart contract or digital asset, for example, can be associated with a DLT account. Corresponding DLT account data are data representing an entity whose data are recorded on a DLT system. DLT account data are generated or updated when a DLT user creates a DLT account or uses the account.

5.3.2.1.3 End user identifiable information

End user identifiable information is linkage to the user but is not directly created by DLT users. End user identifiable information includes connectivity data, usage data.

5.3.2.1.4 Operations data

Operations data are data which is used for supporting the operation of DLT system, which includes service logs, configuration data.

5.3.2.1.5 Access and authentication data

Access and authentication data are data used within DLT system to manage access DLT capabilities, DLT data or smart contract, which includes passwords, cryptographic keys, security certificates. Access and authentication data are controlled by DLT administrator and are critical to its administrative activities.

5.3.2.1.6 Smart contract data

Smart contract data includes not only executable codes of program but also execution results. Smart contract data can be generated when a DLT developer creates or maintains the smart contract, or a DLT operator runs the smart contract.

5.3.2.1.7 Derived data

Derived data include data describing the connections of the DLT system, data describing the usage of the DLT services, etc. Derived data also include end user identifiable information.

5.3.3 Identifier data categories

ISO/TR 6039 specifies the identifiers data including:

- Subject identifiers: natural persons and legal entities used by administrations of countries, for specific (international) government functions and in some industries. Subjects are entities with rights and obligations.
- Object identifiers: object identifiers used for government purposes and in several industries. Objects are entities without right and obligations.

5.3.4 Other data categories

5.3.4.1 Overview

There are many other types of data and data types of selected examples that are important in financial use cases are presented in 5.3.4.2 to 5.3.4.4.

5.3.4.2 Market price data

Market prices are available for many objects. These include, but are not limited to:

- stock prices of listed companies at exchanges;
- currency rates of Forex markets;

- commodity prices for commodity markets;
- derivatives rates;
- interest rates (Central Banks reference rates and market rates);
- prices of retailers and web-retailers for goods and services.

5.3.4.3 Accountancy data categories

- Stock data: Accountants use specific terminology included in the IFRS standard which uses a balance sheet that can be presented in an annual report. These stock data include: the value of the goods, debtor position, creditors position presented on the balance sheet. The stock data covers the aggregation of data at a certain point in time.
- Flow data: Accountants use terminology included in the IFRS standard for flow data such as a) profit and loss account and b) cashflow statement. Flow data includes the flow of values, as they change over time, during a predefined time period.

5.3.4.4 Message data in networks

- Messages: Data in messages can be structured or unstructured. The (industry) networks used for Business to Government (B2G) or for Business to Business (B2B) purposes include mostly instructions on the structure of the data messages used in the network involved.

5.4 Roles from the perspective of data flow

5.4.1 DLT stakeholder roles and stakeholder data

Data flows are triggered by the data-related operations of stakeholders, between system components that belong to or are associated with them. Stakeholders achieve their aims by means of role-based interactions with the DLT system.

ISO 23257:2022, 9.2 describes a set of roles/sub-roles which address the main activities associated with DLT systems and gives overall descriptions for activities of these roles/sub-roles. When discussing data flow and data taxonomy, the detailed data-related activities of these roles/sub-roles are necessary information.

5.4.2 Roles/sub-roles and their activities related to data flow

5.4.2.1 Data-related activities of DLT users

A DLT user often uses a DLT system on their devices, by using a DLT application or an application that interacts with a DLT API. Examples of its activities include:

- providing data to DLT systems;
- using data obtained from DLT systems on their devices;
- installing applications on devices.

5.4.2.2 Data-related activities of DLT administrators

A DLT administrator performs administrative activities which might be data-oriented or produce data. Examples of its activities include:

- developing plans to ensure blockchain data backup and recovery, as well as possible data replication and failover;
- ensuring compliance of data storage and processing;

- discovery, classification and protection of data;
- managing access and authentication data;
- managing application configuration data;
- managing cross-ledger data exchange;
- managing long-term preservation of data.

5.4.2.3 Data-related activities of DLT providers

As defined in ISO 23257:2022, DLT provider is the business stakeholder owning and operating one or more DLT nodes. DLT providers can have data interaction with DLT users and are also responsible for the operation of data.

DLT providers include three sub-roles:

- DLT system operators;
- DLT node operators;
- DLT application operators.

5.4.2.3.1 Data-related activities of DLT system operators

Examples of DLT system operators' activities include:

- providing audit data activities according to audit's requests;
- maintaining operation data.

5.4.2.3.2 Data-related activities of DLT node operators

Examples of DLT node operators' activities include:

- data tracking to achieve the system performance quality control;
- managing access control of data shared by different DLT users on the same node.

5.4.2.3.3 Data-related activities of DLT application operators

Examples of DLT application operators' activities include:

- providing data, applications and data related services;
- processing and using data including data from DLT users under an agreement.

5.5 Considerations related to data flow

5.5.1 Data security

Data security covers preservation of confidentiality, integrity and availability of data.

For DLT systems, it is necessary to ensure full-link security in end-to-end data channel, from IoT, user devices to DLT systems.

5.5.2 Privacy protection

As specified in ISO/TR 23244:2020, there is a series of challenges for privacy protection in DLT systems, which are generally based on characteristics that differentiate them from other ICT systems.

ISO/TR 23244:2020 also lists a range of areas which privacy within a DLT system covers:

- privacy of blockchain users;
- personal information stored within blockchain blocks;
- personal information stored in external resources referenced in DLT content (off-ledger);
- privacy of transactions or data.

Besides, security of authorization data for related parties to use DLT users' data are also an important concern.

A given DLT system might contain PII or it might contain no PII. Establishing whether a given system contains PII requires a privacy impact assessment (PIA), which is dealt with by ISO/IEC 29134. A PIA ideally can be undertaken as part of the design of a DLT system in order to ensure that the solution is capable of compliance with relevant privacy requirements.

5.5.3 Governance of data

Governing bodies of DLT data are structured differently from traditional IT systems. There are multiple stakeholders involved in the life cycle of DLT data. ISO/TS 23635:2022 identifies three main tasks that each group of stakeholders can govern a DLT system through:

- Evaluation of the current and future use of DLT system and identification of obligations and risks.
- Direct preparation and implementation of policies, procedures and internal control frameworks to ensure that the use of DLT systems meets obligations and mitigates significant risk.
- Monitoring of conformance of policies, procedures and performance of the internal control framework operations to ensure sufficient risk mitigation and compliance to obligations.

ISO/IEC 38505-1:2017 also provides an example data management life cycle. See Figure 3.

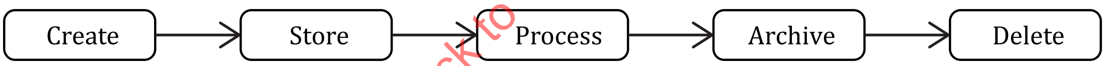


Figure 3 — Example data management life cycle

NOTE Archivists use another life cycle model. To archive is one of two final dispositions, the other being delete.

For DLT system, the storing of data involves numerous stakeholders, and the deletion of on-ledger data which is designed to be immutable also needs to be reconsidered.

5.5.4 Interoperability

ISO/IEC 22123-1:2023 defines interoperability as the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

The interoperability related to data applies to the external flows of data identified.

6 Intra-system data flow

6.1 Overview

A typical process with a serial of data flows taking place within a DLT system is a transaction life-cycle (see Figure 4). Two stages are considered for a whole transaction process, respectively preliminary stage and full life cycle transaction stage. For the full life cycle stage, although a transaction life cycle can differ because of differing protocols or implementations, this document takes a 5-steps-life cycle including submit, broadcast, consensus, execute and feedback as an example.

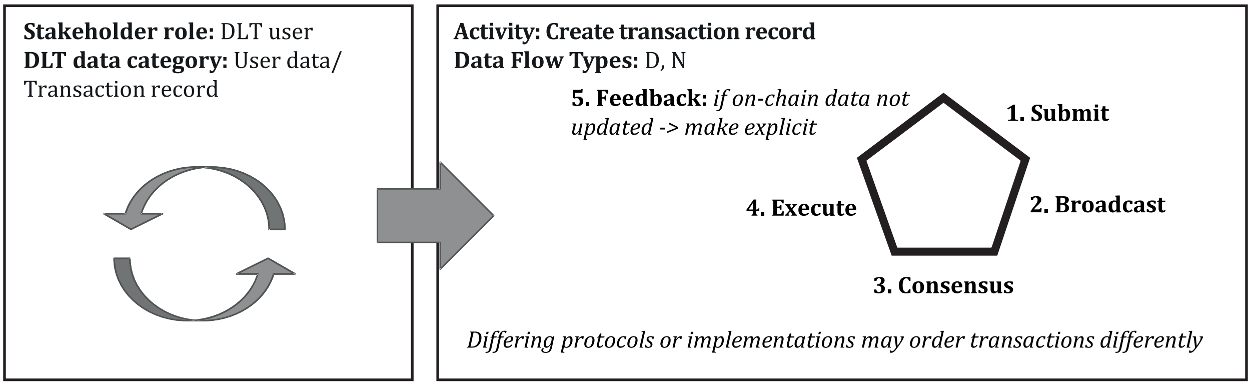

Stakeholder role: DLT user
DLT data category: User data/ Transaction record
Activity: Create transaction record
Data Flow Types: D, N
5. Feedback: *if on-chain data not updated -> make explicit*
1. Submit
2. Broadcast
3. Consensus
4. Execute
Differing protocols or implementations may order transactions differently

Figure 4 — Intra-system data flow process: User creates transaction record

NOTE 1 The data life cycle model works well only when there are clearly identifiable stages in "real-life". When data are actively modified and used during all their lifetime, life cycle model could be unhelpful.

To clarify the data involved activities, this document identifies the following information for each step.

- data categories (from data storage and DLT system role perspectives);
- data flow categories;
- actions of data: data creation, data storage, data processing, data transmission.

NOTE 2 Data content is use case specific.

6.2 Data flow during DLT transaction procedure

6.2.1 Preliminary stage

6.2.1.1 DLT system setup

After the DLT system is created, the DLT developer and provider set up multiple distributed nodes, system configuration, administrator accounts, etc. Accordingly, the operation data and access authentication data are created and stored consistently among multiple nodes.

6.2.1.2 DLT user account registration

The DLT user performs registration on the DLT system before utilizing on-chain services. Optionally, the user can provide identifiable information to establish the link between account and physical item.

- Data creation: the DLT account data are created, including account identity, balance, status, etc.
- Data storage: the account data are consistently stored at distributed nodes. Conforming to the applicable requirements, policies, rules and considerations in ISO/TR 23244, the sensitive information in DLT account data can be stored on the blockchain system with protection based on access control, encryption, etc. Alternatively, the sensitive information can be linked to on-chain identifier and stored in an off-ledger datastore with restricted access.

6.2.2 Full life cycle data flow in one transaction

6.2.2.1 Outline

One transaction implementation is illustrated in Figure 5.

- S1: Transaction submission. The transaction message is submitted by user or admin system. If it is submitted by user, this message can be viewed as data flow D. Otherwise, it is data flow C.

