International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4561

(08/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Services, applications, computation and data processing

Blockchain-based data management for supporting Internet of things and smart cities and communities

Recommendation ITU-T Y.4561

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	**Y.4550–Y.4699**
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.4561

Blockchain-based data management for supporting Internet of things and smart cities and communities

Summary

Along with the development of the Internet of things (IoT) and smart cities and communities (SC&C), various applications have different kinds of requirements for data management, and there are many challenges, especially in data representing, data processing, data service provisioning, and other aspects in a secure and effective manner. Meanwhile, blockchain as an emerging technology possesses the characteristics of trust, transparency, traceability and accountability. It has the potential capabilities to solve the existing issues in data management.

Recommendation ITU-T Y.4561 specifies the requirements, generic reference model, common capabilities, and procedures of blockchain-based data management.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4561	2020-08-29	20	11.1002/1000/14380

Keywords

Blockchain, capability, data management, reference model, requirement.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4561

Blockchain-based data management for supporting Internet of things and smart cities and communities

1 Scope

This Recommendation provides technical descriptions and specifications of the blockchain-based data management in Internet of things (IoT) and smart cities and communities (SC&C) application domains.

The scope of this Recommendation includes:

- Requirements of blockchain-based data management,
- Generic reference model of blockchain-based data management,
- Common capabilities and procedures of blockchain-based data management.

In addition, this Recommendation provides two data management approaches based on blockchain in Appendix I.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 blockchain [b-FG-DPM TR D3.5]: A peer to peer distributed ledger based on a group of technologies for a new generation of transactional applications which may maintain a continuously growing list of cryptographically secured data records hardened against tampering and revision.

NOTE 1 – Blockchains can help establish trust, accountability and transparency while streamlining business processes.

NOTE 2 – Blockchains can be classified as three types (i.e., public, consortium and private) based on the relationship of the participants and the way to provide services.

NOTE 3 – Definition compatible with [b-ISO 22739].

3.1.3 data management [b-ISO/IEC TR 10032]: The activities of defining, creating, storing, maintaining and providing access to data and associated processes in one or more information systems.

3.1.4 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.6 smart sustainable city [b-ITU-T Y.4900]: A smart sustainable city (SSC) is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects.

NOTE – City competitiveness refers to policies, institutions, strategies and processes that determine the city's sustainable productivity.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

ETL Extract Transform Load

FTP File Transfer Protocol

HTTP Hyper Text Transfer Protocol

IoT Internet of Things

ICT Information and Communication Technology

REST Representational State Transfer

SC&C Smart Cities and Communities

SDK Software Development Kit

SSC Smart Sustainable City

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.

6 Overview of blockchain-based data management

In the context of the IoT and SC&C, the requirements of data management based on blockchain need to be specified. Subsequently, generic reference model, functional entities, and their capabilities and interactions are specified according to the requirements.

6.1 Introduction

6.1.1 Data management from an applications perspective

Based on the definition of data management, in the context of IoT and SC&C, data management needs to cover the management aspects in the whole data life cycle, at least including the activities of data collecting, aggregating, transferring, storing and integrating, and the associated processes. It controls all the input-output operations within data processing. The data management in the data life cycle is briefly depicted in Figure 1.

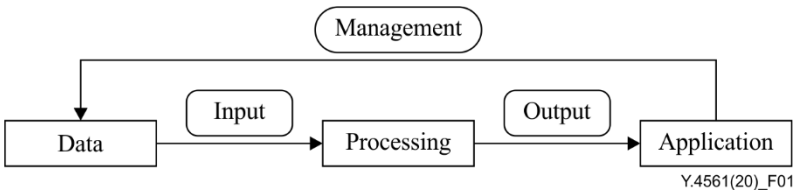

Figure 1 – Introduction of data management in the data life cycle

Figure 1 shows that data can either be raw data collected by the IoT device or processed data from the IoT application, and it needs to be collected and integrated in advance to create the appropriate input. The processing procedure entails the management and converting of data from the input state through to the required output requested by different kinds of applications. During the whole data life cycle, the following stages need to be monitored:

- Data collecting and transferring before data input,
- Data aggregating and storing upon input or after processing,
- Data transferring and data integrating upon processing.

6.1.2 Characteristics of blockchains from a data management perspective

A blockchain is distinguished by the following characteristics:

- Decentralized,
- Distributed storage,
- Asymmetric cryptography,
- Digital fingerprint,
- Tamper-proof.

Each characteristic can be adopted to improve particular aspects of data management as follows:

- Decentralized mechanism can be adopted to reduce the need for intermediaries among multiple parties to establish trust data transaction,
- Each blockchain node usually stores a copy of the entire verified blocks of data, the distributed storage can be adopted to the benefit of data recovery and data sharing,
- Asymmetric cryptography can be adopted to enhance data confidentiality and communication security, and facilitate non-repudiation by using the private key as digital signature,
- Digital fingerprint can be adopted to enhance data integrity,
- Immutable blocks of data are recorded by each node of blockchain.

6.2 Requirements of data management based on a blockchain

6.2.1 Security requirement

It is required to enhance the secure control of IoT data when it is being transferred through all the data processes. Secure control includes managing to keep data confidentiality, data integrity, and non-repudiation.

6.2.2 Authenticity requirement

It is required to record the data in a pre-defined format as per application requirement in the blockchain after consensus, to guarantee data authenticity and immutability.

6.2.3 Data acquisition requirements

It is required to collect data from data source and related metadata for authenticity verification.

It is required to aggregate all the data from data sources according to specific formats.

6.2.4 Data processing requirements

It is required to provide blockchain based realization, including consensus making mechanism, smart contract execution environment, and distributed storage.

