International Telecommunication Union

ITU-T Technical Specification

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(7 April 2019)

ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities

Technical Specification D3.7

Blockchain-based data management for supporting IoT and SC&C

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 procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. ITU-T Study Group 20 set up the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) at its meeting in March 2017. ITU-T Study Group 20 is the parent group of FG-DPM.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Technical Specification D3.7

Blockchain-based data management for supporting IoT and SC&C

Summary

Along with the development of Internet of things (IoT) and Smart Cities & Communities (SC&C), different applications have the 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 emerging technology possesses the characteristics of trust, transparency, traceability and accountability and etc. It has the potential capabilities to solve the existing issues in data management.

This technical specification is to specify the requirements, generic reference model, common capabilities and procedures of blockchain-based data management.

Acknowledgements

This Technical Specification was researched and principally authored by Zheng Huang (ZTE Corporation), Xiongwei Jia (China Unicom), Subin Shen (Nanjing University of Posts and Telecommunications) and Xiaochun Yi (Ziggurat Technology) under supervision of Gyu Myoung Lee (Korea, Rep.of).

Additional information and materials relating to this Technical Specification can be found at: www.itu.int/go/tfgdpm. If you would like to provide any additional information, please contact Denis Andreev at tsbfgdpm@itu.int.

Keywords

blockchain; data management; Internet of Things(IoT); Smart Cities & Communities (SC&C); reference model; requirement; capability

Technical Specification D3.7

Blockchain-based data management for supporting IoT and SC&C

Table of Contents

Technical Specification ITU-T D3.7

Blockchain-based Data Management for supporting IoT and SC&C

1 Scope

This technical specification provides technical descriptions and specifications of the blockchain-based data management in IoT and SC&C application domains.

The scope of this technical specification includes:

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

NOTE – For Data management approaches based on blockchain, see Appendix I.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Technical Specification. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Technical Specification 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 Technical Specification does not give it, as a stand-alone document, the status of a Recommendation.

[ISO/IEC TR 10032] ISO/IEC TR 10032 (2003), *Information technology — Reference Model of Data Management*

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

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

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

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

3 Definitions

3.1 Terms defined elsewhere

This Technical Specification use the following terms defined elsewhere:

3.1.1 data management [ISO/IEC TR 10032:2003, 2.26]:
the activities of defining, creating, storing, maintaining and providing access to data and associated processes in one or more information systems.

3.1.2 application [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.

3.1.3 Internet of Things (IoT) [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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

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

3.1.5 smart sustainable city [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.

3.1.6 blockchain [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.

3.2 Terms defined in this document

None.

4 Abbreviations and acronyms

This Technical Specification uses the following abbreviations and acronyms:

IoT	Internet of things
SC&C	Smart cities and communities

5 Conventions

In this technical specification:

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

6 Requirement of blockchain-based data management

In the context of the IoT and SC&C, from applications point of view, requirements of data management based on blockchain need to be specified. Then, generic reference model, functional entities, and their capabilities and interactions are specified as per the requirements.

6.1 Introduction

6.1.1 Data management from application perspective

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

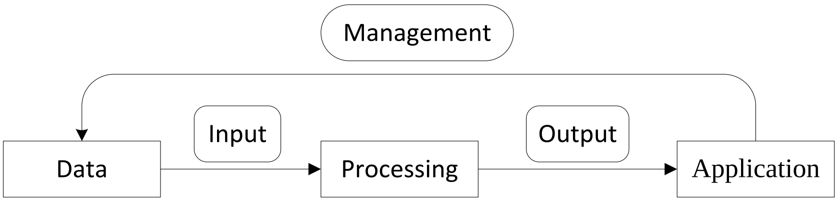

Figure 1 – Introduction of data management in data life cycle

In Figure 1, data can be raw data collected by the IoT or processed data from the IoT application, and it need to be collected and integrated in advance to create the appropriate input. Processing procedure fulfils management and converting of data from input state through to the required output which requested by different kinds of applications. During the whole data life cycle, following stages needed to be under control:

- 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 Characteristic of blockchain from data management perspective

Blockchain is distinguished by following characteristics:

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

Each characteristic can be adopted to improve the certain aspect of data management:

- Decentralized mechanism can be adopted to avoid 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 data recovery and data sharing;

- Asymmetric cryptography can be adopted to enhance data confidentiality and communication security, and use the private key as digital signature to facilitate non-repudiation;
- Digital fingerprint can be adopted to enhance data integrity;
- Immutable blocks of data are recorded in a chain, tamper-proof can guarantee the data authentic.

6.2 Requirements of data management based on blockchain

6.2.1 Security requirement

It is required to enhance the secure control of IoT data when 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 pre-defined data as per application requirement into chained block after consensus, to guarantee the data authentic and immutable.