- S2: Transaction broadcasting. The message is validated and broadcasted among distributed nodes, which corresponds to data flow N.
- S3: Consensus achievement. The consensus protocol is achieved to determine the transaction execution order, which corresponds to data flow N.
- S4: Transaction execution. Each node executes transaction independently.
- S5: Result feedback. The result is sent back to user or admin system. If it is submitted by user, this message can be viewed as data flow D. Otherwise, it is data flow C.

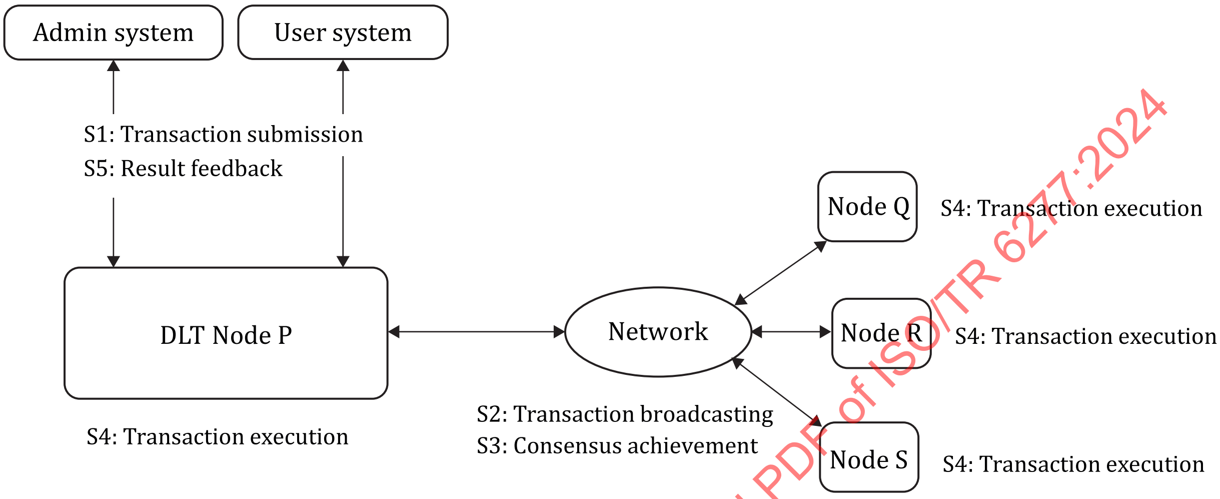

Admin system
User system
S1: Transaction submission
S5: Result feedback
DLT Node P
S4: Transaction execution
Network
S2: Transaction broadcasting
S3: Consensus achievement
Node Q
S4: Transaction execution
Node R
S4: Transaction execution
Node S
S4: Transaction execution

Figure 5 — Illustration of transaction implementation

6.2.2.2 S1: Transaction submission

A user utilizes the corresponding interface to interact with the DLT system and initiates a transaction with or without smart contract.

- Data transmission: the transaction initiation message is submitted by user, which contains transaction content, e.g. sender/receiver account identity, and business information. The business information can be digital asset amount, or parameters to call smart contract.
- Data creation: transaction data submitted by user is recorded on ledger.

6.2.2.3 S2: Transaction broadcasting

A node which receives initiation message verifies the message by checking message format, account identity validity, double spending, signature, etc. If this transaction message is valid, it is sent to other distributed nodes within the given DLT network. Subsequently, other distributed nodes verify the received message independently and buffer it.

- Data processing: the transaction content is verified per node.
- Data transmission: the transaction content is transmitted among distributed nodes within DLT network.
- Data storage: the transaction content is buffered per node.

6.2.2.4 S3: Consensus achievement

The consensus protocol is performed among nodes to determine the execution order of transactions.

- Data creation: interactive messages to determine the execution order are created.

- Data transmission: interactive messages are communicated among distributed nodes according to the implemented consensus protocol.
- Data storage: the execution order is stored per node.

6.2.2.5 S4: Transaction execution

Each node independently executes transactions based on the agreed order.

- Data processing: the data, e.g. business information, archived blocks, account data, smart contract data are processed according to the pre-defined computation rules. Optionally, after computation, the account data and smart contract data are updated accordingly.
- Data creation: receipt data are generated. Optionally, new smart contract data and event data are generated.
- Data storage: the transaction content and receipt data are archived in the confirmed blocks. The smart contract data and event data are consistently stored at distributed nodes.

6.2.2.6 S5: Result feedback

The receipt data are transmitted to the user who initiates the transaction. Optionally, the event data are transmitted to the subscribed users.

- Data creation: log data to record node operation is generated, including event distribution.
- Data storage: the log data are stored per node.

Similarly, the administer can call system-level smart contract and utilize the above procedure to update the administrator data and operation data.

6.2.3 Overview of data process within DLT system

The overview of data process with DLT system is illustrated in Table 1.

Table 1 — Overview of data process within DLT system

Transaction stages	Data actions			
	Data creation	**Data storage**	**Data processing**	**Data transmission**
DLT system setup	Operation data and access authentication data are created by DLT developer and provider	Operation data and access authentication data are stored consistently among multiple nodes		
User account registration	User account data are created	User account data are stored at distributed nodes		
S1: Transaction submission	Transaction data are created	Transaction data are buffered at the received node		Transaction initiation message is submitted by user
S2: Transaction validation and transmission		Transaction data are buffered at distributed nodes	Transaction data are validated	Transaction data are broadcast
S3: Consensus achievement	Interactive messages to determine the execution order are created	Interactive messages are communicated among multiple nodes		
S4: Transaction Execution	Receipt data are generated Operation data are generated/created		Transaction data are processed, and archived in the confirmed block	
S5: Result notification				The receipt data are fed back to the user/admin

7 Inter-system data flow

7.1 Data flows between DLT system and DLT system

7.1.1 Outline

One transaction implementation is illustrated in Figure 6.

- S1: Transaction submission. The transaction message is submitted by user or admin system. If it is submitted by user, this message can be viewed as data flow D. Otherwise, it is data flow C.

- S2: Transaction execution with eventual consistency. The message is validated and executed, and finally eventual consistency is achieved between two DLT systems, which corresponds to data flow A. Eventual consistency means the corresponding operation is either successfully executed or failed for both DLT systems.

- S3: Result feedback. The result is sent back to user or admin system. If it is submitted by user, this message can be viewed as data flow D. Otherwise, it is data flow C. Optionally, the other DLT system can send notification of result to the user/admin depending on practical implementation.

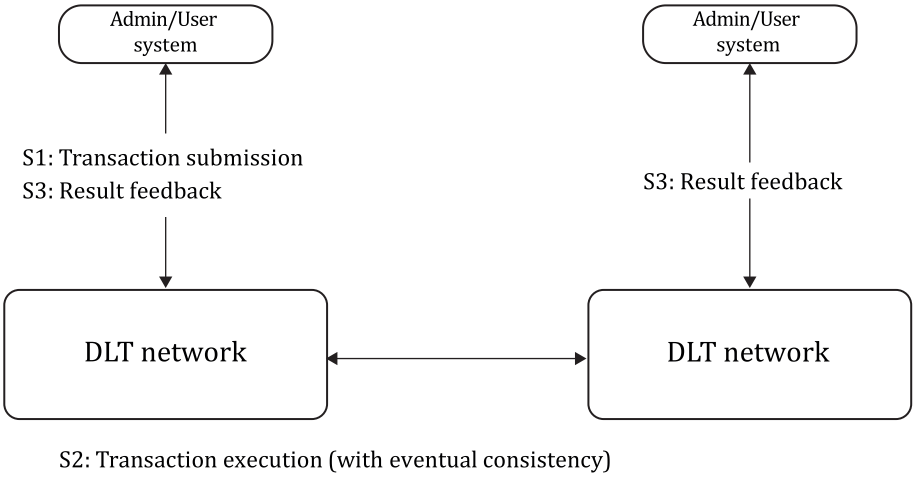


Figure 6 — Illustration of transaction implementation

7.1.2 Transaction submission

The user utilizes the corresponding interface to interactive with DLT system and initiates a transaction with or without smart contract.

- Data transmission: the transaction initiation message is submitted by user. Besides elements within DLT scenario, the message contains additional source DLT and target DLT information.
- Data creation: transaction data submitted by the user is created.

7.1.3 Transaction execution with eventual consistency

From a transactional point of view, one transaction can be divided into two subtransactions. They are executed dependently at two DLT systems with intermediate information exchange. The transaction is either successful or failed synchronously at two DLT systems. For example, inter-chain asset exchange means that after the assets are destroyed (or frozen) in the first DLT system, then the second blockchain will eventually issue the same number of assets.

- Data processing: the data, e.g. business information, smart contract data are processed according to the pre-defined computation rules. The data of two DLT systems can be sequentially or recursively operated. Optionally, after computation, the account data and smart contract data are updated accordingly.
- Data transmission: interactive messages are communicated between two DLT systems.
- Data creation: new archived blocks and receipt data are generated. Optionally, new smart contract data and event data are generated.
- Data storage: the transaction content and receipt data are archived in the confirmed blocks. The smart contract data and event data are consistently stored with eventual consistency.

7.1.4 Result feedback

The result is fed back to the associated user or admin.

- Data creation: the receipt data are generated, as well as notification message.
- Data transmission: the result is sent back to the user who initiates the transaction. The notification is sent to the subscribed users at two DLT systems.

7.1.5 Overview of data process between DLT system and DLT system

The overview of data process with DLT system is illustrated in Table 2.

Table 2 — Overview of data process between DLT system and DLT system

Transaction stages	Data actions			
	Data creation	Data storage	Data processing	Data transmission
S1: Transaction submission	Transaction initiation message is submitted by user Transaction data are created	The receive DLT network buffers the transaction initiation message		Transaction initiation message is submitted by user
S2: Transaction execution with eventual consistency	The transaction content and receipt data are archived in the confirmed blocks	New archived blocks and receipt data are generated. Optionally, new smart contract data and event data are generated	The data, e.g. business information, smart contract data are processed according to the pre-defined computation rules	Interactive messages are communicated between two DLT systems
S3: Result feedback	The receipt data are generated, as well as notification message.			The result is sent back to the user who initiates the transaction. The notification is sent to the subscribed users at two DLT systems

7.2 Data flows between DLT system and non-DLT system

To some extent, DLT systems are relatively isolated systems which do not obtain data directly from external sources. DLT oracle is the most common way for data exchange between DLT system and non-DLT system. Therefore, this document takes the data flow process using DLT oracles as example for analysing data flow process between DLT system and non-DLT system. The data process of data exchange using DLT oracles mainly includes:

- Data processing: format the external data compatible with the DLT system or validate the data to ensure the data provided to DLT system is correct.
- Data transmission: access external data from web-server, off-chain APIs or IoT devices; exchange processed external data to DLT system.

7.3 Data flow of DID

Decentralized identifier (DID) is a type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g. a person, organization, thing, data model, abstract entity) as determined by the controller of the DID. Each DID document can express cryptographic material, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject. A DID can be resolved to a DID document that contains information associated with the DID.

A DID can be bonded to a person or an organization in the physical world by using verifiable credential (VC) with the same subject. One example of VC is digital educational certificates. Figure 7 illustrates data flows related to VCs using DIDs. The actors of the DID system can request their DIDs on DID applications, the DIDs will be stored on the distributed ledger which acts as verifiable data registry. Another process is for the VC holder to request a VC. The DID issuer can issue a VC for the DID holder and store the VC schema and revocation registry that uses a privacy-preserving mechanism on the distributed ledger. The VC and its linked content can also be stored in an off-ledger database for privacy considerations. In some cases, the DID holder can authorize to verify the VC for proof of identity, age or other attributes for accessing services provided by third party service providers via non-DLT applications.