It is required to execute operation of the blockchain in response to the requests for data management.

6.2.5 Data management requirement

It is required to open the data to the authorized party and to protect the privacy of sensitive data.

6.2.6 Application requirements

It is required to provide the interface to IoT and SC&C applications for accessing data in a secure manner.

It is required to provide transparency and traceability to identify the source of the data assets, ownership, right to use, transferring path, etc., when integrating data including reusing, sharing, circulation, and exchanging.

7 Generic reference model of a blockchain-based data management

The generic reference model of a blockchain-based data management includes data management functional entities for providing capabilities of blockchain-based data management, external functional entities that are related to data management and external to the generic reference model, reference points for representing interaction between the data management functional entities, and reference points for representing interaction between the data management functional entity and the external functional entity.

The external functional entities specified in the generic reference model of a blockchain-based data management are termed as "actors" of data management in this Recommendation.

NOTE – The term "actors" is explained in [b-ITU-T Y.4100].

The generic reference mode of a blockchain-based data management can fulfil the requirements of data management specified in clause 6, and it is independent of any specific application in the IoT and SC&C application domains.

7.1 Data management functional entities

The generic reference model of blockchain-based data management is illustrated in Figure 2. The data management functional entities in this generic reference model include data blockchain representation, blockchain-based data processing, data service provisioning, blockchain-based data controlling, and blockchain-based data monitoring functional entities, as illustrated in the figure.

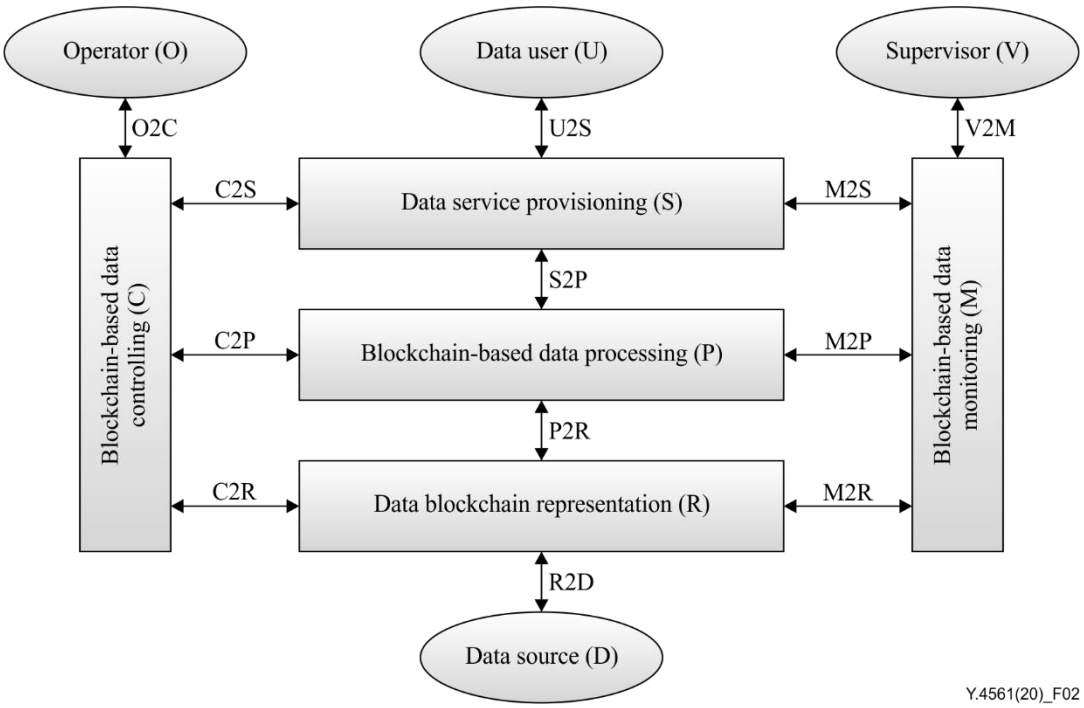

Figure 2 – A generic reference model of blockchain-based data management

7.1.1 Data blockchain representation functional entity

Data blockchain representation functional entity is responsible for connecting the data source directly. It collects metadata for validation from data source according to specified data formats, integrates and encapsulates the metadata with sampling data from data source into a data management transaction operation, then encapsulates one or multiple operations into a data block. In addition, it invokes the functional interfaces provided by the blockchain-based data processing functional entity and submits the processing requests to the blockchain-based data processing functional entity and receives corresponding responses.

7.1.2 Blockchain-based data processing functional entity

The blockchain-based data processing functional entity is responsible for validating the authenticity of a data block in the data management operations and recording the validated data block into the blockchain. It is responsible for processing the data management requests including data retrieval, searching, and auditing. In addition, it provides the blockchain related processing capabilities including consensus among verification nodes of the blockchain, smart contract execution, linking new block into the blockchain, and searching the blockchain in response to the requests of data management.

7.1.3 Data service provisioning functional entity

The data service provisioning functional entity is responsible for providing common services to the data user based on the data management capabilities in the blockchain-based data processing functional entity. It is also responsible for providing the customized services of data management to the data user according to the data user's service requirements.

7.1.4 Blockchain-based data controlling functional entity

The blockchain-based data controlling functional entity is responsible for the configuration and control of blockchain-based data management capabilities, according to data user's service requirements and blockchain related capabilities. It is also responsible for configuration and control of different data sources based on data sources' characteristics, and management of the data users subscribing to the data management services.

7.1.5 Blockchain-based data monitoring functional entity

The blockchain-based data monitoring functional entity is responsible for the supervision of data management capabilities according to data user's service requirements and blockchain related capabilities. It is also responsible for the supervision of different data source based on data source's characteristics, and supervision of the operations of data users based on their subscribed services.

