ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.751.10 (09/2023)

SERIES F: Non-telephone telecommunication services

Multimedia services

Framework and requirements for distributed ledger technology (DLT)-based digital collection services

ITU-T F-SERIES RECOMMENDATIONS

Non-telephone telecommunication services

TELEGRAPH SERVICE	F.1-F.109
Operating methods for the international public telegram service	F.1-F.19
The gentex network	F.20-F.29
Message switching	F.30-F.39
The international telemessage service	F.40-F.58
The international telex service	F.59-F.89
Statistics and publications on international telegraph services	F.90-F.99
Scheduled and leased communication services	F.100-F.104
Phototelegraph service	F.105-F.109
MOBILE SERVICE	F.110-F.159
Mobile services and multidestination satellite services	F.110-F.159
TELEMATIC SERVICES	F.160-F.399
Public facsimile service	F.160-F.199
Teletex service	F.200-F.299
Videotex service	F.300-F.349
General provisions for telematic services	F.350-F.399
MESSAGE HANDLING SERVICES	F.400-F.499
DIRECTORY SERVICES	F.500-F.549
DOCUMENT COMMUNICATION	F.550-F.599
Document communication	F.550-F.579
Programming communication interfaces	F.580-F.599
DATA TRANSMISSION SERVICES	F.600-F.699
MULTIMEDIA SERVICES	**F.700-F.799**
ISDN SERVICES	F.800-F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850-F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900-F.999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T F.751.10

Framework and requirements for distributed ledger technology (DLT)-based digital collection services

Summary

DLT-based digital collection services are provided by distributed ledger technology (DLT) systems to perform various operations on digital collections, including issuance, sale, purchase, auction, transaction, transfer, etc.

Recommendation ITU-T F.751.10 specifies a framework and requirements for DLT-based digital collection services, and may be used to guide the DLT-based digital collection services.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.751.10	2023-09-13	16	11.1002/1000/15624

Keywords

Digital collection service, distributed ledger technology, framework and requirements.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T F.751.10

Framework and requirements for distributed ledger technology (DLT)-based digital collection services

1 Scope

This Recommendation specifies a framework and requirements for DLT-based digital collection services. It includes the overall architecture, information flows and functional requirements for DLT-based digital collection services.

This Recommendation may be used as guidance by the relevant parties to research, develop, test, deploy and manage the DLT-based digital collection services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.751.2] Recommendation ITU-T F.751.2 (2020), *Reference framework for distributed ledger technologies*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 account [b-ITU-T F.751.1]: Representation of an entity whose data is recorded on a distributed ledger.

3.1.2 asset [b-ITU-T F.751.0]: A representation of value. It can be a diamond, a unit of currency, items inside a shipping container, etc. An asset can be physical or virtual.

3.1.3 consensus [b-ITU-T F.751.0]: Agreement that a set of transactions is valid.

3.1.4 distributed ledger [b-ISO 22739]: A ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism.

3.1.5 distributed ledger technology (DLT) [b-ITU-T F.751.1]: Technology enabling large groups of nodes in distributed ledger networks to reach agreement and record information without the need for a central authority.

3.1.6 ledger [b-ITU-T F.751.0]: Information store that keeps final and definitive (immutable) records of transactions.

3.1.7 node [b-ITU-T F.751.0]: Device or process that participates in a distributed ledger network.

3.1.8 private distributed ledger technology system [b-ISO 22739]: DLT system that is accessible for use only to a limited group of DLT users.

3.1.9 smart contract [b-ITU-T F.751.0]: Program written on the distributed ledger system that encodes the rules for specific types of distributed ledger system transactions in a way that can be validated and triggered by specific conditions.

3.1.10 transaction [b-ITU-T F.751.0]: An incident or an operation that leads to a change in the status of a ledger, such as adding a record or equivalent exchange based on currency.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 DLT-based digital collection: Digital collection generated and issued by a private distributed ledger technology (DLT) system, which is non-fungible and has a unique identifier.