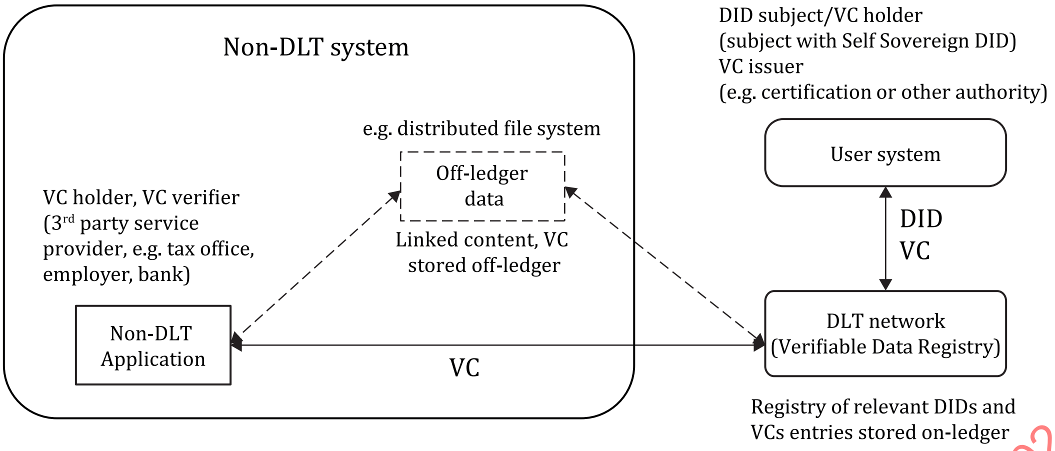

Non-DLT system
e.g. distributed file system
Off-ledger data
Linked content, VC stored off-ledger
VC holder, VC verifier (3rd party service provider, e.g. tax office, employer, bank)
Non-DLT Application
VC
DID subject/VC holder (subject with Self Sovereign DID)
VC issuer (e.g. certification or other authority)
User system
DID
VC
DLT network (Verifiable Data Registry)
Registry of relevant DIDs and VCs entries stored on-ledger

Figure 7 — Example of DID data flow

8 Data flow analysis in DLT use cases

8.1 Overview

For the purpose of clarity and consistency, a strategy similar to that pursued in ISO/TR 3242:2022 DLT use cases was implemented. In order to facilitate the collection of comparable and consistent material for analysis within the descriptive framework and data flow models, a use case descriptor and visualization template was disseminated widely seeking contributions and participation. The template resources are attached in Annex A and further elaborated below.

8.2 Template development

8.2.1 DLT Data flow categories between components and interfaces

Common kinds of interfaces include external interfaces and intersystem interfaces.

Functional components and data flow categories are viewed in the system-view reference architecture described in ISO 23257:2022 and ISO/TR 3242:2022 as illustrated in Figure 8.

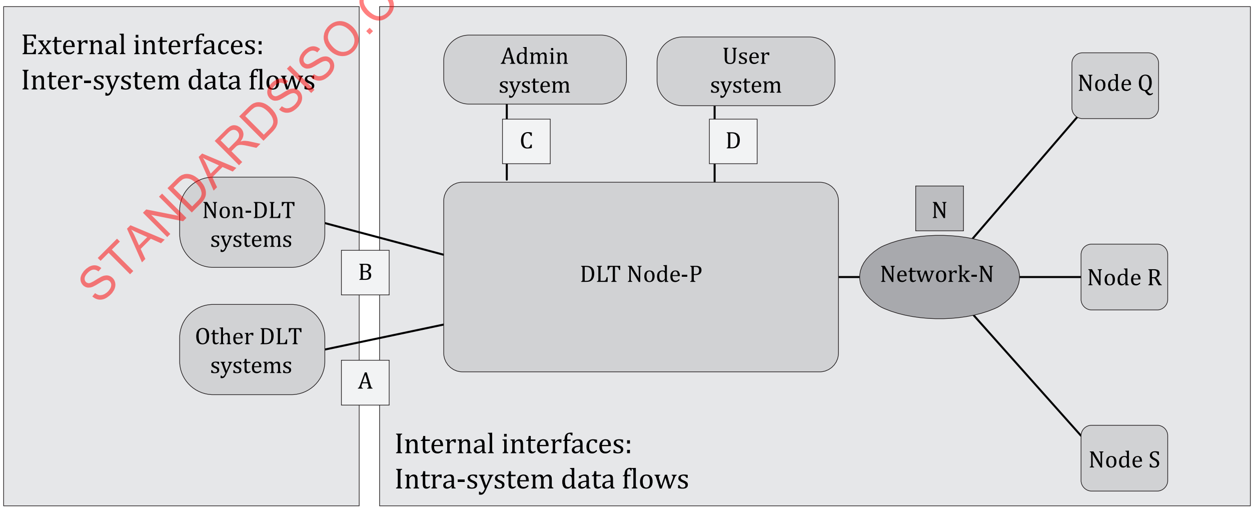


Figure 8 — DLT nodes - Data flow analysis model. Source: ISO/TR 3242:2022

DLT node A with external and inter-system components described:

- C + D: Application systems: for administration and for users, providing end-user capabilities and capabilities for administration and management of the DLT system respectively.
  - Common data identifier categories used here include: subject, object and message data. It is at this point that a more in-depth view of inter-system data-flows can be useful.
- B: Non-DLT systems: off-chain code, the DLT oracles, the non-DLT applications and off-ledger data can be presented and specified based on the actual use case situation.
  - Subject, object, market price, stock, flow and message data will likely all be included here.
- A: Other DLT systems: include the separate DLT systems that interoperate with the DLT system.
  - Subject, object and message identifiers: One purpose for interoperating blockchains is to notarize asset ownership data from one system, perhaps via an exchange, to another system. This is usually information describing a wallet and custody and does not always require owner-as-data-subject detail.
  - Subject data: Another reason can be to provide decentralized identifiers (DIDs) for use in another blockchain systems e.g. Hyperledger Indy to create DIDs, privacy preserving reference identifiers, for system users/data subjects in a primary blockchain system.
  - Market price, stock, flow, message: It is hypothesized that in the future in some sectors e.g. agri-food, that multiple product or commodity blockchains will be available to provide trusted data to other systems. These might include a butter chain, a grassfed chain, an organic food chain that become reference sources (oracle systems) for enterprise supply chain and trade environments. In this view, modelling interoperating blockchains is explicit as well as regional blockchains and permissionless/permissioned protocols. However, a future that presents multiple products or commodity blockchains for ensured data, can be available to any digital enterprise system. There are many examples of market innovation based on DLT ecosystem approaches in the complex eCommerce sector in the Chinese domestic marketplace.
- Multi-layer functions: one or more of the multi-layer function components could be included as per use case situations such as development, management and operations, security and governance and compliance.
  - Further consideration of multi-layer functions can be required.

8.2.2 DLT use case categories

There are five use case categories described in ISO/TR 3242:2022. This document applies the methodology of use case categorization in ISO/TR 3242:2022.

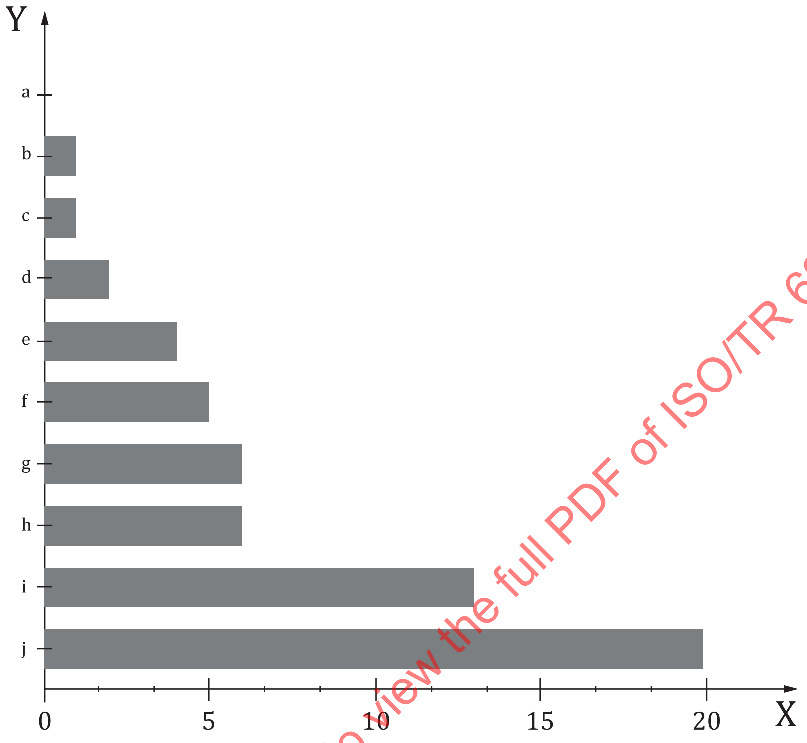
8.2.2.1 Transversal category

See Figure 9.

Key enablers of ICT standardization in the EU ICT rolling plan are:

- Cloud computing
- Public sector information and open data
- Internet of Things
- Cybersecurity/network and information security
- Electronic id, trust services, e-signatures
- e-Privacy

- e-Infrastructures for research
- Accessibility of ICT services
- Artificial intelligence
- 5G
- Broadband infrastructure mapping



Key

X count of transversal category selection across 22 use cases

Y common ICT standardization transversal categories

a 5G.

b AI.

c Cybersecurity/network and information security.

d e-Infrastructures for research.

e e-Privacy.

f Internet of things.

g Accessibility of ICT products and services.

h Cloud computing.

i Public sector information and open data.

j Electronic identification, trust services, e-signatures.

Figure 9 — Spread of use cases presented in ISO/TR 3242:2022 by category 1. Transversal

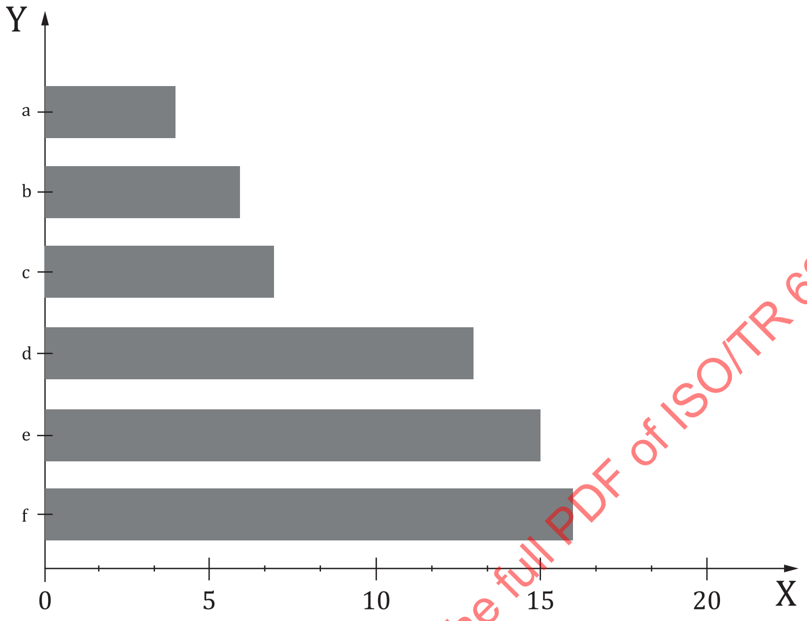
8.2.2.2 Horizontal category

See Figure 10.