7.2 Data management actors

The data management actors that are related with data management and external to the generic reference model include data source, data user, operator, and supervisor, which are illustrated in the ellipses in Figure 2. The interaction between these data management actors and the functional entities specified in the generic reference model can be used to describe the capabilities for fulfilling the data management requirements in the IoT and SC&C application domains.

7.2.1 Data source actor

The implementation of the data source actor can connect directly to the implementation of the data blockchain representation functional entity in the specific blockchain designed for a data management application. It performs the data submission operation according to the specified data format if it has the permission of the data blockchain representation functional entity.

7.2.2 Data user actor

The implementation of the data user actor can connect directly to the implementation of the data service provisioning functional entity in the specific blockchain designed for a data management application. It can access the data in the blockchain with the permission of the data service provisioning functional entity. It submits the data query, search and other data management operations.

7.2.3 Operator actor

The implementation of the operator actor can connect directly to the implementation of the blockchain-based data controlling functional entity in the specific blockchain designed for a data management application. It can access the data and configure the data management with the permission of the blockchain-based data controlling functional entity. It submits the configuring operation, such as nodes management, consensus configuration, and smart contract configuration.

7.2.4 Supervisor actor

The implementation of the supervisor actor can connect directly to the implementation of the blockchain-based data monitoring functional entity in the specific blockchain designed for a data management application. It can access the data in the blockchain with the permission of the blockchain-based data monitoring functional entity and can supervise all the data and data operations.

7.3 Reference points

7.3.1 U2S reference point

The U2S reference point specifies the data management service categories, related parameters, and invoke methods.

7.3.2 O2C reference point

The O2C reference point specifies the data control service categories, related parameters, and invoke methods.

7.3.3 V2M reference point

The V2M reference point specifies the data monitoring service categories, related parameters, and invoke methods.

7.3.4 R2D reference point

The R2D reference point specifies the categories and parameters of the data interface, including the data source actor registration and authentication, and data submission.

7.3.5 P2R reference point

The P2R reference point specifies the interface categories and the parameters of function invocation, including data encapsulation, data record, configuration.

7.3.6 S2P reference point

The S2P reference point specifies the service categories, related parameters, and invoke methods.

7.3.7 C2S reference point

The C2S reference point specifies the control interface categories, related parameters, and control methods in the service provision aspect.

7.3.8 C2P reference point

The C2P reference point specifies the control interface categories, related parameters, and control methods in the blockchain process aspect.

7.3.9 C2R reference point

The C2R reference point specifies the control interface categories, related parameters, and control methods in the data representation aspect.

7.3.10 M2S reference point

The M2S reference point specifies the monitoring interface categories, related parameters, and monitoring methods in the service provision aspect.

7.3.11 M2P reference point

The M2P reference point specifies the monitoring interface categories, related parameters, and monitoring methods in the blockchain processing aspect.

7.3.12 M2R reference point

The M2R reference point specifies the monitoring interface categories, related parameters, and monitoring methods in the data representation aspect.

8 Common capabilities and procedures of blockchain-based data management

The common capabilities of the blockchain-based data management can be classified by data blockchain representing capabilities, blockchain-based data processing capabilities, data service provisioning capabilities, blockchain-based data controlling capabilities, and blockchain-based data monitoring capabilities. Each category of the common capabilities is related to each functional entity specified in the generic reference model of the blockchain-based data management as illustrated in Figure 2. The common procedures describe the typical interactions between the two connected functional entities.

8.1 Data blockchain representing capabilities

The category of data blockchain representing capabilities that is related to the data blockchain representation functional entity is required to have the following capabilities:

- Identifying, binding, and authenticating data sources,
- Creating and updating data block to be linked in certain blockchain,
- Creating and adding timestamp in block,
- Creating and updating data management control data in block.

8.2 Blockchain-based data processing capabilities

The category of blockchain-based data processing capabilities that is related to the blockchain-based data processing functional entity is required to have the following capabilities:

- Authenticating data sources in the data block,
- Checking the validation of data accessing in the blockchain,
- Checking validation of data updating in the blockchain,
- Verifying and storing the validated data blocks via specific consensus mechanism,
- Controlling data user in accessing and updating the data block.

8.3 Data service provisioning capabilities

The category of data service provisioning capabilities that is related to the data service provisioning functional entity is required to have the following capabilities:

- Identifying, binding, and authenticating data user in the data block,
- Searching and accessing data in the blockchain,
- Searching and accessing timestamping in the blockchain,
- Checking the validation of data stored in the blockchain.

8.4 Blockchain-based data controlling capabilities

The category of blockchain-based data controlling capabilities that is related to the blockchain-based data controlling functional entity is required to have the following capabilities:

- Identifying, binding, and authenticating operators,
- Configuring data management in the blockchain,
- Configuring data access in the blockchain,
- Checking data management configuration validation in the blockchain.

8.5 Blockchain-based data monitoring capabilities

The category of blockchain-based data monitoring capabilities that is related to the blockchain-based data monitoring functional entity is required to have the following capabilities:

- Identifying, binding, and authenticating supervisors,
- Supervising data creation, updating and accessing in the blockchain,
- Supervising the time sequence of data stored in the blockchain,
- Supervising validation of data stored in the blockchain.

8.6 Data submission procedure

Figure 3 illustrates the steps for data submission procedure.