3.2.2 DLT-based digital collection service: Digital collection service provided by a private distributed ledger technology (DLT) system, which can use a private DLT platform to perform various operations on digital collections, including issuance, sale, purchase, auction, transaction, transfer, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DCS Digital Collection Service

DDoS Distributed Denial of Service

DLT Distributed Ledger Technology

P2P Peer-to-Peer

PKI Public Key Infrastructure

SDK Software Development Kit

5 Conventions

In this Recommendation:

– The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

– The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

DLT-based digital collections are generated and issued by private distributed ledger technology (DLT) systems. They are non-fungible, and each has a unique identifier. They can only be owned by the DLT users who have passed an identity authentication. DLT-based digital collections are indivisible, unchangeable, and verifiable.

DLT-based digital collections use DLT to indicate the ownership of a certain digital collection. DLT can mark the owner of the digital collection in the DLT network. DLT-based digital collections are indivisible, unique, and the values are not equal. DLT can be used to support the issuance, circulation, management, and other functions of digital collections.

7 Overall architecture

7.1 Architecture of the DLT-based digital collection service system

The overall architecture of DLT-based digital collection services is shown in Figure 1.

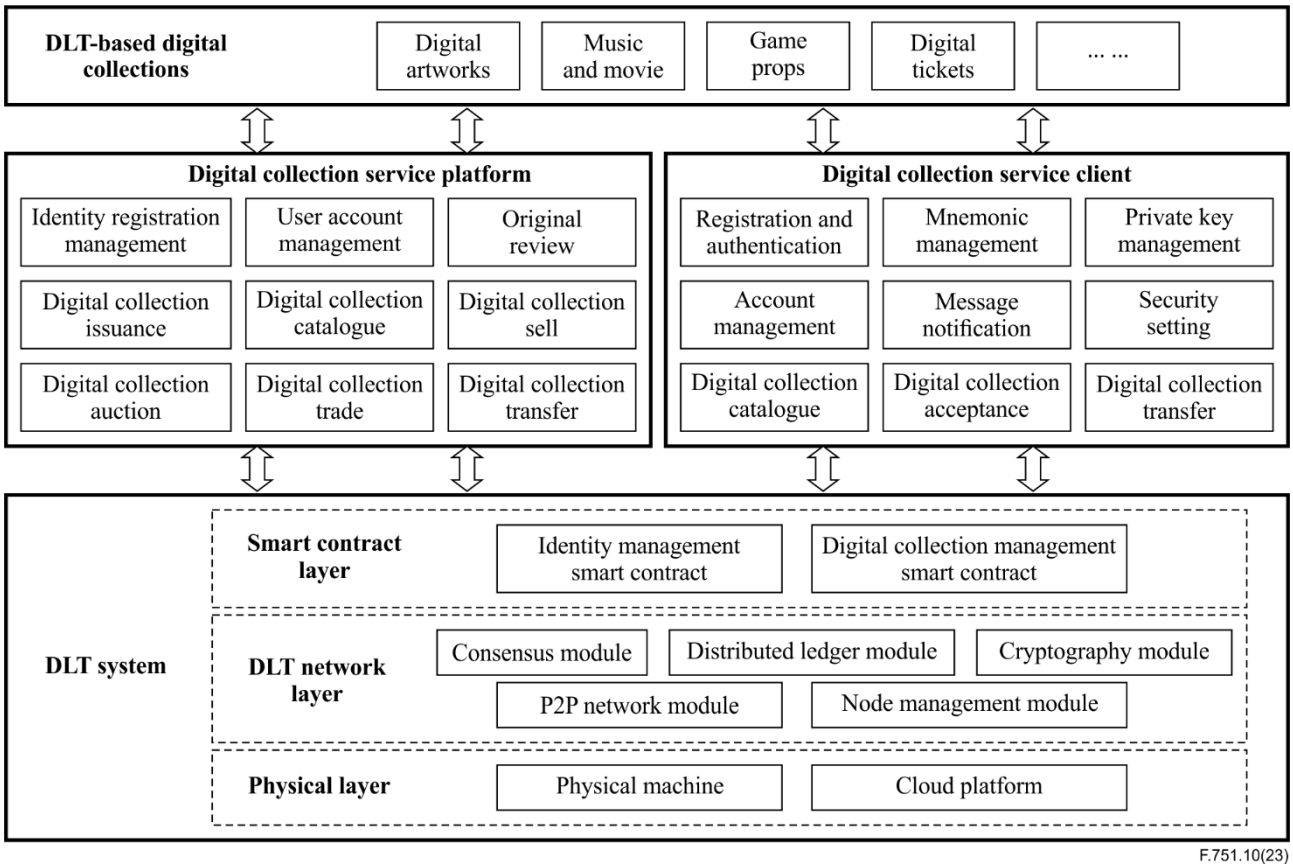

Figure 1 – Architecture of the DLT-based digital collection service system

The DLT-based digital collection service system includes the DLT system, digital collection service platform, digital collection service client and DLT-based digital collections.