Emerging categories of common application and solution domains defined in ISO/TS 23258:2021 are:

- Identity management - Rights and identity management, Identification

- Data provenance - Disintermediation in production, Actions traceability
- Governance - Collaboration, Decision making, structuration
- Cryptocurrency and asset exchange - Electronic payment, Cryptocurrency, Token exchange
- Process optimization - Intellectual property protection, Certification
- Automation - Contract management, Automation



Key

X count of horizontal category selection across 22 use cases

Y utility of blockchain and DLT systems: horizontal categories

[a] Crypto assets and tokenisation.

[b] Governance.

[c] Automation.

[d] Identity management.

[e] Process optimization.

[f] Data provenance.

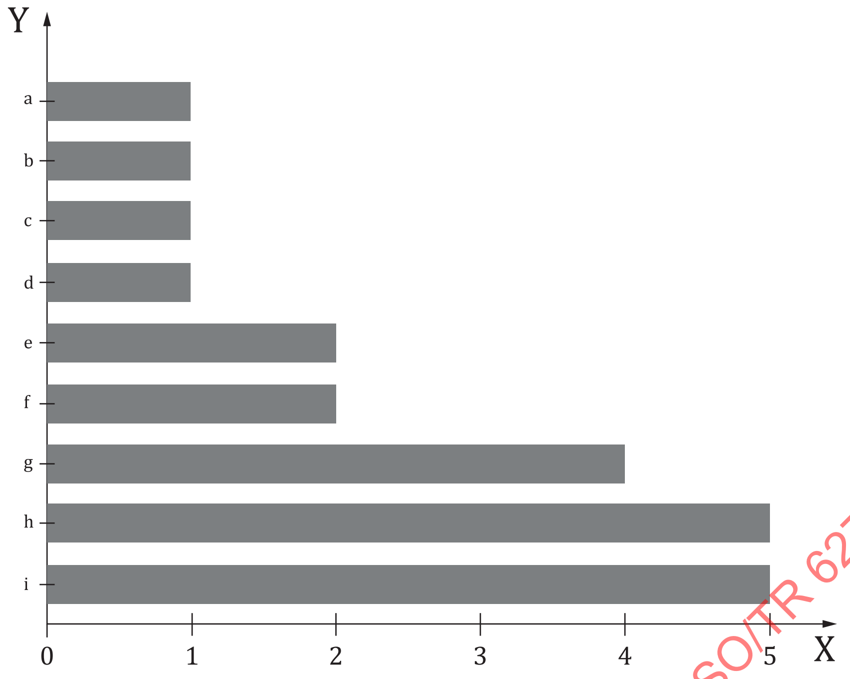
Figure 10 — Spread of use cases presented in ISO/TR 3242:2022 by category 2. Horizontal

8.2.2.3 Vertical category

See Figure 11.

UN International Standard Industrial Classification of All Economic Activities (ISIC) are:

- A (Div. 1-3) = Agriculture, forestry and fishing, through to
- U (Div. 99) = Activities of extraterritorial organizations and bodies.



Key

X count of vertical category selection across 22 use cases

Y ISIC economic activity sections: vertical categories

a Human health and social work activities (Q).

b Education (P).

c Agriculture, forestry and fishing (A).

d Transportation and storage (H).

e Public administration and defence; compulsory social.

f Professional, scientific and technical activities (M).

g Water supply; sewerage, waste management and remediation activities (E).

h Financial and insurance activities (K).

i Information and communication (J).

Figure 11 — Spread of use cases presented in ISO/TR 3242:2022 by category 3. Vertical

8.2.2.4 UN sustainable development goals

There are 17 UN sustainable development goals (SDGs):

- 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

8.2.2.5 Use case status

ISO/TR 3242:2022 defines category of use case status from initial concept through to integration and adoption a) through to i).

- 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.

8.2.3 Data flow description in DLT use cases

8.2.3.1 Relationship between reference architecture and data flow models

From a systematic perspective, data flows are the results of manipulations of stakeholders on DLT system. The user view and system view in ISO 23257:2022 are given as a basis for describing data flows between DLT components and systems.

Data flows can also be regarded as connection between user view which includes a set of roles/subroles with their activities related to the system and system view which includes key functional components and interfaces. Data flows are triggered by specific stakeholders when implementing their activities via interfaces, and they can be demonstrated via system view. An activity can induce more than one data flows. Therefore, analysis of data flows can be focused on different sets of data flows triggered by different activities of stakeholders. From the point of view, data flow analysis can help users and other stakeholders know their data flows when they use certain functions of the system.

Figure 12 gives a description of relationship of reference architecture and data flow models provided in this document. User view is about why and what activities users initiate, while system view is about what and which components or interfaces when activities occur. Data flow model is a bridge of user view and system view which reflexes interaction of users and a DLT system. Actors and their activities in use cases are key elements of user view, which can be described using behavioural UML models and selected for use case descriptive purposes in ISO/TR 3242:2022. Data flow models describe what sets of data flow occur when a certain stakeholder initiates a certain activity. Since data flows frequently happen when a system runs, the analysis can be focused on critical data flows especially the ones significant to users of the DLT system.

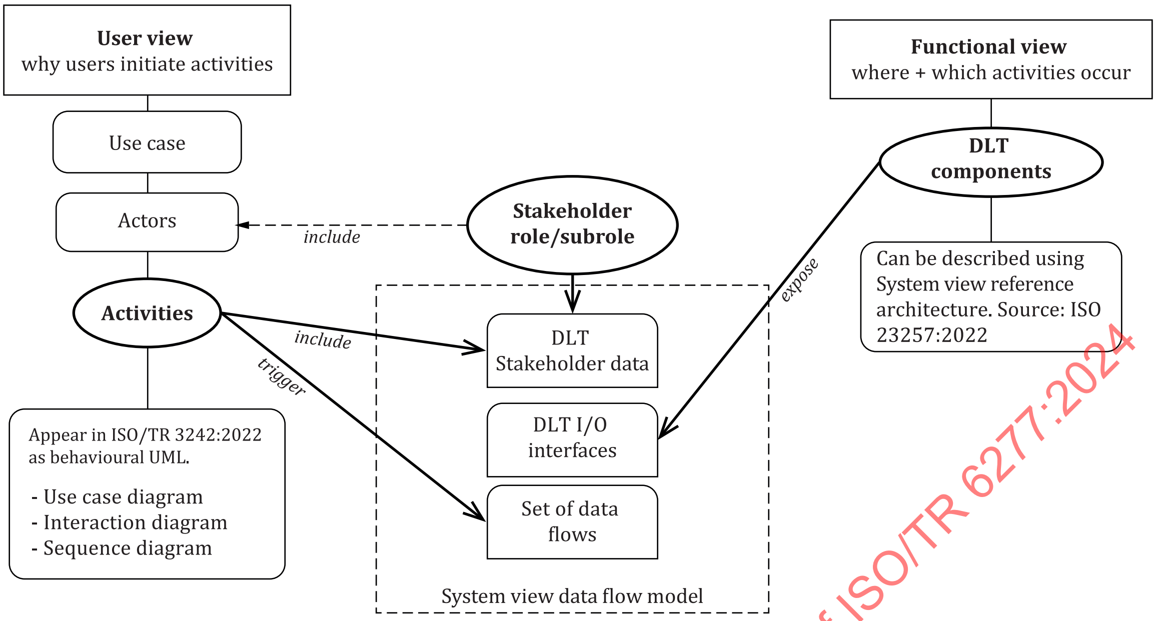


Figure 12 — Relationship between diverse views in DLT data flow models

The process of analyse data flows in DLT use cases are suggested as:

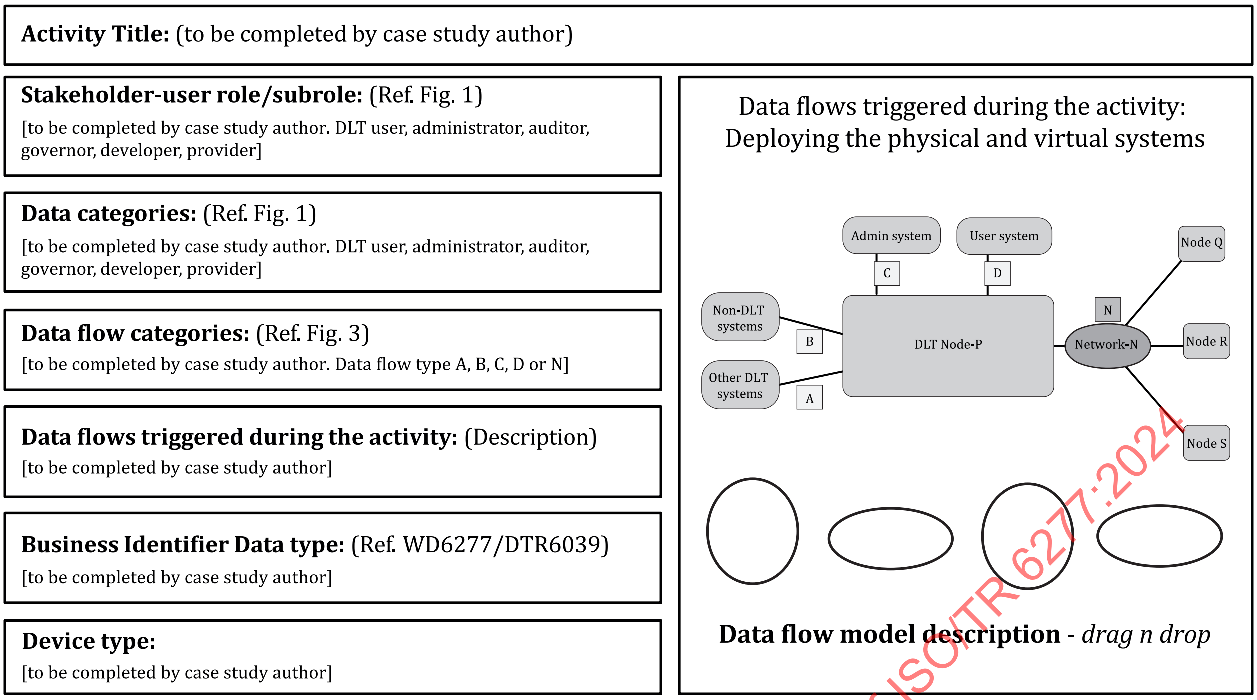
- identifying stakeholders and roles/subroles they act as;
- identifying data types in business level especially data related to users, such as transaction record and smart contract data;
- analysing critical activities of each stakeholder related to data flows;
- identifying data flows triggered by each critical activity, including the data flow type, data type, etc;
- analysing data flow considerations.

8.2.3.2 Data flow description template

The data flow description template includes a table and a set of figures. The critical data flow list (see Table 3) provides general information of critical data flows in a use case. The data flow description card (see Figure 13) provides a visualizing description of each critical data flow.