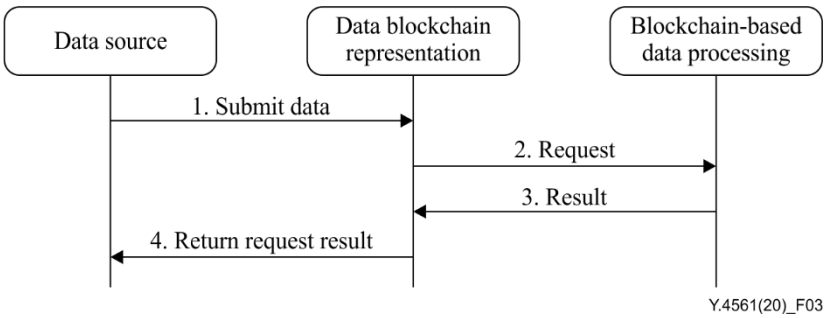

Figure 3 – Data submission procedure

- Step 1, data source actor submits the data to the data blockchain representation functional entity, which collects source data and its metadata for validation according to the specified data format.
- Step 2, data blockchain representation functional entity creates the data hash calculation and sends the request to the blockchain-based data processing functional entity.
- Step 3, blockchain-based data processing functional entity integrates the validated data such as description, type, data hash and timestamp into the blockchain, and return the result to the data blockchain representation functional entity.
- Step 4, the data blockchain representation functional entity returns the request result to the data source actor.

8.7 Service request procedure

Figure 4 illustrates the steps for service request procedure.

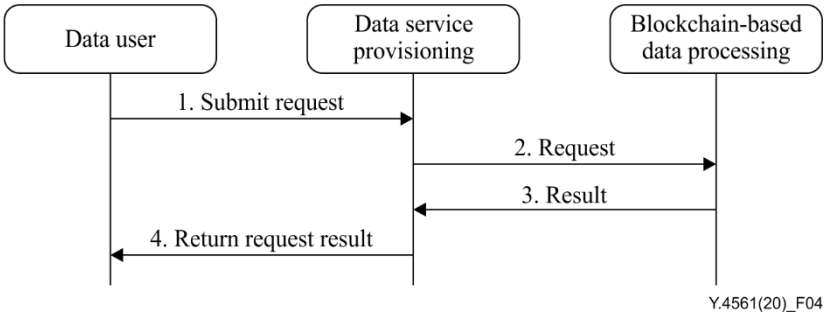

Figure 4 – Service request procedure

- Step 1, the data user actor submits the service request to the data service provisioning functional entity.
- Step 2, the data service provisioning functional entity processes the request and sends the data request to the blockchain-based data processing functional entity.
- Step 3, the blockchain-based data processing functional entity finishes the processing and returns the result to the data service provisioning functional entity.
- Step 4, the data service provisioning functional entity returns the request result to the data user actor.

8.8 Controlling procedure

Figure 5 illustrates the steps for controlling procedure.

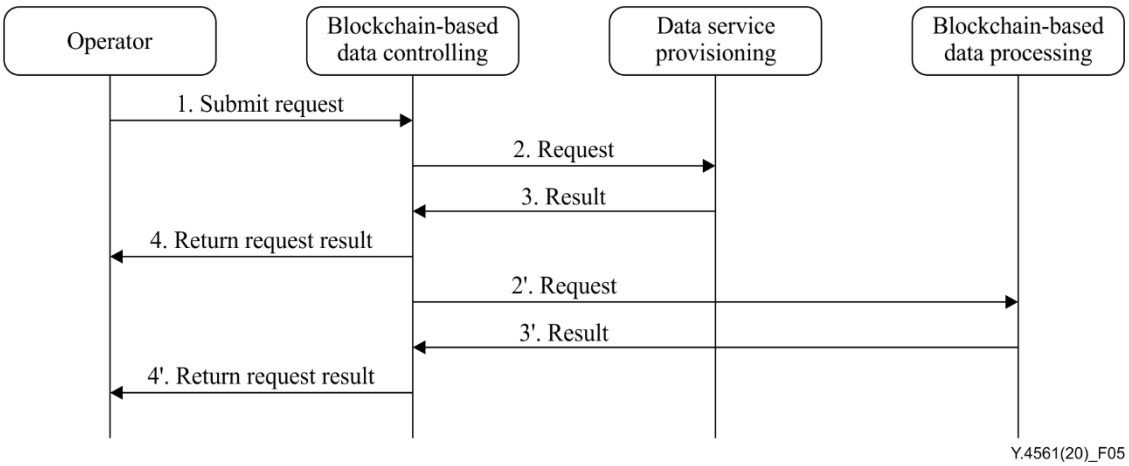

Figure 5 – Controlling procedure

- Step 1, the operator actor submits the controlling request, including controlling operation, controlling type and parameters to the blockchain-based data controlling functional entity.
- Step 2, the blockchain-based data controlling functional entity makes a controlling request to the data service provisioning functional entity according to the type of the operator's request.
- Step 3, the data service provisioning functional entity executes the request and returns the result to the blockchain-based data controlling functional entity.
- Step 4, the blockchain-based data controlling functional entity returns the request result to the operator actor.

Alternative procedure:

- Step 2', the blockchain-based data controlling functional entity makes a controlling request to the blockchain-based data processing functional entity according to the type of the operator's request.
- Step 3', the blockchain-based data processing functional entity executes the request and returns the result to the blockchain-based data controlling functional entity.
- Step 4', the blockchain-based data controlling functional entity returns the request result to the operator actor.

8.9 Monitoring procedure

Figure 6 illustrates the steps for monitoring procedure.