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 aggregation all the data from data sources according to specific format.

6.2.4 Data processing requirements

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

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

6.2.5 Data management requirement

It is required to open the data to authorized party and 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 secure manner.

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

7 Generic reference model of blockchain-based data management

The generic reference model of 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 blockchain-based data management are termed as “actors” of data management in this technical specification.

NOTE – The term “actors” is explained in the ITU-T Recommendation: Common requirements of the Internet of Things [ITU-T Y.2066].

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

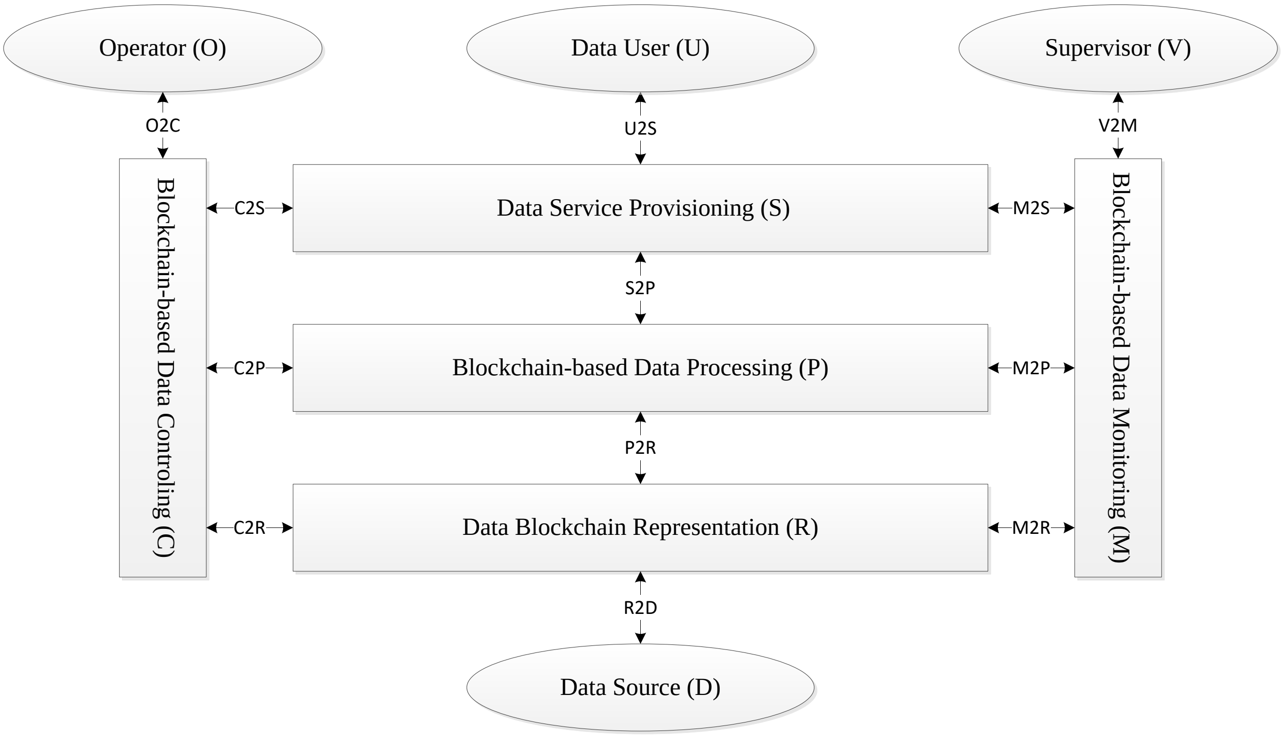
Operator (O)
Data User (U)
Supervisor (V)
O2C
U2S
V2M
Blockchain-based Data Controling (C)
C2S
Data Service Provisioning (S)
M2S
Blockchain-based Data Monitoring (M)
S2P
C2P
Blockchain-based Data Processing (P)
M2P
P2R
C2R
Data Blockchain Representation (R)
M2R
R2D
Data Source (D)

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

7.1 Data management functional entities

The generic reference model of blockchain-based data management is illustrated in Figure 1. 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, which are illustrated in the boxes in Figure 2.

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 format, integrates and encapsulates data from source into a data management operation, then encapsulates one or multiple operations into one data block. In addition, it invokes the function interfaces provided by blockchain-based data processing functional entity, and submits the processing requests to blockchain-based data processing functional entity, and receives corresponding responds.