Table 3 — Critical data flow list: Example

No.	**Activity title**	**Inter or intra sys data flow**	**Stakeholder role**	**Data category**	**Data flow type (A-D, N)**	**Data type**	**Device type**
EXAMPLE *n*	**User activity:** *Create transaction record*	Intra-system	DLT user	Transaction record	D and N	array, timestamp/ entity, event data	Mobile wallet to cloud hosted node



Activity Title: (to be completed by case study author)

Stakeholder-user role/subrole: (Ref. Fig. 1)
[to be completed by case study author. DLT user, administrator, auditor, governor, developer, provider]

Data categories: (Ref. Fig. 1)
[to be completed by case study author. DLT user, administrator, auditor, governor, developer, provider]

Data flow categories: (Ref. Fig. 3)
[to be completed by case study author. Data flow type A, B, C, D or N]

Data flows triggered during the activity: (Description)
[to be completed by case study author]

Business Identifier Data type: (Ref. WD6277/DTR6039)
[to be completed by case study author]

Device type:
[to be completed by case study author]

Data flows triggered during the activity: Deploying the physical and virtual systems

Data flow model description - *drag n drop*

Figure 13 — Data flow description card: unfilled template

8.3 Use case: Insurance service for fish farming

8.3.1 Abstract

Financial service for smart fish farming with blockchain and IoT technology helps to provide effective insurance service for the fish farmers and lower the cost and risks of the insurance compared with the traditional fish farming. It can help to evaluate the insured value of the aquaculture for the insurance company beforehand, lower the risks during the aquaculture, and rapid disposition and compensation of the insured amount. Three types of stakeholders are involved which are fish farmer, insurance company, and aquaculture service provider.

8.3.2 Use case categories

8.3.2.1 Transversal category

- Internet of Things
- Electronic identification, trust services, e-signatures
- Accessibility of ICT products and services
- 5G

8.3.2.2 Horizontal category

- Identity management
- Data provenance
- Cryptocurrency and asset exchange

8.3.2.3 Vertical category

- 0312 Freshwater fishing

8.3.2.4 UN Sustainable development goals

- Good health and well-being
- Sustainable cities and communities

8.3.2.5 Use case status

- A completed trial or pilot

8.3.3 Use case summary

8.3.3.1 Business problem or opportunity

Due to the lack of safe and reliable aquaculture data, it is difficult to control fish farmers' risks of aquaculture.

8.3.3.2 Scale

The use case is mainly used in aquaculture base in Huzhou, Zhejiang province, east of China, which is one of largest freshwater aquaculture base in China. This project is supported by the local government.

8.3.3.3 Objectives

This use case is set to reduce the risks of aquaculture, and to improve the scope and digitalization capability of the insurance business.

8.3.3.4 Stakeholders

Fish farmer, insurance company, and aquaculture service provider.

8.3.3.5 Why distributed ledger technology?

DLT in this use case improves the trustworthiness of the IoT device, ensures reliable and tamperproof data, and boosts the cooperation of the multiple stakeholders among the aquaculture.

8.3.4 Data flow considerations

8.3.4.1 Data security

The aquaculture data are the key references for the financial institutions to determine whether to provide the financial services to fish farmers; thus, the security of aquaculture data is maintained, and the data are not tampered with. So, data security is essential for this case. The cryptography, device authentication, secure communication protocols and DLT technologies are used in this use case to guarantee the data security.

8.3.4.2 Privacy protection

The aquaculture data are only accessible by the fish farmers, aquaculture service providers and authorized financial institutions. The authenticated users are permitted to use the data of aquaculture. Data authentication, privilege management and access control are used for privacy protection.

8.3.5 Visualizations

8.3.5.1 Data categories

In the financial service for smart fish farming use case, the insurance company and the fishing farmer both act as users. Data tightly related to business scenario including transaction record and smart contract data are critical data which are concerned by the DLT users as well as DLT provider. The transaction records are insurance claim settlement data which are stored on DLT ledger to ensure the credibility. Smart contract data are insurance contract data, which can help automatically generating insurance assessment report. See Figure 14.

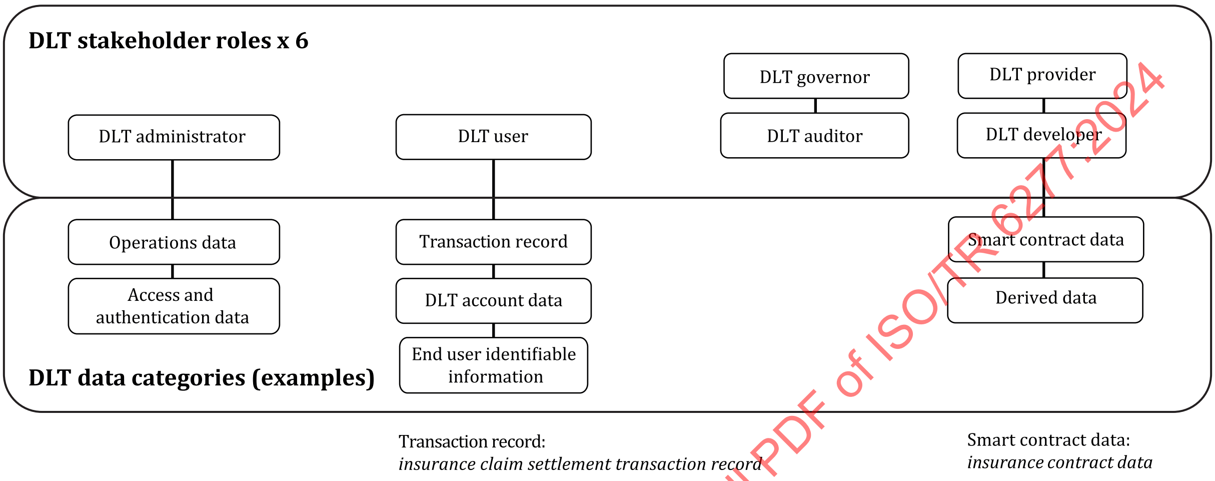


Figure 14 — DLT data categories from the data source perspective: Insurance service for fish farming

8.3.5.2 System view architecture

In the system view architecture, the non-DLT system includes IoT devices, non-DLT platform and off-ledger data. In this use case, the non-DLT platform can be cloud or third-party info platform which provides environmental and market information such as weather and fish price. IoT devices can collect live fishing data and send it to DLT system through API connection. The DLT system provides insurance service portal for the insurance company and fish farmer Apps for the fish farmer. See Figure 15.

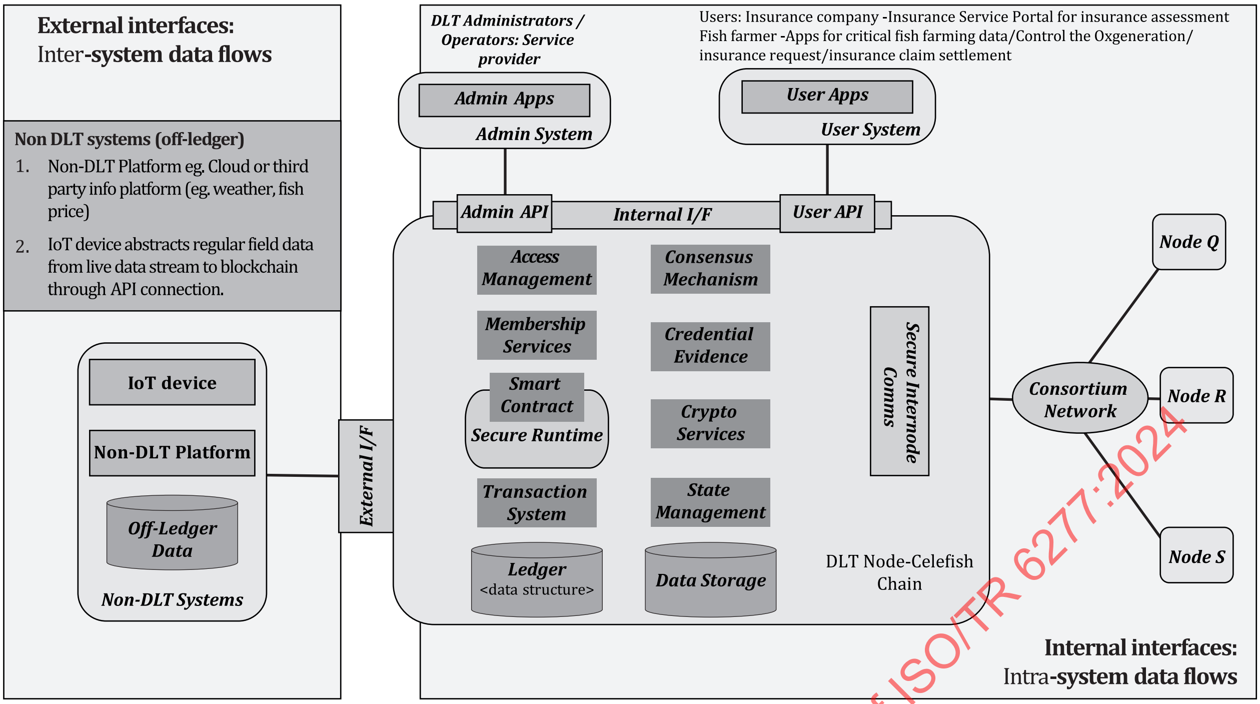


Figure 15 — System view architecture: Insurance service for fish farming

8.3.5.3 Use case diagram

See Figure 16.

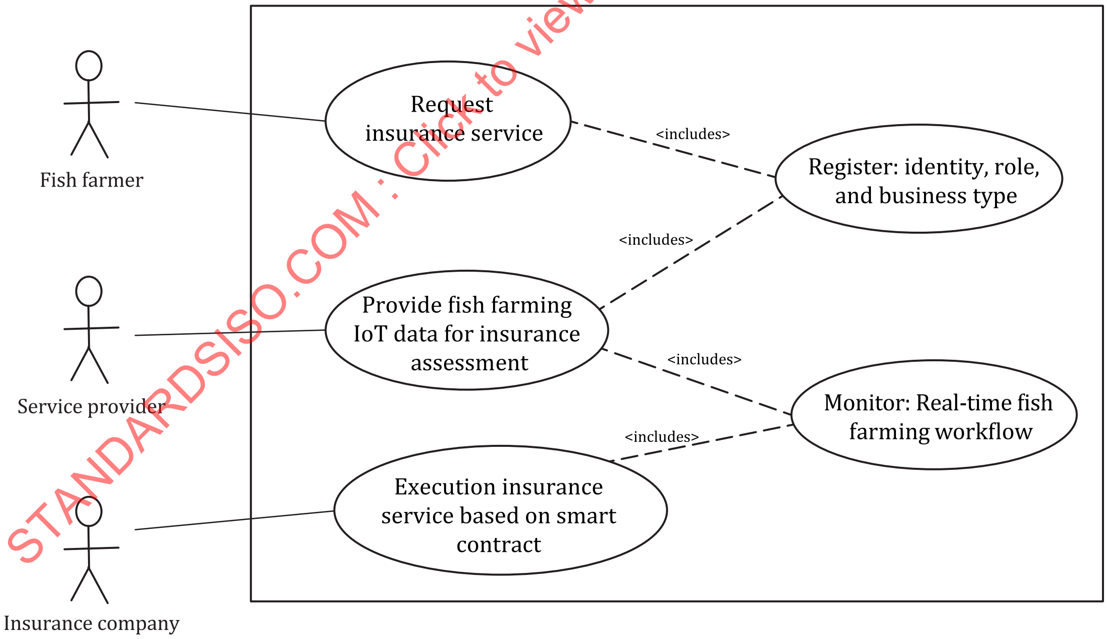

Fish farmer
Service provider
Insurance company
Request insurance service
Register: identity, role, and business type
Provide fish farming IoT data for insurance assessment
Monitor: Real-time fish farming workflow
Execution insurance service based on smart contract
<includes>
<includes>
<includes>
<includes>

Figure 16 — Use case diagram: Insurance service for fish farming

8.3.5.4 Data flow analysis

As shown in Figure 17, there are four fundamental DLT data flows in this use case.