7.2 Core functional components

7.2.1 DLT system

The DLT system mainly includes the physical layer, the DLT network layer and the smart contract layer.

a) The physical layer can be a physical machine or a cloud platform.

b) The DLT network layer provides DLT network services, including a consensus module, distributed ledger module, cryptography module, peer-to-peer (P2P) network module, and node management module. These modules cooperate with each other to ensure that each node in the DLT network forms a consensus on the transaction, thereby ensuring the consistency of the node data.

c) The smart contract layer contains an identity management smart contract and digital collection management smart contracts.

The reference framework of a DLT system is described in [ITU-T F.751.2].

7.2.2 Digital collection service platform

The digital collection service platform is deployed in the server backend to provide functions such as identity registration management, user account management, and original review, issuance, display, sale, transaction, auction, and transfer of digital collections.

7.2.3 Digital collection service client

The digital collection service client is for users to realize the management of digital collections, including real-name authentication and registration, mnemonic management, private key management, account management, message notification, security settings, digital collection catalogue, digital collection acceptance, digital collection transfer and other functions.

7.2.4 DLT-based digital collections

DLT-based digital collections can be digital artworks, digital music & movies, digital game props, digital tickets, etc.

8 Information flows

8.1 Overall information flow diagram

The overall information flow diagram of the DLT-based digital collection services is shown in Figure 2.