7.1.2 Blockchain-based data processing functional entity

Blockchain-based data processing functional entity is responsible for validating authenticity of data block in data management operations and recording the validated data block into blockchain. It is responsible for processing the data management requests including data retrieval, searching, auditing. In addition, it provides the blockchain related processing capabilities including making consensus among verification nodes of blockchain network, 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

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

7.1.4 Blockchain-based data controlling functional entity

Blockchain-based data controlling functional entity is responsible for 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 for subscribing data management services.

7.1.5 Blockchain-based data monitoring functional entity

Blockchain-based data monitoring functional entity is responsible for supervision of data management capabilities according to data user's service requirements and blockchain related capabilities. It is also responsible for supervision of different data source based on data source's characteristics, and supervision of data users operations 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 ellipses in Figure 1. 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 acts the data submission operation according to the specified data format if it has the permission of the data blockchain representation functional entity. Data source actor can be personal user, organization user or IoT device or IoT application.

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 blockchain with the permission of the data service provisioning functional entity. It acts the data querying and searching 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 Blockchain-based data controlling functional entity. It acts 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 blockchain with the permission of 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 data management service categories, related parameters, and invoke methods.

7.3.2 O2C reference point

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

7.3.3 V2M reference point

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

7.3.4 R2D reference point

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

7.3.5 P2R reference point

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

7.3.6 S2P reference point

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

7.3.7 C2S reference point

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

7.3.8 C2P reference point

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

7.3.9 C2R reference point

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

7.3.10 M2S reference point

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

7.3.11 M2P reference point

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

7.3.12 M2R reference point

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

8 Common capabilities and procedure 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 blockchain-based data management as illustrated in Figure 1.

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 time-stamping 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 data block；
- Checking validation of data accessing in blockchain；
- Checking validation of data updating in blockchain；
- Verifying and storing the proved data blocks via specific consensus mechanism；
- Controlling data user in accessing and updating 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 data block；
- Searching and accessing data in Blockchain；
- Searching and accessing time-stamping in blockchain；
- Checking the validation of data stored in 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 blockchain;
- Configuring data access in blockchain;
- Checking data management configuration validation in 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 creating, updating and accessing in blockchain;
- Supervising time sequence of data stored in blockchain;
- Supervising validation of data stored in blockchain.

8.6 Data submission procedure

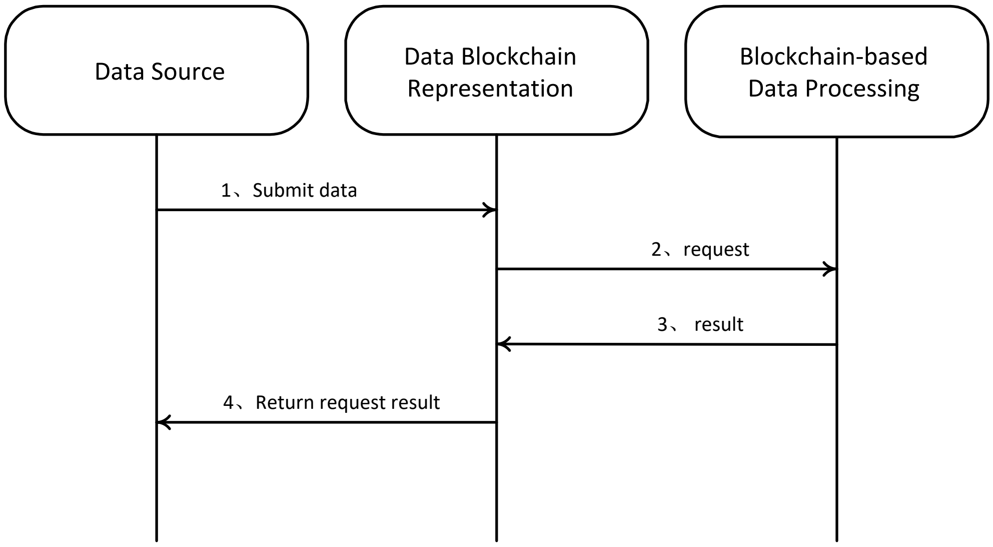

Figure 3 – Data submission procedure

- Step 1, data source actor submits the data to data blockchain representation functional entity, which collects metadata for validation according to specified data format.
- Step 2, data blockchain representation functional entity creats the data hash calculation, and sends request to 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 blockchain, and return the result to data blockchain representation functional entity.
- Step 4, data blockchain representation functional entity returns the request result to data source actor.