- B: Inter-system data flows. Between Celefish Blockchain DLT node and non-DLT systems (IoT devices and third-party system) connected to it.

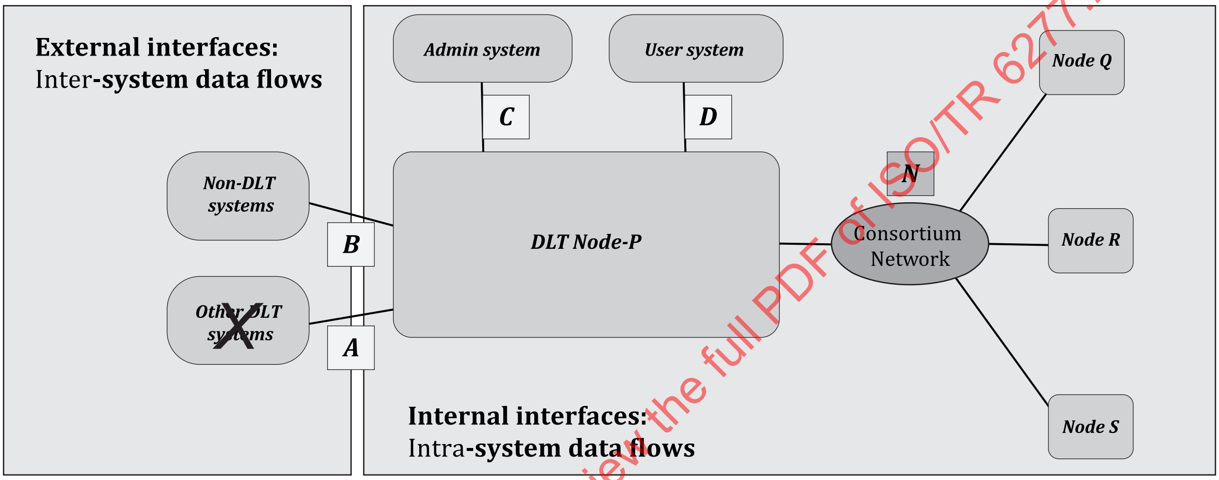
- C: Intra-system data flows. Between administration application system and Celefish Blockchain DLT node.
- D: Intra-system data flows. Between user application system and Celefish Blockchain.
- N: Intra-system data flows. Within and between the nodes of the Celefish Blockchain DLT node.

Different stakeholders such as insurance company, financial department of government agencies, can run different nodes, therefore the N-type data flows can be between nodes owned by different entitles.

B: Non-DLT system
IoT device: Fish farming data flow
Third party information platform: Other fish farming relevant exchangeable data flow

C: Admin system
Service provider- Celefish Technology

D: User system
Fish farmer and insurance company:
Report of insurance assessment
Generate the insurance contract
Execution of insurance claim settlement service
The fish farming record/the operation of oxygenation/feeding automatically



N: Project uses Celefish Blockchain which uses consortium network infrastructure
Nodes are run by insurance companies, blockchain research institutes and financial department of government agencies.

Figure 17 — Data flow category: Insurance service for fish farming

As displayed in Table 4, four critical sets of data flows led by different activities of DLT user and DLT provider are identified in the insurance service for fish farming use case. The single data flow cards are given in Figure 18 to Figure 21.

Table 4 — Critical data flow list: Insurance service for fish farming

No.	Activity title	Inter or intra sys data flow	Stakeholder role	Data category	Data flow type (A-D, N)	Business identifier data types	Device type
1	Create smart contract for fish farming insurance	Intra-system	DLT user and DLT provider	Smart contract data (terms of the smart contract for insurance)	C, D and N	User entity (Access and authentication for DLT user)	Apps, insurance service portal and cloud hosted node
2	Request an insurance service	Intra-system	DLT user/ Fish farmer and insurance company	Insurance claim settlement record	D and N	User entity (Access and authentication for DLT user)	Apps, insurance service portal and cloud hosted node
3	Providing fish farming IoT data for insurance assessment	Inter-system	Service provider/ Celefish	Smart contract data (terms of the smart contract for insurance)	B, D and N	Event record (Weather, fish farming data including the feeding food and water quality which is collected from IoT device)	IoT device, third party platform and cloud hosted node
4	Execution insurance service based on smart contract	Intra-system	DLT user/ Fish farmer and insurance company	Transaction record	D and N	User entity Event record of transfer	Mobile wallet and cloud hosted node

User activity: *Create smart contract for fish farming insurance*

Stakeholder-user role/subrole:

- DLT user/account holder

Data categories:

- Transaction record

Data flow categories:

- Data flow type (C)
- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by *DLT user/Fish farmer* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Data type:

- User entity

Device type:

- Apps
- Insurance service portal
- Cloud hosted node

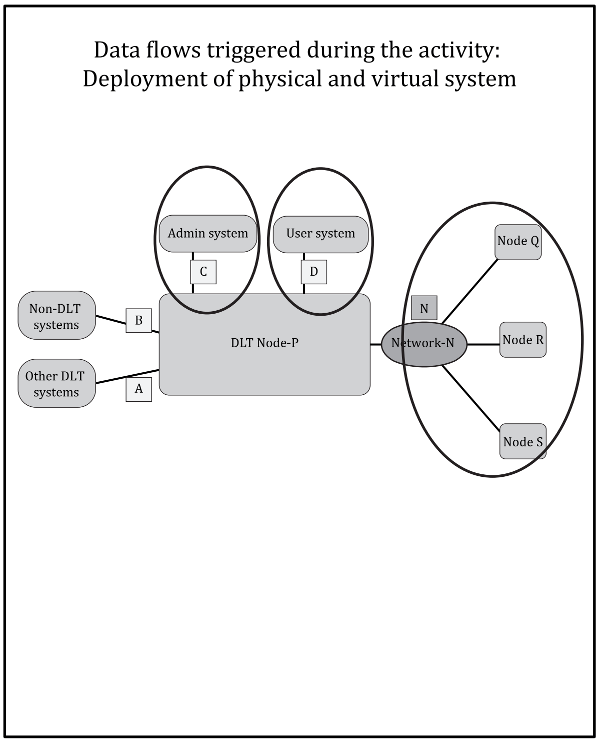

Data flows triggered during the activity:
Deployment of physical and virtual system

Figure 18 — Single data flow analysis card 1: Insurance service for fish farming - Create smart contract for fish farming insurance

User activity: *Request an insurance service*

Stakeholder-user role/subrole:

- DLT user/account holder

Data categories:

- Insurance claim settlement record

Data flow categories:

- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by *DLT user/Fish farmer* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Data type:

- User entity (Access and authentication for DLT user)

Device type:

- Apps
- Insurance service portal
- Cloud hosted node

Data flows triggered during the activity:
Deployment of physical and virtual system

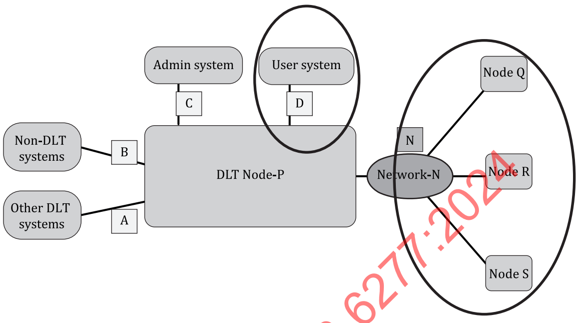


Figure 19 — Single data flow analysis card 2: Insurance service for fish farming - Request an insurance service

User activity: *Providing fish farming IoT data for insurance assessment*

Stakeholder-user role/subrole:

- DLT user/account holder

Data categories:

- Smart contract data (terms of the smart contract for insurance)

Data flow categories:

- Data flow type (B)
- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by*DLT service provider/Celefish* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Data type:

- Event record (Weather, fish farming data including the feeding food and water quality which is collected from IoT device)

Device type:

- IoT device
- Third party platform
- Cloud hosted node

Data flows triggered during the activity:
Deployment of physical and virtual system

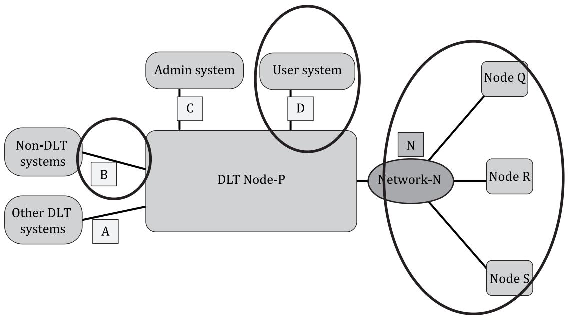


Figure 20 — Single data flow analysis card 3: Insurance service for fish farming - Providing fish farming IoT data for insurance assessment

User activity: *Execution insurance service based on smart contract*

Stakeholder-user role/subrole:

- DLT user/account holder

Data categories:

- Transaction record

Data flow categories:

- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by *DLT user/Insurance company* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Data type:

- User entity
- Event record of transfer

Device type:

- Mobile wallet
- Cloud hosted node

Data flows triggered during the activity:
Deployment of physical and virtual system

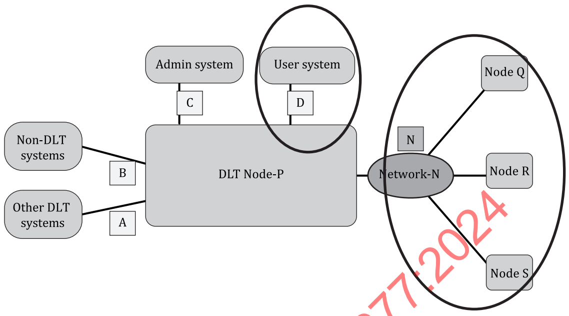


Figure 21 — Single data flow analysis card 4: Insurance service for fish farming - Execution insurance service based on smart contract

8.4 Use case: International trade platform

8.4.1 Abstract

International trade platform is a digital platform for international trade and e-commerce services based on AntChain technologies. It utilizes the blockchain and DLT to connect buyers, sellers, and the third parties in the international trade link, to build the trustworthy relationships and solve financing difficulties. It also provides digital international trade and e-commerce services to facilitate the international trades.