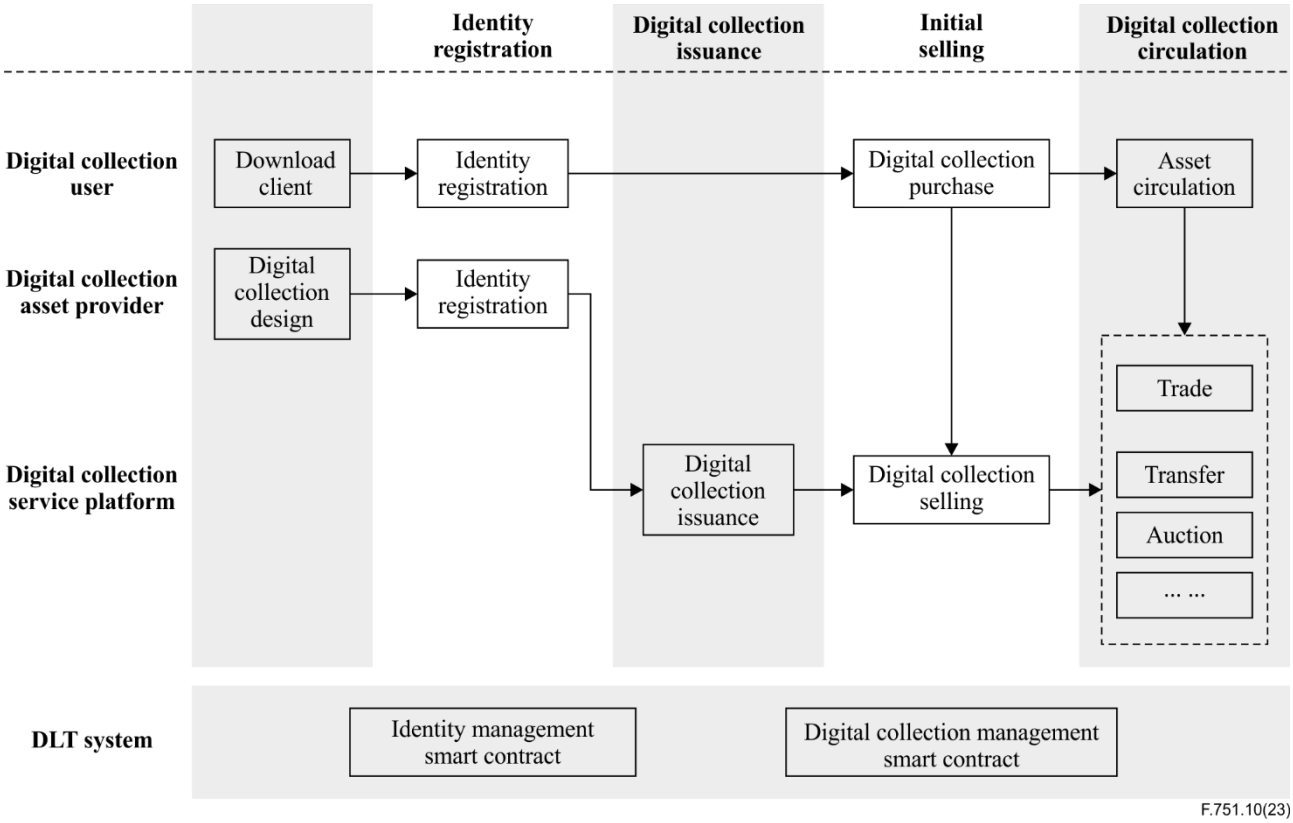

Figure 2 – Information flows of the DLT-based digital collection services

The DLT-based digital collection service system mainly includes digital collection users, digital collection asset providers, the digital collection service platform, and the DLT system. Its process mainly includes identity registration, digital collection issuance, initial selling, and digital collection circulation. Different roles involve different activities.

a) The digital collection users mainly involve downloading digital collection clients, performing identity registration, purchasing, and circulating digital collections.

b) The digital collection asset provider is mainly involved in the design of digital collections, DLT identity registration, and the issuance of digital collections.

c) The digital collection service platform mainly involves the issuance, sale, and circulation of digital collection assets.

d) The DLT system mainly involves the execution of DLT identity management smart contracts, digital collection management smart contracts, etc.

8.2 Information flows of the digital collection service platform

From the perspective of the digital collection service platform side, the overall process of the digital collection service is described as below:

a) DLT identity registration

The digital collection service platform receives and completes the identity registration from the digital collection asset provider, and the digital collection user.

b) Original review of the digital collections

The digital collection asset provider completes the design of the digital collections. The service platform completes the original review of the digital collections.

c) Digital collection issuance

The service platform receives requests from the digital collection asset provider and completes the issuance of the digital collections.

d) Digital collection selling

The service platform supports the initial selling of the digital collections.

e) Digital collection circulation

The service platform supports the circulation of the digital collections, including transfers, auctions, selling and buying.

8.3 Information flows of the digital collection user

From the perspective of the digital collection user side, the overall process of the digital collection service is described as below:

a) Download the client

Digital collection users download the client from the service platform. The service platform provides and supports users to download the client.

b) DLT identity registration

Digital collection users perform identity registration and real-name authentication based on the client.

c) Digital collection purchase

Digital collection users purchase the digital collections from the client.

d) Digital collection circulation

Based on the client, digital collection users can realize the circulation and transfer of digital collections.

9 Functional requirements

9.1 Functional requirements of the DLT-based digital collection service client

The functional requirements of the DLT-based digital collection service client are as follows:

a) The functions of real-name authentication and registration of users are required, including new user registration, registered user restoration, and user cancellation.

b) It is required to support the functions of mnemonic management, including generating mnemonic words, backup of mnemonic words, import of mnemonic words, export of mnemonic words and other functions.

c) It is required to support the functions of private key management, including importing private keys, exporting private keys, etc.

d) It is required to support the function of accepting digital collections, that is, users can accept and own the products after purchasing the digital collections.

e) It is required to support the function of digital collection transfer. That is, after the user owns the digital collection, it can be transferred to other users, or transferred to other receiving addresses.

f) It is required to support account management functions, including exporting private keys, changing account names, exporting mnemonics, viewing product lists and details, viewing address details, etc.

g) It is required to support the function of querying transaction records lists for users to query transaction records.

h) It is required to support the security setting function to allow users to change passwords, backup accounts, etc.