8.7 Service request procedure

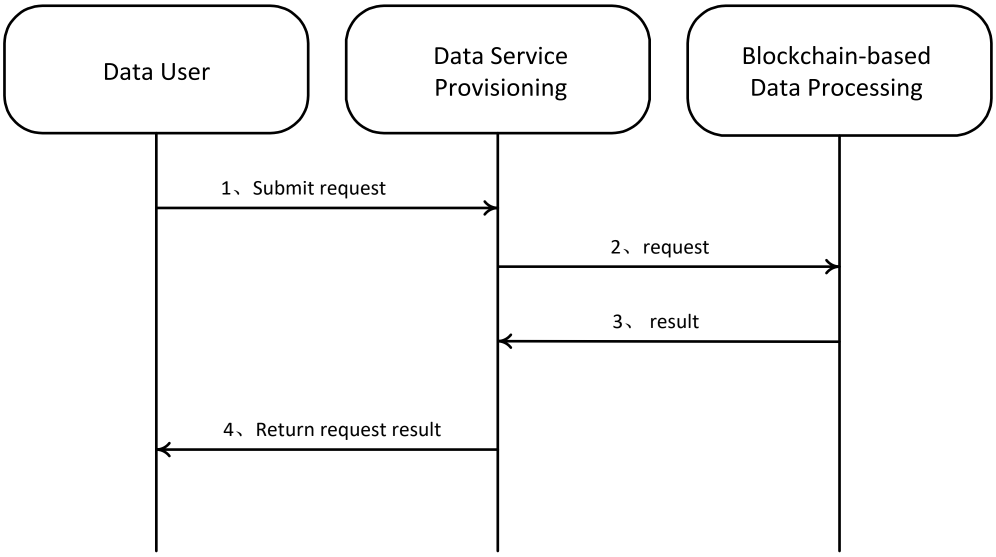

Figure 4 – Service request procedure

- Step 1, data user actor submits the service request to data service provisioning functional entity.

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

8.8 Controlling procedure

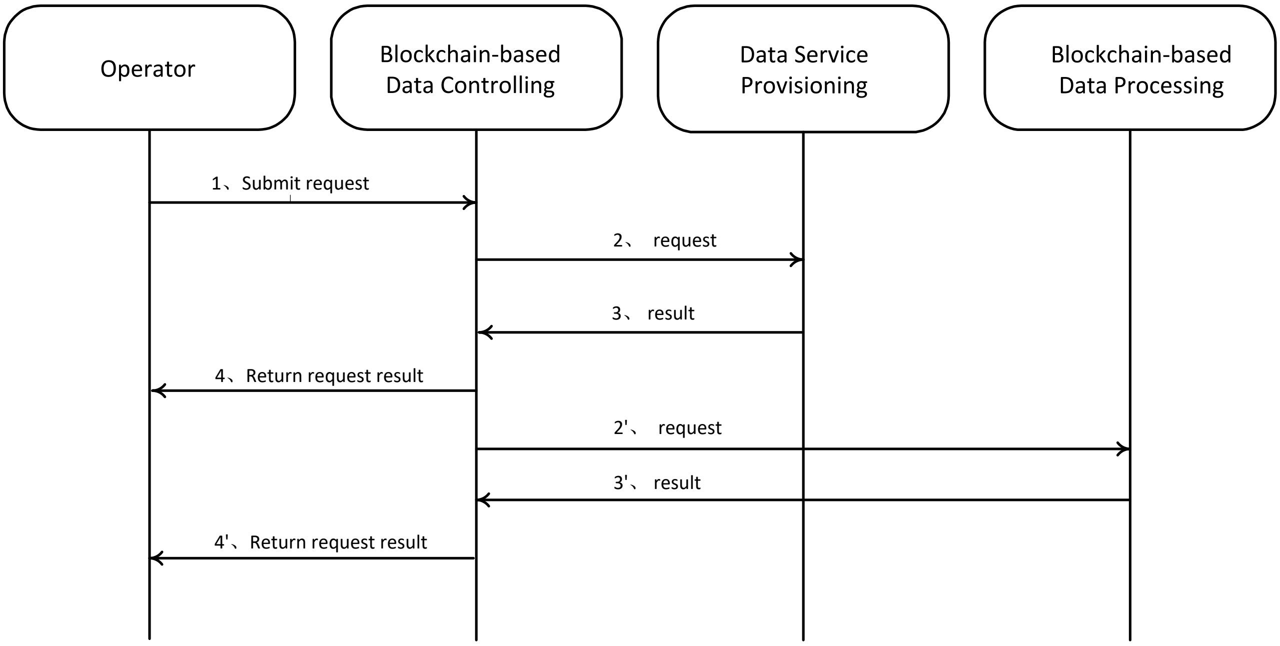

Figure 5 – Controlling procedure

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

Alternative procedure:

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

8.9 Monitoring procedure

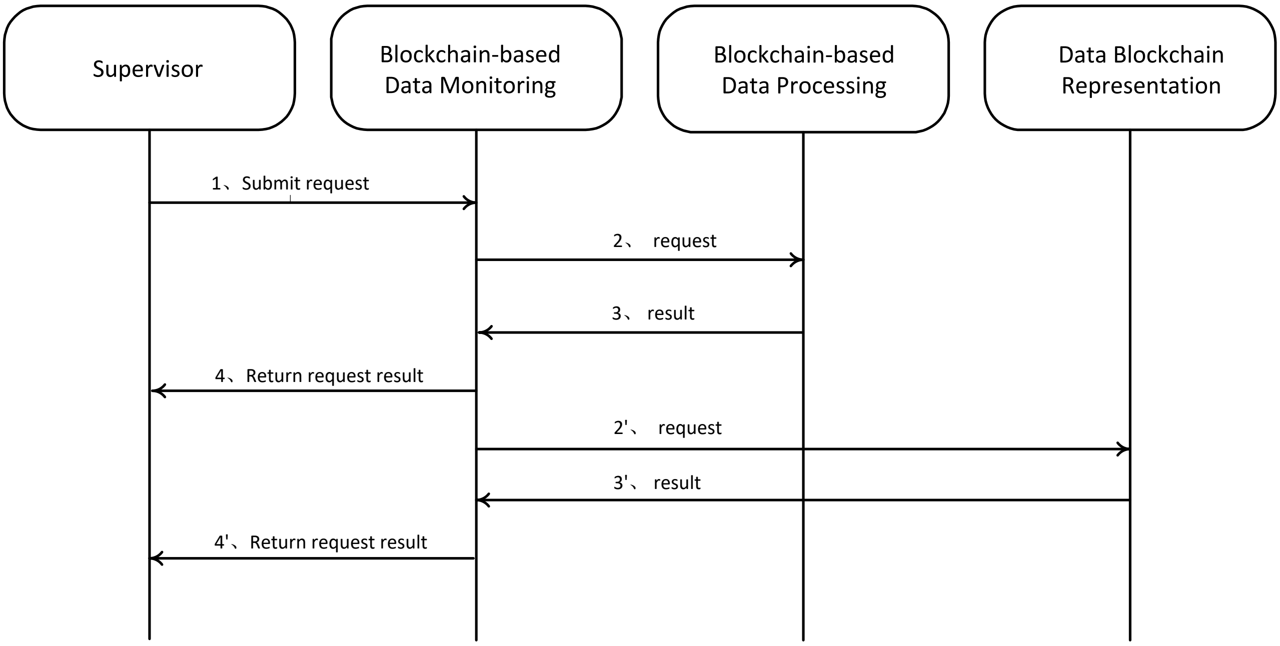

Figure 6 – Monitoring procedure

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

Alternative procedure:

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

Appendix I
Data management approaches based on blockchain

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

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 fast spreading 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 copyright system is shown below.