8.4.2 Use case categories

8.4.2.1 Transversal category

— Accessibility of ICT products and services

8.4.2.2 Horizontal category

— Data provenance

— Process optimization

8.4.2.3 Vertical category

— G. Wholesale and retail trade

8.4.2.4 UN Sustainable development goals

— No poverty

— Affordable and clean energy

- Decent work and economic growth

8.4.2.5 Use case status

- An integration with current systems

8.4.3 Use case summary

8.4.3.1 Business problem or opportunity

- To introduce more certainty and trust in international trade by digitalizing the trade value chain.
- To decrease the overall costs in the trade process for all participants, with increased efficiency.
- To provide SME buyers and suppliers with more financial services.

8.4.3.2 Scale

International.

8.4.3.3 Objectives

- Connect to trade marketplaces to acquire more customers and business opportunities.
- Co-create the next generation trade network to serve global SMEs with AntChain technologies.
- Mitigate uncertainties and risks with traceable trade data and deliver inclusive financial services.

8.4.3.4 Stakeholders

- DLT administrator: service provider
- Users: buyers, sellers, the third parties

8.4.3.5 Why distributed ledger technology?

The smart contracts are written and executed according to the terms of the order between the buyer and the seller, so that the execution rules are transparent and traceable among authorized parties. Key proof information, such as bill of lading, customs declaration, will be achieved in the DLT system, which can be shared to the authorized parties. Payment based on smart contract improves efficiency and greatly shortens the money collection time of small and medium-sized sellers.

8.4.4 Data flow considerations

8.4.4.1 Data security

This use case utilizes the following techniques to ensure data security:

- Data encryption methods to prevent sensitive data from being snooped by other data providers, platform and users.
- Transmission of messages only among specific authorized nodes.
- Secure transmission that ensures transferred data will not be intercepted or tampered with.
- Secure storage of sensitive assets that ensures confidentiality and availability of data.
- Data authentication methods so that the integrity of computation results can be verified.

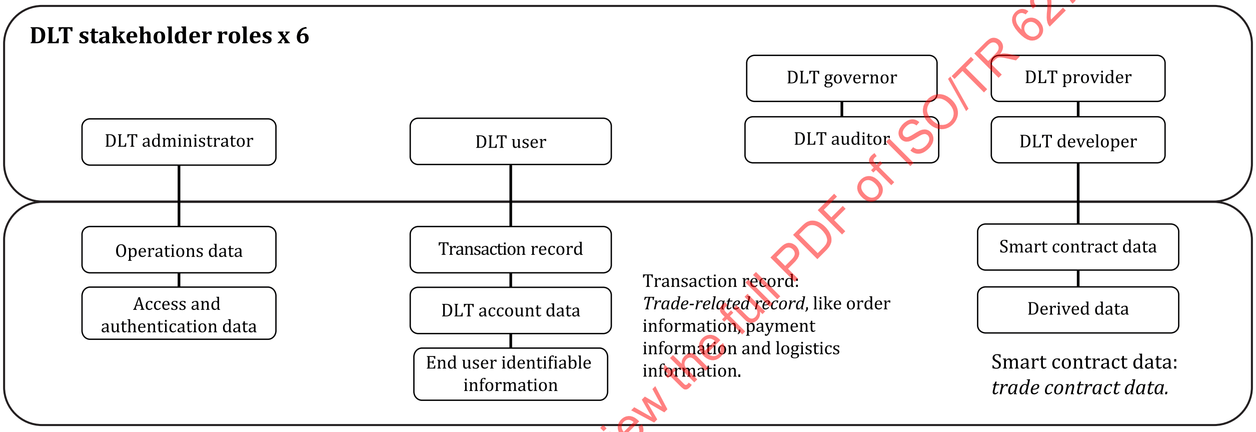
8.4.4.2 Privacy protection

In this use case, collaborators of cross-border trade are distributed in many countries and regions around the world, thus privacy protection is significant both in policy and technical facet. To meet the compliance requirements of data privacy in many countries and regions, through the settings of roles and permissions of each participant and configuring the smart contract to run in secure execution environment, the core data in the platform is visible only within the scope of authorization.

8.4.5 Visualizations

8.4.5.1 Data categories

Data tightly related to business scenario including transaction record and smart contract data are critical data which are concerned by the DLT users as well as DLT provider. The transaction records are trade-related data on order, payment, logistics and other information. Smart contract data are trade contract data, which can support high-efficiency payment. See Figure 22.



DLT stakeholder roles x 6
DLT governor
DLT provider
DLT administrator
DLT user
DLT auditor
DLT developer
Operations data
Transaction record
Smart contract data
Access and authentication data
DLT account data
Derived data
End user identifiable information
Transaction record: *Trade-related record*, like order information, payment information and logistics information.
Smart contract data: *trade contract data.*

Figure 22 — DLT data categories from the data source perspective: International trade platform

8.4.5.2 System view architecture

See Figure 23.

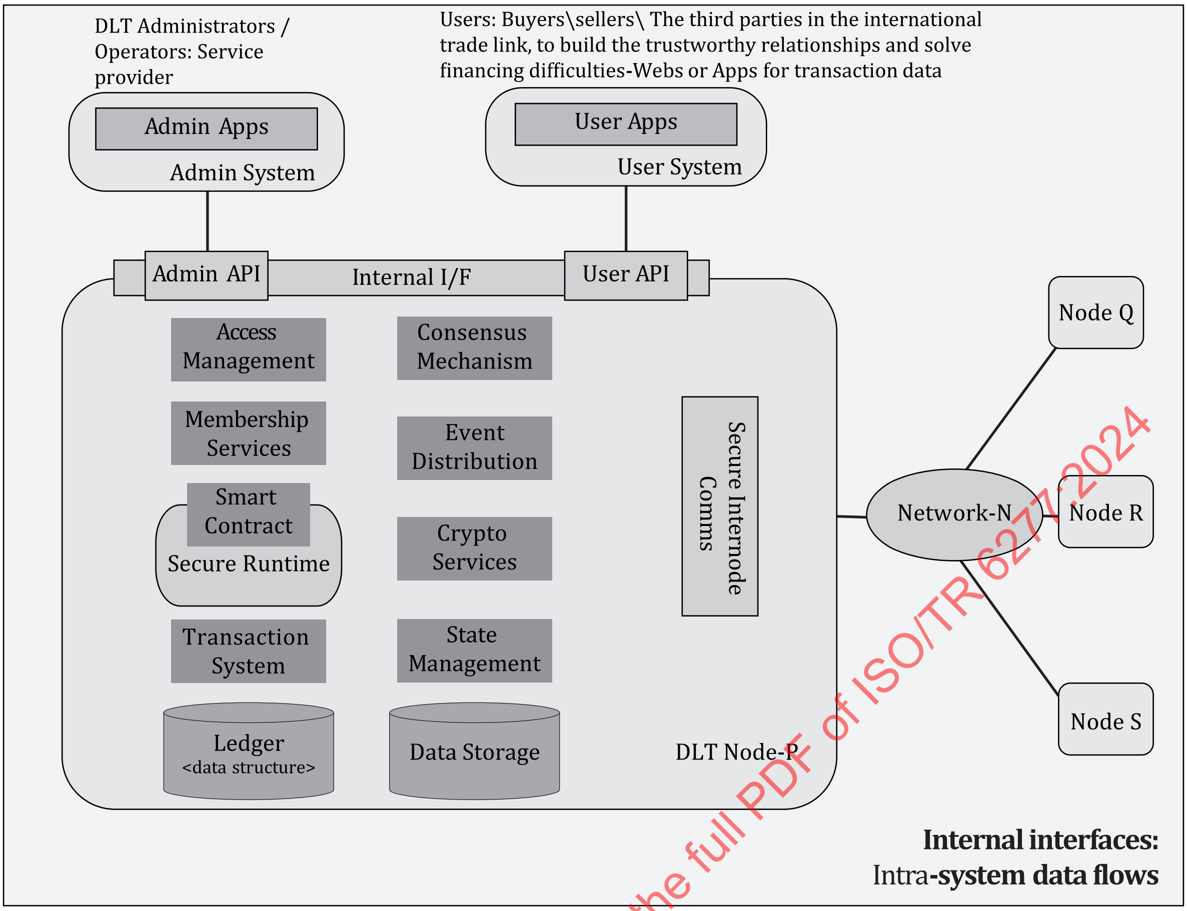


Figure 23 — System view architecture: International trade platform

8.4.5.3 Use case diagram

See Figure 24.

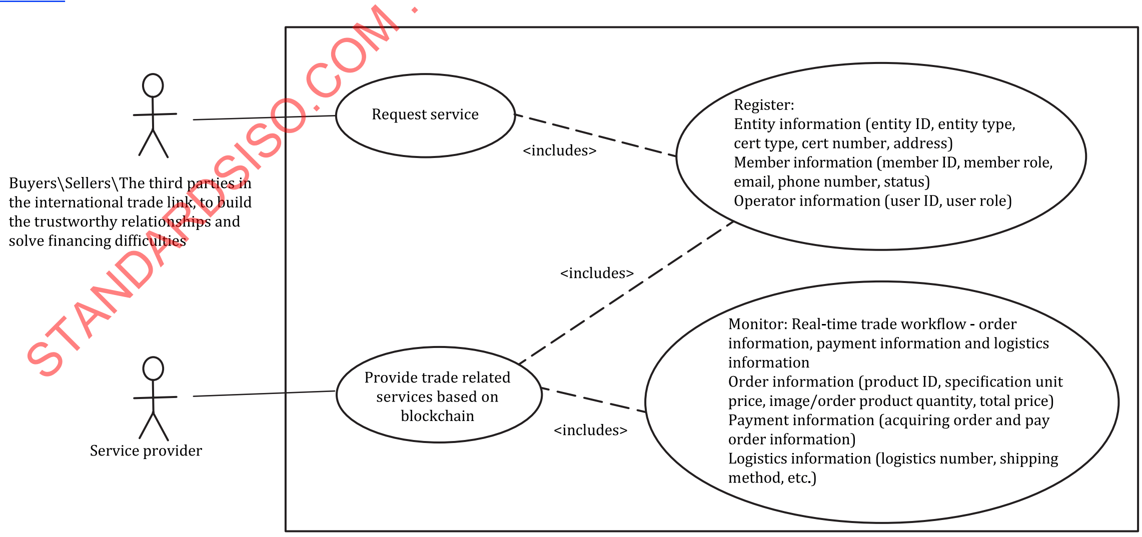

Buyers\Sellers\The third parties in the international trade link, to build the trustworthy relationships and solve financing difficulties
Service provider
Request service
<includes>
Register:
Entity information (entity ID, entity type, cert type, cert number, address)
Member information (member ID, member role, email, phone number, status)
Operator information (user ID, user role)
<includes>
Provide trade related services based on blockchain
<includes>
Monitor: Real-time trade workflow - order information, payment information and logistics information
Order information (product ID, specification unit price, image/order product quantity, total price)
Payment information (acquiring order and pay order information)
Logistics information (logistics number, shipping method, etc.)

Figure 24 — Use case diagram: International trade platform

8.4.5.4 Data flow analysis

As shown in Figure 25, there are three types of intra-system DLT data flows in this use case.

- Data flow type C: Between administration system and nodes of the international trade platform.
- Data flow type D: Between user system and nodes of the international trade platform.
- Data flow type N: Within and between the nodes of the international trade platform. Different nodes are run by merchant users, blockchain companies and financial department of government agencies.