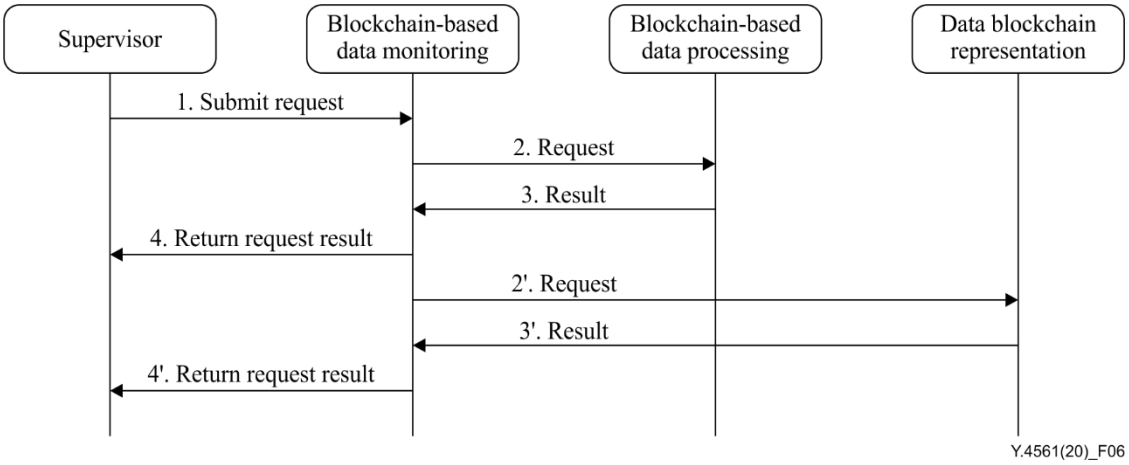

Figure 6 – Monitoring procedure

- Step 1, the supervisor actor submits the request to the blockchain-based data monitoring functional entity.
- Step 2, the blockchain-based data monitoring functional entity makes a request to the blockchain-based data processing functional entity according to the type of the supervisor's request.
- Step 3, the blockchain-based data processing functional entity executes the request and returns the result to the blockchain-based data monitoring functional entity.
- Step 4, the blockchain-based data monitoring functional entity returns the request result to the supervisor actor.

Alternative procedure:

- Step 2', the blockchain-based data monitoring functional entity makes a request to the data blockchain representation functional entity according to the type of the supervisor's request.
- Step 3', the data blockchain representation functional entity executes the request and returns the result to the blockchain-based data monitoring functional entity.
- Step 4', the blockchain-based data monitoring functional entity returns the request result to the supervisor actor.

Appendix I

Data management approaches based on blockchain

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

I.1 Authentic copyright data

The conventional copyright registration is time-consuming, so it is hard to guarantee the timeliness of copyright protection of digital publications, which have features of high production and rapid dissemination in the internet era. Once the copyright is violated, its owner will be required to provide evidence of copyright infringement. However, it is difficult to obtain valid evidence if there is no efficient copyright registration system or protection mechanism.

Features of blockchains such as authorized right, traceability and tamper-proof can be applied in the solution of distributed authentic copyright data.

I.1.1 Overview of solution

The functional architecture of a copyright system is shown in Figure I.1.

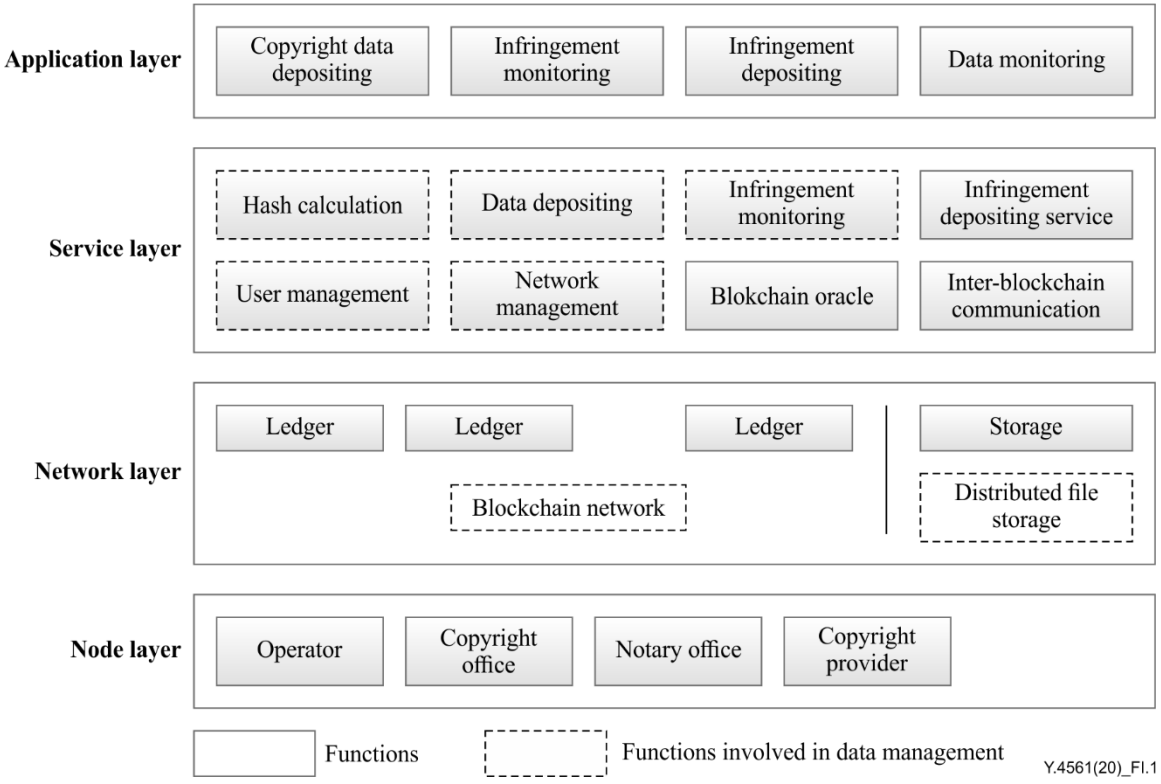

Figure I.1 – The functional architecture of copyright system

The functional architecture of a copyright system includes four layers: node layer, network layer, service layer and application layer. The node layer includes the operator node, as well as the notary office, the copyright office, the copyright provider, whereas some well-known universities are the depositing nodes and supervising nodes of the copyright depositing consortium blockchain. The system builds a blockchain network and a distributed file storage network based on the underlying resources of each node, providing services such as user management, hash calculation, copyright data depositing, infringement monitoring and so on.