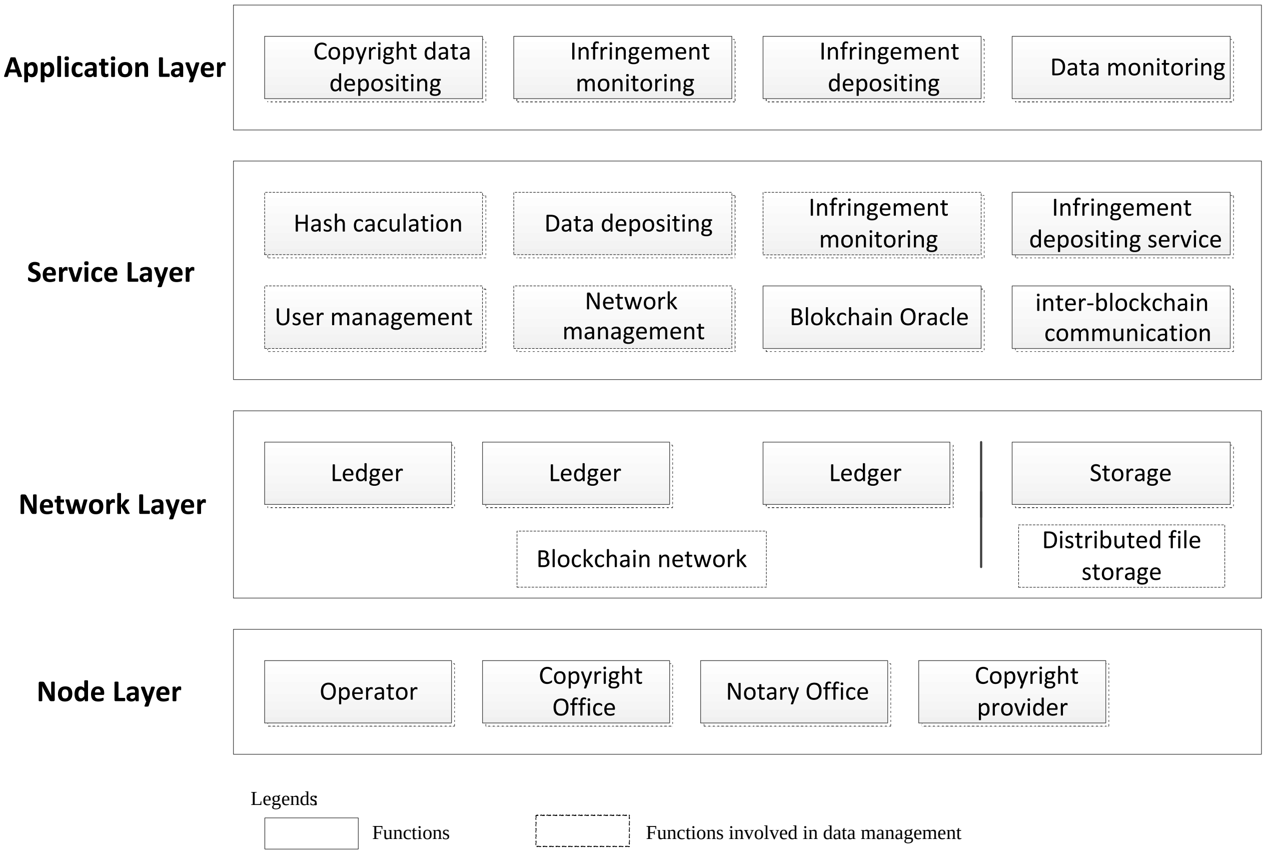

Figure I-1 – The functional architecture of copyright system

The functional architecture of 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 following:

1, Copyright data depositing

The user submits the registration application with required information, such as the applicant, the author and the content of the copyright, to the copyright system. Based on 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 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

Firstly, 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 analyzed. 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 copyright system and the generic reference model of blockchain-based data management is described as following:

(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 realizes 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 will describe some of the key reference points.

1, 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.

2, 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.

3, 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:

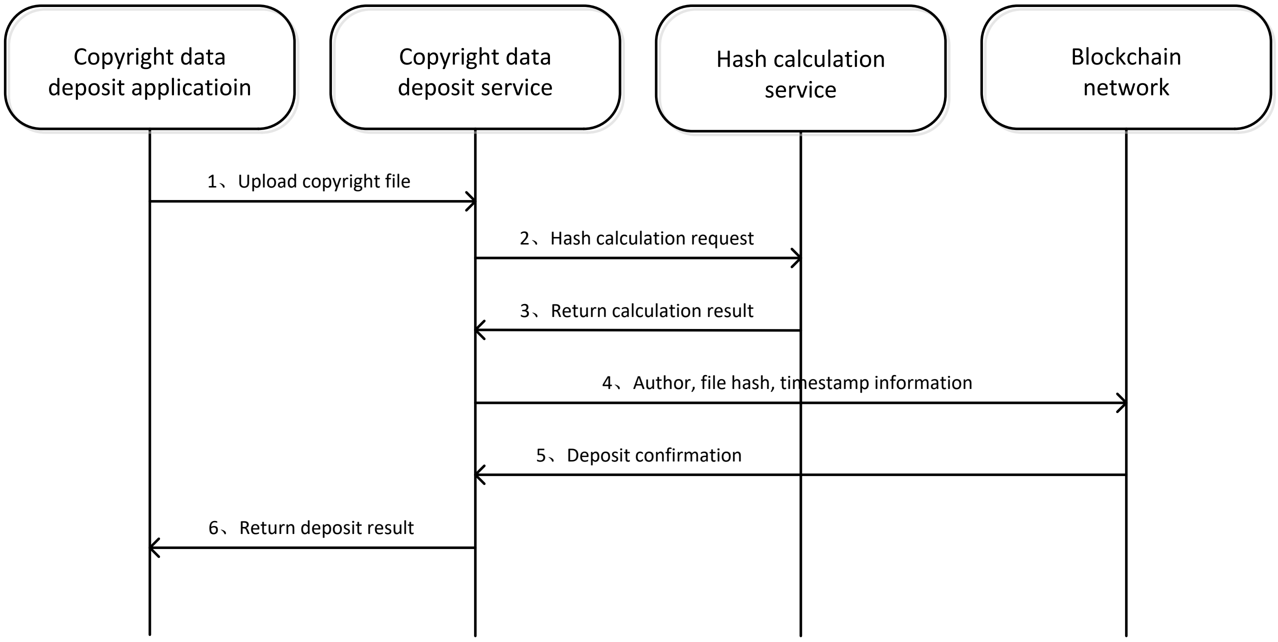
Copyright data deposit applicatioin
Copyright data deposit service
Hash calculation service
Blockchain network
1、Upload copyright file
2、Hash calculation request
3、Return calculation result
4、Author, file hash, timestamp information
5、Deposit confirmation
6、Return deposit result

Figure I-2 – Copyright depositing certificate flow

Step 1, copyright file is uploaded from copyright data deposit application to copyright data deposit service.