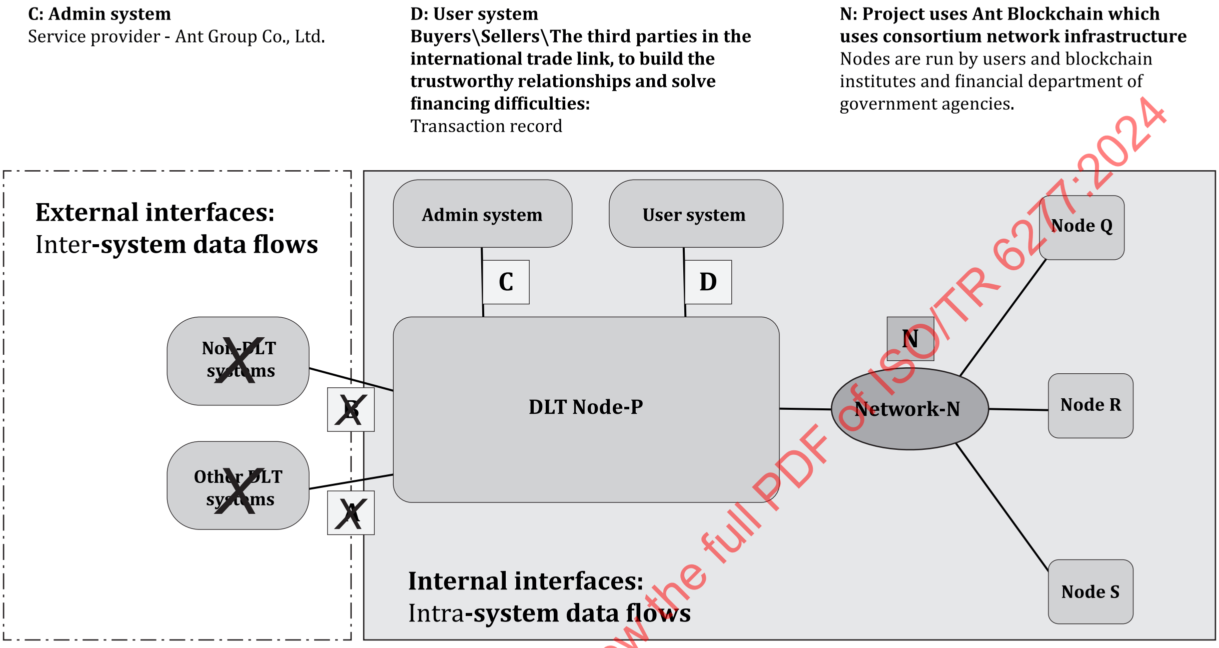

C: Admin system
Service provider - Ant Group Co., Ltd.
D: User system
Buyers\Sellers\The third parties in the international trade link, to build the trustworthy relationships and solve financing difficulties:
Transaction record
N: Project uses Ant Blockchain which uses consortium network infrastructure
Nodes are run by users and blockchain institutes and financial department of government agencies.
External interfaces:
Inter-system data flows
Non-DLT systems
Other DLT systems
B
A
Admin system
User system
C
D
DLT Node-P
N
Network-N
Node Q
Node R
Node S
Internal interfaces:
Intra-system data flows

Figure 25 — Data flow category: International trade platform

As displayed in Table 5, three critical sets of data flows led by different activities of DLT user and DLT provider are identified in the international trade platform use case. The single data flow cards are given in Figure 26 to Figure 28.

Table 5 — Critical data flow list: International trade platform

No.	Title	Inter or intra sys data flow	Stakeholder role	Data category	Data flow type	Business identifier data types	Device type
1	Create smart contract for trade service	Intra-system	DLT user and service provider	Smart contract data (terms of the smart contract for trade)	C, D and N	User entity (Access and authentication for DLT user)—— [Entity information(entity ID, entity type, cert type, cert number, address) Member information(member ID, member role, email, phone number, status) Operator information(user ID, user role)]	Apps/ Webs, Nodes
2	Request a trade-related service	Intra-system	DLT user/Buyers, Sellers, The third parties in the international trade link, to build the trustworthy relationships and solve financing difficulties	Trade-related claim settlement record	C, D and N	User entity (Access and authentication for DLT user)—— [Entity information(entity ID, entity type, cert type, cert number, address) Member information(member ID, member role, email, phone number, status) Operator information(user ID, user role)]	Apps/ Webs, Node
3	Execution trade-related service based on smart contract	Intra-system	Service provider	Transaction record	D and N	User entity Event record of transfer—— [Order information (product ID, specification unit price, image/ order product quantity, total price) Payment information (acquiring order and pay order information) Logistics information (logistics number, shipping method, etc.)]	Node

Activity Title: Create smart contract for trade service

Stakeholder-user role/sub role:

- DLT user and service provider

Data categories:

- Smart contract data (terms of the smart contract for trade)

Data flow categories:

- Data flow type (C)
- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by service provider on **Node-P** (C)
- Transaction record created by DLT user on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Identifier Data type:

- User entity

Device type:

- Apps/Webs> Node

Data flows triggered during the activity:
Deploying the physical and virtual systems

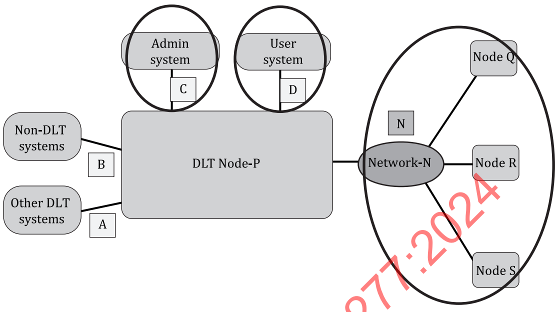


Figure 26 — Single data flow analysis card 1: International trade platform - Create smart contract for trade service

Activity Title: Request a trade-related service

Stakeholder-user role/sub role:

- DLT user

Data categories:

- Trade-related claim settlement record

Data flow categories:

- Data flow type (C)
- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by service provider on **Node-P** (C)
- Transaction record created by DLT *user/Fishfarmer* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Identifier Data type:

- User entity

Device type:

- Apps/Webs> Node

Data flows triggered during the activity:
Deploying the physical and virtual system

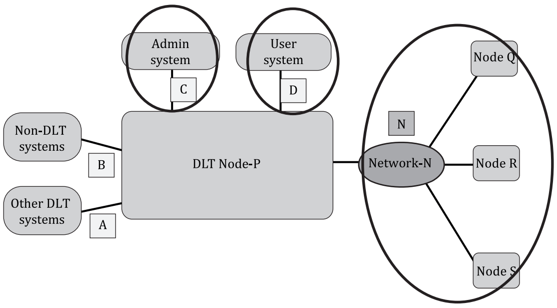


Figure 27 — Single data flow analysis card 2: International trade platform - Request a trade-related service

Activity Title: Execution trade-related service based on smart contract

Stakeholder-user role/sub role:

- Service provider

Data categories:

- Transaction record

Data flow categories:

- Data flow type (D)
- Data flow type (N)

Data flows triggered during the activity:

- Transaction record created by *DLT user company* on **Node-P** (D)
- Transaction record data are then broadcast and stored consistently across the **Network-N** (N)

Business Identifier Data type:

- User entity
- Event record of transfer

Device type:

- Node

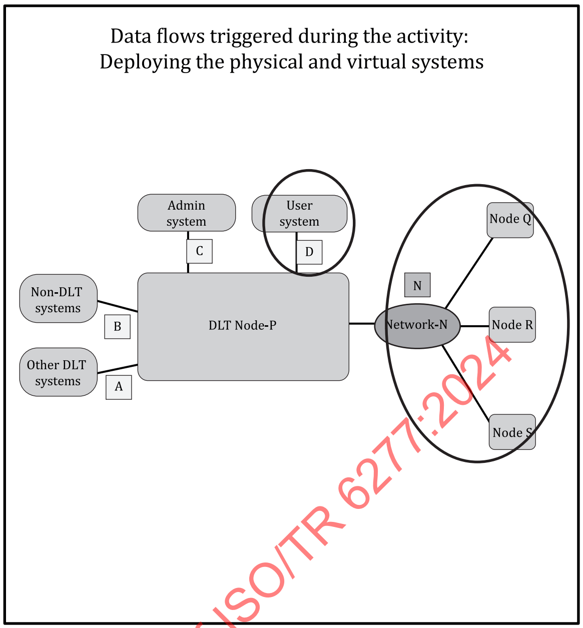


Figure 28 — Single data flow analysis card 2: International trade platform - Execution trade-related service based on smart contract

8.5 Use case: Peer-to-peer metaverse traveller network

8.5.1 Abstract

A metaverse traveller (MT) is an individual who seeks to co-create a bespoke travel experience and commissions a real world traveller (RT) to create and share the desired content, transferring the content to the MT on demand basis. Their interactions are facilitated with a purpose-built smart contract system.

The project presents a hybrid peer-to-peer computing infrastructure with edge networks and proposes a partnership with Valladolid Data Centre, enabling peer nodes to compute directly with servers and/or other peers in diverse or same edge networks. This enablement provides stable and high-performance computing power and big data transmission. This process is referred to as “KRON Computing” herein. This use case presents one use case for contract management.

The metaverse traveller (MT) requests the content creator, real world traveller (RT), to create the content based on the smart contact policy by posting the buy request on the omni communication channel website, Owake.Me. Omni-communication relates to the neologic omni-digital strategy to provide consistent customer experiences across every digital interface for a brand or business. Omni-communication is the technical abstraction of the work of manual integration on the part of individual users or customers. In this case, the KRON system offers automatic self-service integration with prepared API connectivity.

- The MT can specify the content requirement related to, include but not limited to, Location, Time, Content creating device (smart phone or digital camera or sensors or any other type of device), Creator, Storage, Delivery, Token, Payment, Data, encryption, Buyer, Address, RWA, Warrant, Representation, Promise, Content, Amount, Signature, Transfer Device, and Network. (Terms and conditions)
- e.g.: The MT wishes to visit Leon in Spain right now.
- Thus, the MT requested the creator whoever lives in Leon Area to take the live video in real time and sell to the buyer the live video with 100 Euros in Owake.Me website.
- The RT who saw this request in Owake.Me wants to go into the contract and provides the live video service.

- The MT and the RT sign the smart contract with certain condition and terms.
- The RT broadcasts or transfers the non-fungible tokenized live video content as contracted with MT.
- The content is transmitted fully and the entitlement transferred from the RT to the MT as contracted.

8.5.2 Use case categories

8.5.2.1 Transversal category

- Internet of Things
- Electronic identification, trust services, e-signatures
- Accessibility of ICT products and services
- 5G

8.5.2.2 Horizontal category

- Identity management
- Data provenance
- Process optimization
- Automation

8.5.2.3 Vertical category

- R9329 Other amusement and recreation activities n.e.c.

Section: R Arts, entertainment and recreation

Division: 93 Sports activities and amusement and recreation activities

Group: 932 Other amusement and recreation activities

Class: 9329 Other amusement and recreation activities n.e.c.

8.5.2.4 UN Sustainable development goals

- GOAL 8: Decent work and economic growth
- GOAL 9: Industry, innovation and infrastructure
- GOAL 10: Reduced inequality
- GOAL 12: Responsible consumption and production
- GOAL 17: Partnerships to achieve the goal

8.5.2.5 Use case status

- A completed trial or pilot