9.2 Functional requirements of the DLT-based digital collection service platform

The functional requirements for the DLT-based digital collection service platform are as follows:

a) It is required to support the user's identity registration function on the platform, including the registration of individual users and the registration of corporate users. It is also required to support the log-off function of registered users on the platform, and deletion of user information.

b) It is required to support the function of initializing the user's on-chain identity, including the initialization of the basic identity information of individual users and corporate users.

c) It is required to support user account management functions, including generating public and private keys of user accounts in advance, maintaining the relationship between account addresses and real users, etc.

d) It is required to support the function of originality review of DLT-based digital collections. That is, initial screening of digital collection originality, and filter and identify collections that may be infringing.

e) It is required to support the function of registering and issuing DLT-based digital collections. Before the issuance, the issuance of the DLT-based digital collections is recommended to be reviewed, and the risks in laws, regulations, and regulatory policies are required to be evaluated. After the evaluation is passed, the issuance can be carried out.

f) It is required to support the function of DLT-based digital collections display, and display user assets on the front-end page. It is also required to support the DLT-based digital collections information query function, and support users to query various types of the DLT-based digital collections, including transaction information, prices, etc., based on the unique digital collections identifier and other information.

g) It is required to support the function of issuing and selling DLT-based digital collections, that is, according to the issuer's pricing, the bidder who meets the conditions of the smart contract will obtain the ownership of the DLT-based digital collections under the contract logic.

h) It is recommended to support the auction function, including the public welfare auction function.

i) It is required to support the function of trading DLT-based digital collections, that is, reselling from one user to another user.

j) It is required to support the function of transferring and gifting DLT-based digital collections, that is, users can transfer any DLT-based digital collections that belong to them to any legal address on the chain.

k) It is recommended to support the compliance risk assessment of the entire life cycle of the DLT-based digital collections, including issuance, sale, transaction, transfer and gift, auction, etc.

9.3 Functional requirements of the DLT system

9.3.1 Functional requirements of the smart contracts

The functional requirements of the smart contracts are as follows:

a) It is required to support the registration and issuance of smart contracts as well as the triggering and execution of smart contracts.

b) It is required to support the user to define the logic of a smart contract through some programming language, and then publish it on the DLT system and have it executed by the user's signature or other events to complete the logic of smart contract such as transaction settlement according to the logic of the smart contract terms.

c) It is required to support the smart contract verification function. The upper layer application can encode the business execution rules into smart contract scripts according to the actual business requirements, and then deploy the smart contracts in the underlying DLT system, and the bookkeeping node is responsible for running them in a secure container environment and giving the running results.

d) It is required to support the distributed multi-party consensus bookkeeping function. The participants verify the business through smart contracts and record the consensus results into the distributed ledger after consensus is completed, while the distributed ledger contains the transactions in data blocks by means of hash chains to reduce the possibility of data tampering.

e) It is required to add a licensed credible institution to the consensus or validation node to ensure the stability and security of the parties' collaboration in the DLT system.

9.3.2 Functional requirements of the storage

The functional requirements of the storage are as follows:

a) It is required to support local database storage and file system storage, and cloud storage is recommended to be supported.

b) Local storage is required to support hot and cold separation, database storage is required to support the mode of splitting library and table, cloud storage is required to support lossless expansion, and support unlimited expansion according to the cloud's clustering rules.

c) It is recommended to use a dual database approach of chain database and state database for storage. The chain database saves the chain data, and all business data exists in this data, so that the data is traceable to the source. The state database is used to save the current state value to avoid traversing all transaction logs to calculate the current state value. The dual

database solution can improve the speed of data query while preserving all the evidence of transaction history.