Step 2, copyright data depositing service send the file to hash calculation service to calculate the file hash.

Step 3, hash calculation service completes the hash calculation and returns the result to copyright data depositing service.

Step 4, copyright deposit service integrates information such as author, file hash, timestamp, and stores the information on the blockchain.

Step 5, copyright depositing service obtains and confirms the result of the copyright depositing on blockchain.

Step 6, copyright depositing service returns the depositing information to the user.

I.2 E-government service data sharing

With the continuous deepening 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 has the 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 block chain technology can realize 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 the more efficient and stable services to public.

I.2.1 Overview of solution

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

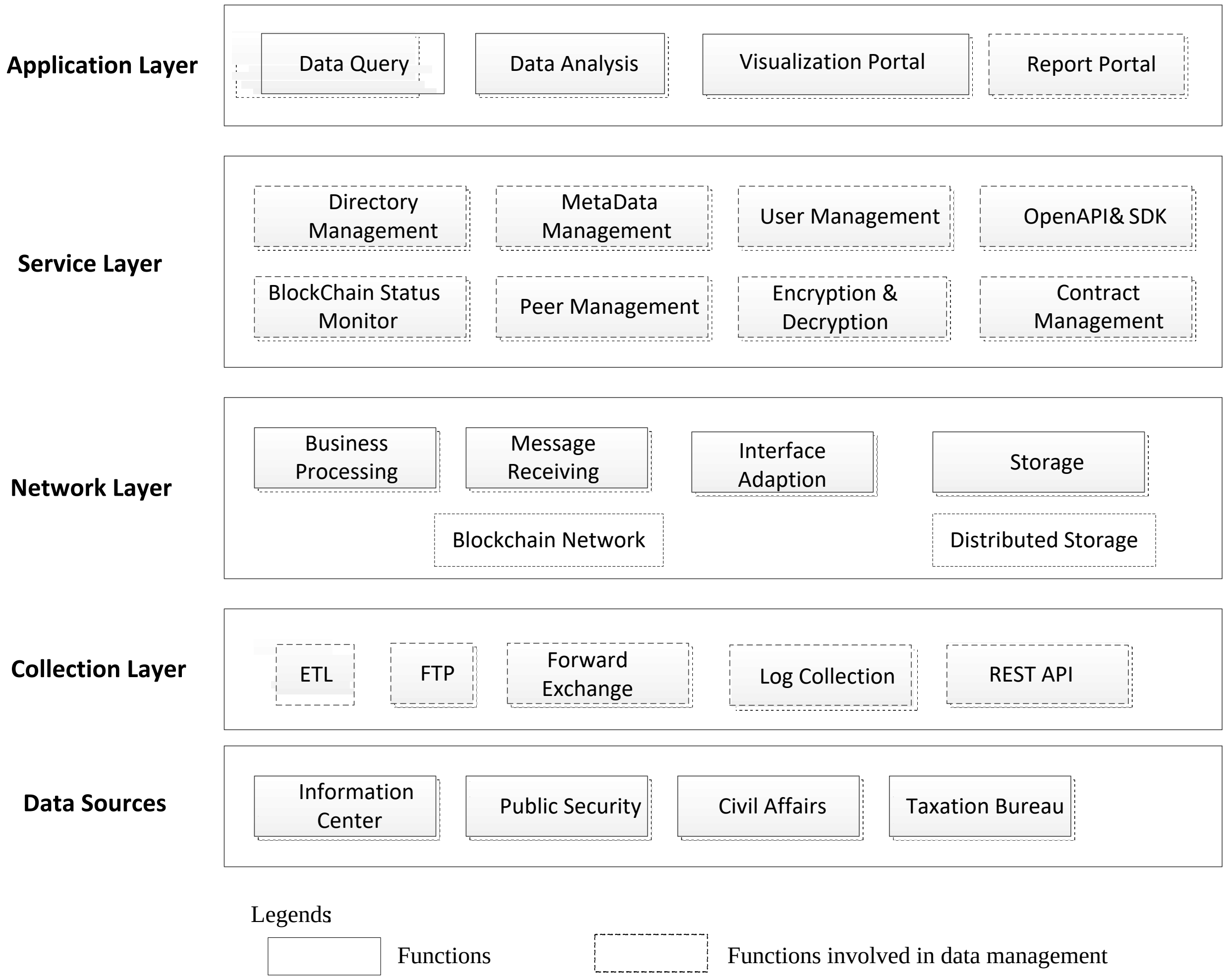

Figure I-3 – The functional architecture of e-government system

The description of 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 analyze 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 analyze common visualization scenarios in report, to help users utilizing the data for decision-making.

