International Telecommunication Union

ITU-T Technical Specification

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(19 July 2019)

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

Technical Specification D3.6
Blockchain-based data exchange and sharing 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 D3.6

Blockchain-based data exchange and sharing for supporting IoT and SC&C

Summary

Blockchain is an emerging technology and its most important characteristics are traceable, un-erased. It is able to efficiently ensure integrity, authenticity, and auditability of all transactions. Blockchain has an important impact and benefits for data exchange and sharing to support IoT and smart city and communities (SC&C). In most of the IoT and SC&C scenarios, it is needed to ensure data processing, circulation, sharing and management to be all trust operations. Blockchain technologies can meet the needs.

This Technical Specification is to specify the requirements, functional models, a platform and deployment modes of blockchain-based data exchange and sharing for supporting IoT and SC&C.

Acknowledgements

This Technical Specification was researched and principally authored by liangliang ZHANG (Huawei) Xiongwei Jia (China Unicom), Hui DING (Chaincomp Technologies) and Yuan Tao (Computer Network Information Center, Chinese Academy of Sciences) 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 sharing; data exchange; functional mode; Internet of Things (IoT); Smart Cities & Communities (SC&C)

Technical Specification D3.6

Blockchain-based data exchange and sharing for supporting IoT and SC&C

Table of Contents

Technical Specification ITU-T D3.6

Blockchain-based data exchange and sharing for supporting IoT and SC&C

1 Scope

This Technical Specification provides technical descriptions and specifications of blockchain-based data exchange and sharing in Internet of things (IoT) and smart city and communities (SC&C) application domains.

The scope of this technical specification includes:

- Overview of blockchain in data exchange and sharing;
- Requirements for blockchain-based data exchange and sharing;
- Functional models of blockchain-based data exchange and sharing;
- Platform of blockchain-based data exchange and sharing;
- Deployment modes for blockchain-based data exchange and sharing.

NOTE – For data exchange and sharing approaches are 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 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.

[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 uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 blockchain data [FG-DPM TR D3.5]: The data in a blockchain, such as distributed append-only ledgers, state information, permission policies etc.
NOTE – Blockchain data may be distributed and be stored in blockchain peers. A blockchain peer may store whole or part of the data in a blockchain.
3.1.3 blockchain peer [FG-DPM TR D3.5]: A functional entity or physical entity (e.g., device, gateway and system) which utilizes blockchain-related functionalities (e.g., executing transactions, and maintaining the blockchain data) in peer to peer communications.
3.1.4 blockchain transaction [FG-DPM TR D3.5]: An operation (e.g. deploying, invoking and querying results of blockchain contracts) in a blockchain in which an authorized end user performs operations (e.g. reading/writing blockchain data, invoking a blockchain contract).
3.1.5 consensus: Agreements to confirm the correctness of the blockchain transaction.
3.1.6 data sharing [FG-DPM TS D0.1]: The process of data exchange among different parties with specified conditions.
3.1.7 data exchange [FG-DPM TS D0.1]: Data exchange: Accessing, transferring and archiving of data.

3.1.8 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.

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

3.1.10 smart contract [FG-DPM TR D3.5]: Embedded logic that encodes the rules for specific types of blockchain transactions. A smart contract can be stored in the blockchain, and can be invoked by specific blockchain applications.
3.1.11 thing [ITU-T Y.4000]: In the Internet of Things, object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this technical specification

None.

4 Abbreviations and acronyms

This technical specification uses the following abbreviations and acronyms:

DPM Data processing and management

IoT Internet of things

SC&C Sustainable smart city and communities

M2M Machine to machine

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.
- The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement needs not be present to claim conformance.
- The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of blockchain in data exchange and sharing

6.1 Positive impacts of blockchain in data processing and management

The IoT consists of a global network of billions of uniquely identifiable and addressable objects, embedded with transducers (e.g. sensors, actuators, and controllers) and connected to the Internet.