9.3.3 Functional requirements of the operation and management

The functional requirements of the operation and management are as follows:

a) It is required to provide a comprehensive, real-time, visualized operation and maintenance management system to quickly identify system status and meet operational management needs at multiple levels.

b) It is required to provide visualization of service delivery. Visual management of the entire service delivery process, from code compilation, testing, acceptance to formal environment deployment.

c) It is required to provide visualization of service metrics. Standardized hierarchical categorization of data, from infrastructure, upper layer components, application services to user side, based on the topology architecture of the application, collection of various metrics and unified presentation in one analysis platform.

d) It is required to provide generic and efficient information collection components to display machine system information (CPU, memory, hard disk, network status, etc.), node usage status (node access, access time consumption, node health status, etc.) and business usage (business access, success rate, time consumption distribution, etc.) to the monitoring interface in real time to facilitate the management of the whole system.

e) It is recommended to support the continuous auditing function, to audit the data operations and service operations in the DLT system.

f) It is recommended to support the data posture presentation function. By extracting and analysing the data in the ledger, the system forms the current world status and historical records of the data, and then presents them through the interface, and monitors the current operation status of the system nodes.

9.4 Performance requirements

The performance requirements are as follows:

a) It is required to analyse and pressure test using various models and support large concurrent processing capacity.

b) In terms of fault tolerance, when node failure or fraud is detected, the system is required to automatically enable the algorithmic feature of Byzantine fault tolerance.

c) It is required to support multiple load balancing of applications and databases, support a large number of users online and simultaneous operations, and that it will not cause a significant decrease in system responsiveness due to the growth of the number of users or the growth of the volume of information.

d) The system deployment is recommended to be designed in a highly available mode to minimize and shorten the time of external service stoppage during regular maintenance and release to ensure that the system provides long time continuously available services.

e) It is required to have high reliability to ensure the correctness of business logic under normal and extreme conditions, including but not limited to no single point of failure, fault recovery, disaster recovery, sudden user volume response, etc.

f) It is required to have linear expansion and elastic scaling capability. The hardware equipment is recommended to adopt cluster or distributed deployment mode to achieve dynamic loading of nodes and support rapid horizontal expansion of nodes while eliminating single point of failure. It can also rely on cloud computing technology to realize the automatic elastic scaling of basic resources.

9.5 Security requirements

9.5.1 Identity authentication requirements

The identity authentication requirements are as follows:

a) It is required to support digital certificate identity and is recommended to support a centralized public key infrastructure (PKI) system.

b) The authentication certificate between DLT nodes is recommended to adopt the international security certificate standard, and the process of issuing, storing, updating, and revoking the software development kit (SDK) certificate.

c) Real-name authentication is required to be done for users in advance to ensure that all users participating in digital collections pass real-name authentication to ensure the authenticity of users, which can prevent behaviours harmful to business such as hoarding and speculation.

9.5.2 Data security requirements

The data security requirements are as follows:

a) It is required to support data encryption, digital signatures, and other technologies to ensure the confidentiality, integrity, and resistance to repudiation of data.

b) It is required to support digital signatures through asymmetric encryption to ensure the tamper-evident nature of business requests and data during transmission.

c) It is required to support the provision of regulatory keys to the supervisor of the application to reduce the risk of privacy leakage, while ensuring the auditability of data.

d) It is required to support the storage of consistent data across nodes through a consensus mechanism.

e) For the stored data records, it is required to be possible to ensure that the stored data records cannot be modified through self-checkability within the nodes and quasi-real-time multi-node data checking.

9.5.3 Privacy protection requirements

The privacy protection requirements are as follows:

a) It is required to protect the connections user information and DLT addresses. From the record storage of each node, the associated user information cannot be obtained.

b) For the storage of user information, multi-layer protection such as permission control, access authentication and encrypted storage is required to be available.

c) Privacy protection services are required to be provided for users, including schemes such as dual key pairs, ring signatures, and zero-knowledge proofs.

d) It is required to support users to select corresponding services according to their actual needs, which are used to encrypt and de-link their transaction information.

e) When it comes to the display of users' personal information (name, ID number, etc.), user privacy security is required to be ensured by hiding part of the key information, desensitization, etc.

f) In some high-security scenarios, it is required to be possible to hash out the uploaded content through encryption algorithms to ensure user privacy.

9.5.4 System security requirements

The system security requirements are as follows:

a) In the process of system operation, the normal operation of the system is required to be ensured to prevent malicious attacks from causing business anomalies and unpredictable

problems, including but not limited to service unavailability, business data errors, malicious data, leakage of user privacy and other problems.

b) It is required to ensure the security of the business system by setting the necessary network whitelist.

c) On the system, all network requests are required to enter through a unified portal, and the system is recommended to be able to prevent attacks such as distributed denial of service (DDOS) attacks.

d) In certain business scenarios with high security requirements, the system is required to be secured by means of authentication codes to avoid the impact of heavy traffic.