The services of copyright depositing usually include copyright data depositing, infringement monitoring, and infringement depositing. They are described as follows:

1) Copyright data depositing

The user submits the registration application with the required information, such as the applicant, the author and the content of the copyright, to the copyright system. Based on the selected copyright file, the system calculates the data fingerprint of the file and related information by using the hash algorithm. Then the system writes the obtained data fingerprint into the blockchain after the user's confirmation. Once the data is verified, blocks are created and linked to the blockchain based on the information through the consensus mechanism. The copyright system can generate a certificate for the user online, which has a unique and traceable copyright hash value and a timestamp on the blockchain.

2) Infringement monitoring

First, a unique hash value is generated for the copyright data, and the hash value will be stored on the blockchain. Based on this, the system provides automated web crawlers for key websites and compares the monitored content with the authentic copyright data. Pre-alert procedures against the infringement will be automatically performed if the degree of similarity satisfies the threshold level, and the infringing content will be continuously tracked and further analysed. Once the infringement is confirmed, the infringement evidence will be obtained and stored on the blockchain directly.

3) Infringement depositing

Once infringement is discovered, the infringing depositing service will be invoked immediately, and the infringing website screen capture will be crawled and stored as well. All the infringement evidence will be stored on the blockchain. The system stores the infringing content through the blockchain oracle trustable service and generates rationality evidence for the depositing process that can be verified by the third party. The infringement evidence data in the blockchain can be permanently stored and cannot be tampered with.

I.1.2 Data management applied in solution

The correspondence between the copyright system and the generic reference model of blockchain-based data management is described as follows:

1) Data blockchain representation

The hash calculation and the data depositing service in the system provide the function of data blockchain representation. Through the service interface, the user as a data source submits the copyright data file, confirms the author, fills in the relevant registration information, and generates the data fingerprint hash value and timestamp of the copyright file and the related information.

2) Blockchain-based data processing

The network management service of the service layer, along with the blockchain network and the distributed storage network of the network layer provide the functions of blockchain-based data processing. After receiving the data depositing request, the nodes at the network layer perform the consensus process, generate blocks from the verified data and store them accordingly.

3) Data service provisioning

Both the data depositing service and the infringement monitoring service provide the function of data service provisioning. When the user obtains the result of the depositing, it is needed to read the depositing information on the blockchain. When the user requests digital fingerprint verification, it is needed to read the digital fingerprint of the depositing information on the blockchain. Infringement monitoring is realized by searching the digital fingerprint of the depositing information on the blockchain for comparative analysis.

4) Blockchain-based data controlling

The user management, network management, data depositing service and other functional modules of the service layer mainly provide the function of blockchain-based data controlling, which serves as the user management of the copyright system, the control of the number and content of copyright submission, and the runtime management of blockchain network.

5) Blockchain-based data monitoring

The user management, network management, data depositing service of the service layer and the data monitoring of the application layer mainly provide blockchain-based data monitoring function. They provide a visual platform for supervisors to monitor the operation of the copyright blockchain network, and the information of copyright data on the blockchain.

On this basis, reference points of the functional entities and actors such as copyright data source, copyright data users and platform operators are very important as well. The following are some of the key reference points:

– R2D connects copyright data blockchain representation functional entity and the copyright data source. This interface needs to deliver the copyright source data for computing data hash and data integration.

– U2S connects copyright data blockchain representation functional entity and the copyright data source. This interface mainly presents authentic copyright information to data users, including the copyright author, authentication time, copyright data name and data hash.

– O2M connects blockchain-based copyright data operating and monitoring functional entity and the copyright platform operator. This interface provides operator authentication, user management, copyright data query and other functions for platform operators.

I.1.3 General copyright depositing certificate flow

The process of copyright depositing certificate is as follows:

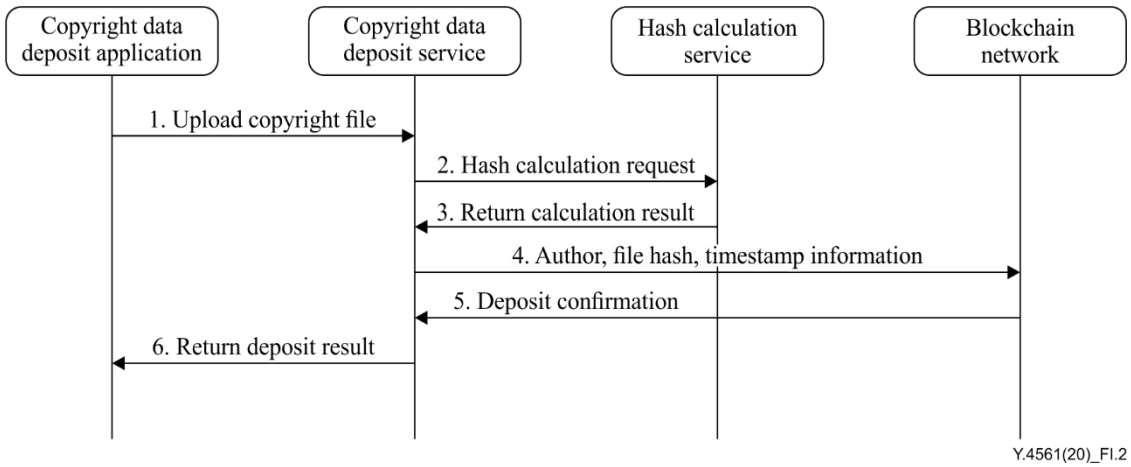

Figure I.2 – Copyright depositing certificate flow

- Step 1, the copyright file is uploaded from the copyright data deposit application to the copyright data deposit service.
- Step 2, the copyright data depositing service send the file to the hash calculation service to calculate the file hash.
- Step 3, the hash calculation service completes the hash calculation and returns the result to the copyright data depositing service.
- Step 4, the copyright deposit service integrates information such as author, file hash, timestamp, and stores the information on the blockchain.