(2) Service layer

Responsible for realizing the underlying services, processing business logic by running smart contract, including 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;
- OpenAPI & 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: be responsible for linking different nodes of the blockchain, and manage to access them through peer-to-peer network;
- Encryption & 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 following functions:

- Business processing

Use gRPC to establish the connection with blockchain and complete user verification, data security verification and data integrity verification, so as 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 interface adaption services such as Gossip protocol.

- Distributed storage

Decentralized, multi-node distributed storage management.

(4) Collection layer

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

- ETL: process extracting, transforming and loading data from the source to the destination;
- 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 pv 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 center, goverment 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 HB-Cloud e-government system and the generic reference model of blockchain-based data management is described as following:

(1) Data Blockchain Representation

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

(2) Blockchain-based Data Processing

The functions of network layer, and encryption & 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 certain smart contract, perform the consensus process, generate blocks from the verified data and store them accordingly.

(3) Data Service Provisioning

OpenAPI & SDK provides the function of data service provisioning. It supports the data query in 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 monitor of service layer and report portal of application layer provide blockchain-based data monitoring function.

I.2.3 General e-government service data sharing flow

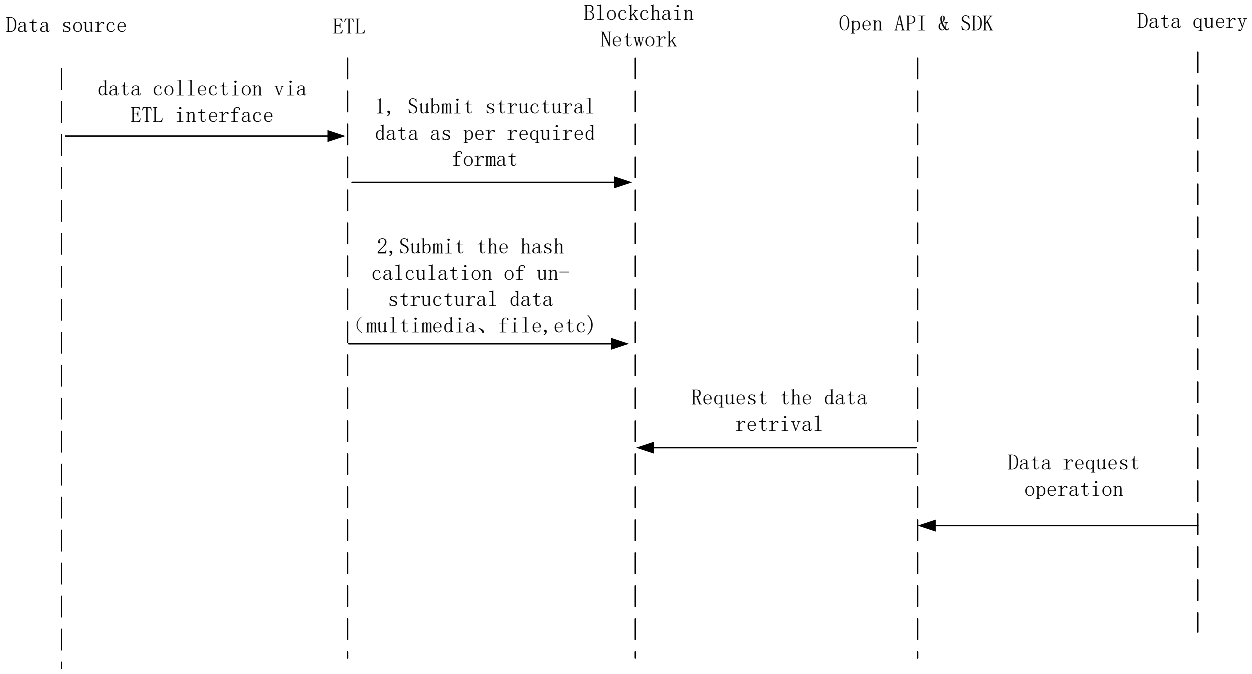
Data source
ETL
Blockchain Network
Open API & SDK
Data query
data collection via ETL interface
1, Submit structural data as per required format
2,Submit the hash calculation of un-structural data（multimedia、file,etc)
Request the data retrival
Data request operation

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