9.5.5 Content security requirements

The content security requirements are as follows:

a) It is required to ensure the content security of digital collections. The content of digital collections is diverse, with text, images, audio, and video, etc. These contents are recommended to be detected to prevent the uploading of contents related to pornography, terrorism, violence, etc.

b) It is required to detect the content at the time of data submission by users through the detection capability of content security products.

c) It is required to set up a blacklist mechanism. Platforms that submit malicious content are recommended to be blacklisted, in particular if after repeated occurrences.

Appendix I

Examples of the DLT-based digital collection services

(This appendix does not form an integral part of this Recommendation.)

I.1 DLT-based digital culture collections

Users can rent or purchase digital culture collections. There is a distinction between the procedure of purchase and the procedure of rental by the user. In the process of performing digital culture content rental, rental can be performed for all rights to the digital culture content, and rental can be performed only for some rights. For example, in the case of rental for exhibition, rental is performed only for exhibition rights, and in this process, authority is transferred only for exhibition rights. The asset provider needs an ID verification and digital culture contents registration process. The user has a process of checking IDs and searching for digital culture content and purchasing necessary digital culture content. In the distributed leger technology, updates are performed on digital culture content issues.

I.2 DLT-based digital music collections

Based on DLT, digital music can be issued limitedly on the DLT network, and they can be collected by music fans.

I.3 DLT-based digital game assets

Based on DLT, digital game assets can be issued limitedly on the DLT network, and they can be collected by game players. The digital game assets include lands, characters, costumes, props, game points, etc.

I.4 DLT-based digital sport assets

Based on DLT, digital sport assets can be issued limitedly on the DLT network, and they can be collected by sport fans. The digital sport assets include sport snap shots, wonderful moments, etc.

I.5 DLT-based digital tickets

Based on DLT, digital tickets can be issued limitedly on the DLT network, and they can be collected by users. The digital tickets include concert tickets, sport tickets, etc.

Appendix II

Value of using DLT for digital collection services

(This appendix does not form an integral part of this Recommendation.)

II.1 Guarantee authenticity, durability and continuity

DLT can verify the authenticity of the digital collections, which effectively solves the long-term pain point of rampant counterfeiting in the industry.

For antique or rare collection types, DLT can ensure their continuity and durability.

II.2 Ownership confirmation and information traceability

DLT can realize the ownership confirmation and information traceability of digital collections.

In the field of digital collections, piracy is prevalent. DLT can solve the problem of digital ownership by making it non-replicable so it can be bought and sold like tangible assets. Owners of digital collections can significantly enhance their sense of acquisition and protect the rights and interests of owners through the determination of ownership.

II.3 Enhance collection value through uniqueness and scarcity

Through DLT, digital collections have the uniqueness and scarcity consistent with traditional collections, avoiding malicious additional issuance and unlimited copying of digital collections.

DLT has made possible digital collections with rare attributes and enhanced their collection value.

II.4 Reduce transaction costs and improve circulation

DLT can realize the separation of viewing rights and ownership, helping small and medium catalogue creators avoid the high cost of publishing collections offline.

In terms of circulation channels, due to the large number of trading markets for DLT-based digital collections, online trading channels have been introduced into the traditional market. With its confirmation of rights, it greatly shortens the transaction process, reduces transaction costs, and broadens the circulation channels for digital collections.

II.5 Speed-up the construction of the digital collection trading market

The promotion of DLT in the field of digital collections has broadened the product form in this field, effectively boosted the development of digital collections, and promoted the release of the value of digital collection commemoration and circulation.

With DLT, the problems of forgery and the difficulty of circulation encountered in the transaction of digital collections have been solved, the commercial value of digital collections has been realized, and the market construction of digital collections has been accelerated.

Bibliography

[b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger system*.

[b-ITU-T F.751.1] Recommendation ITU-T F.751.1 (2020), *Assessment criteria for distributed ledger technology platforms*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	**Non-telephone telecommunication services**
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023