- Step 5, the copyright depositing service obtains and confirms the result of the copyright depositing on the blockchain.
- Step 6, the copyright depositing service returns the depositing information to the user.

I.2 E-government service data sharing

With the continuous expansion and development of government informatization, the government has the urgent need of trans-regional and high-efficiency management and service capabilities. However, the traditional mode of centralized information management system encounter problems in the aspects of regional restriction, trust, service stability and comprehensive information collection.

Relying on the characteristics of block chain technology, the government service data sharing system based on the block chain technology can carry out the collection and trust transfer of service data among different government sectors. It improves the efficiency of government management and service, improve the anti-counterfeiting ability of license information, and provides more efficient and stable services to the public.

I.2.1 Overview of solution

The functional architecture of the e-government service data sharing system is depicted in Figure I.3.

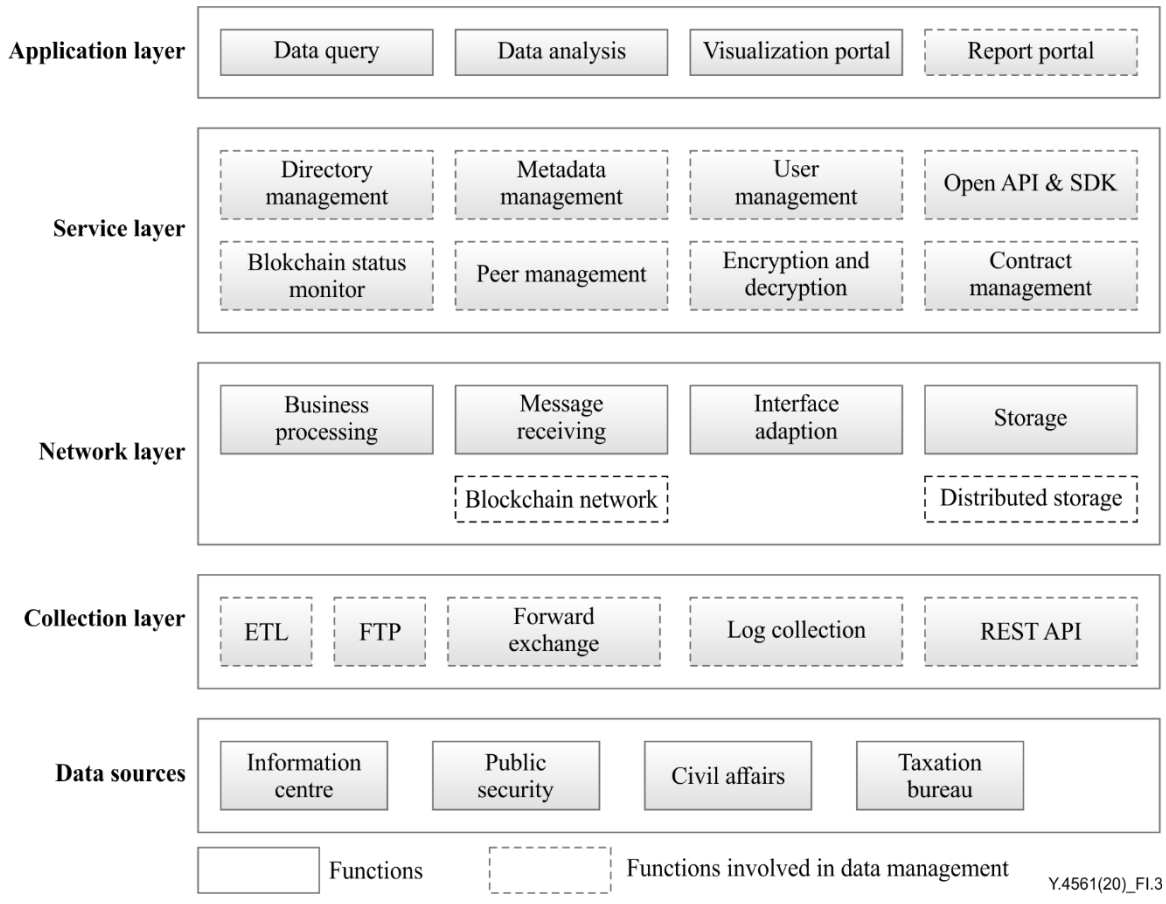

Figure I.3 – The functional architecture of e-government system

The description of the function modules is as follows:

(1) Application layer

Providing applications to different kinds of users, including:

- Data query: provide single or multiple queries for associated data, depending on the business type and data field,
- Data analysis: use appropriate statistical methods to analyse the large amount of collected data, extract useful information and form conclusions, and summarize the data in detail,
- Visualization portal: the collected data can be observed from different dimensions for further observation and analysis, and presented by visual interface,
- Report portal: display and analyse common visualization scenarios in reports, to help users utilizing the data for decision-making.

(2) Service layer

This layer is responsible for executing the underlying services, processing business logic by running smart contract, including the following services:

- Directory management: define government service data directory, provides access control, encryption and decryption control functions,
- Metadata management: provides metadata data for various services,
- User management: provide management to different users,
- Open API & SDK: provide a set of API and SDK interface services for the applications,
- Blockchain status monitoring: monitor the normal operation status of the chain,
- Peer management: is responsible for linking different nodes of the blockchain, and manage to access them through peer-to-peer network,
- Encryption and decryption: invoke encryption machine service or software to implement encryption and decryption function,
- Contract management: deploy, release, review the smart contracts.

(3) Network layer

Building a blockchain network and a distributed file storage network, including the following functions:

- Business processing

Use gRPC [b-gRPC] to establish the connection with blockchain and complete user verification, data security verification and data integrity verification, in order to support data transaction and query of blockchain.

- Message receiving

Use the message interface protocol, and the message is HTTP encapsulated and only visible between the sender and the receiver.

- Interface adaptation

Provide RESTful/WebService [b-WebService] interface adaption services such as Gossip [b-Gossip] protocol.

Distributed storage

Decentralized, multi-node distributed storage management.

(4) Collection layer

Responsible for the unified collection of data sources, including the following functions:

- Extract transform load (ETL): process extracting, transforming and loading data from the source to the destination,
- File transfer protocol (FTP): transfer files by FTP protocol,
- Forward exchange: provide data format conversion, connection management, business flow management,
- Log collection: collect a large number of logs (generally streaming data, such as page view of search engine, query, etc.) generated during the daily operation of the system,
- RESTful API: extract different data sources through RESTful API interface.

(5) Data sources

Connecting the blockchain through the nodes of information centre, government sectors such as public security, civil affairs, taxation bureau, providing all kinds of information including public security, civil affairs, personnel, labour and social security, health care, education, and citizen cards, tax and so on.

I.2.2 Data management applied in solution

The correspondence between e-government system and the generic reference model of the blockchain-based data management is described as follows:

(1) Data blockchain representation

The functions of the collection layer and the metadata management of the service layer provide the function of data blockchain representation. All data sources submit the information data through interfaces provided by the collection layer.

(2) Blockchain-based data processing

The functions of the network layer, and the encryption and decryption function, contract management function, together provide the functions of blockchain-based data processing. After receiving the data submit request, the functions of network layer process the smart contract, perform the consensus process, generate blocks from the verified data and store them accordingly.

(3) Data service provisioning

Open API & SDK provides the function of data service provisioning. It supports the data query in the application layer.

(4) Blockchain-based data controlling

The user management, peer management, directory management and contract management of the service layer mainly provide the function of blockchain-based data controlling.

(5) Blockchain-based data monitoring

Blockchain status monitoring of the service layer and the report portal of application layer provide blockchain-based data monitoring function.

I.2.3 General e-government service data sharing flow

Figure I.4 shows the structure of the general e-government service data sharing flow.

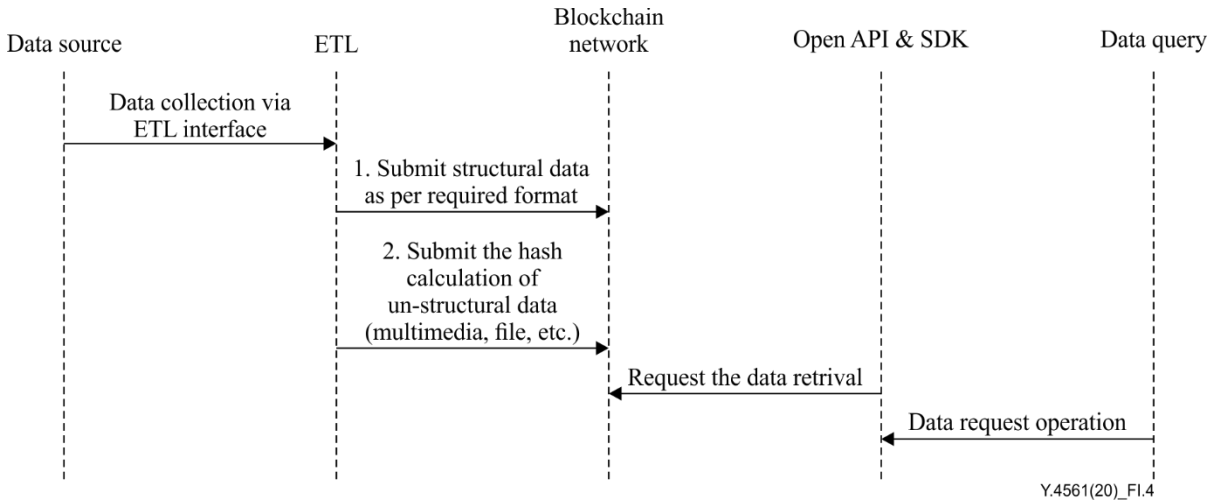

Figure I.4 – General e-government service data sharing flow

Bibliography

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

[b-ITU-T Y.4900] Recommendation ITU-T Y.4900/L.1600 (2016), *Overview of key performance indicators in smart sustainable cities*.

[b-FG-DPM TR D3.5] Technical Report D3.5 (2019), *Overview of blockchain for supporting IoT and SC&C in DPM aspects*.

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

[b-ISO/IEC TR 10032] ISO/IEC TR 10032:2003, *Information technology – Reference Model of Data Management*.

[b-Gossip] https://en.m.wikipedia.org/wiki/Gossip

[b-gRPC] https://www.grpc.io/

[b-WebService] https://en.m.wikipedia.org/wiki/Web_service

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

Printed in Switzerland
Geneva, 2020