The blockchain is widely acknowledged as a potential solution for enhancing current centralization, privacy and security problems when storing, tracking, monitoring, managing and sharing data. The blockchain usually consists of one or multiple distributed ledger(s) which contain(s) all transactions ever executed within their network(s), enforced with cryptography and carried out collectively by peer-to-peer workgroup(s). The blockchain is a trust-free, tamper-proof, auditable, and self-regulating system, with no human intervention required to execute computations.

Blockchain will have a group of positive impacts for data processing and management to support IoT and SC&C:

- Generally, IoT is peer to peer network, the multi-centre, weak centre characteristics of blockchain are suitable for IoT network. And blockchain can help the central structure will reduce the high operation and maintenance costs, especially when using blockchain on data exchange and data sharing.
- Consensus in blockchain would help to identify illegal nodes and prevent malicious access, thus it is good to support device security, and further to improve data security.
- Relying on the chain structure and distributed architecture of blockchain, it helps to break the existing data information islands of the IoT, and promote the horizontal flows of information and multi-party collaborations.
- As the backbone of all these interactions, blockchain creates a secure and democratized platform that is independent and levels the field for all involved parties, making sure everyone plays fair.
- The information encryption, secure communications in blockchain would help data security, protect privacy, and identity rights management.
- Blockchain makes data auditable and traceability. Blockchain supports audit trails on data storage and data transaction, to improve the trustworthiness of the data and the data transaction. Blockchain makes data and data transactions auditable. Once the data or transaction is recorded in the blockchain, it can’t allow be detected and rejected by the other nodes in the network. In addition, with using timestamp, the data in blockchain is traceable.

- Blockchain may support data monetization, where owners of IoT devices and sensors may share the generated IoT data in exchange for real-time micropayments.

6.2 Benefits of using blockchain to support data exchange and sharing

6.2.1 Blockchain making data trusted to support data exchange and sharing

In the IoT and SC&C scenarios, it is very important to build a trusted IoT framework to ensure data processing, circulation, sharing and management to be all trust operations. And smart city requires the exchange of credit relations. Trust and credit are the basis of all IoT transactions.

The blockchain technologies are arising, which have the specific characteristics as follows: trust, transparency, highly resistant to outage, tamper-proof, auditable, and self-regulating system. The blockchain is able to efficiently ensure integrity, authenticity, and auditability of all transactions. It could hence help to make data trusted to support data exchange and sharing:

- **Realise trusted transaction between the parties:** Blockchain could make distrusted parties to realise trusted transaction, and finally to reach trust relationship between the parties. So as long as a trust relationship is required, the blockchain can be used. Being trusted is the most important characteristic for the blockchain when it is applied in various application scenarios.
- **Data's terminal device became trusted**: Consensus in blockchain would help to identify illegal nodes and prevent malicious access, it helps to guarantees data's terminal device trusted.
- **Data becomes trusted and verifiable:** Data becomes trusted and verifiable, and can be traced back to the origination based on blockchain.
- **Trusted data storage:** Blockchain itself is an untampered database storage technology. The data can be recorded directly on blockchain, or be encrypted by blockchain technology before storing in distributed databases.

6.2.2 Blockchain making data transaction trusted to support IoT and SC&C

In data transmission and circulation, blockchain enables trusted data transmission and circulation:

- **Trusted data asset transfer:** The blockchain may enable trusted micro-payments and automated transfer of assets between IoT devices, through cryptocurrencies and smart contracts. Each data asset transfer could be one transaction in blockchain. All these transactions are traceable. And based on cryptographic protocols, the blockchain is able to effectively protect integrity, authenticity, auditability and consistency of all transactions. So blockchain can make the process of data asset transfer more safe, convenient, reliable, and trusted.
- **Safeguard related rights and interests of data owners:** Smart contracts technology in blockchain make data assets transaction easy, fair, reasonable in blockchain network; in addition, the private-key encryption, digital signature of data owners guarantee their ownership, and the authentication of data assets can be recorded in the blockchain, which can be used for rights protection.

6.3 Roles of blockchain in data exchange and sharing

The most important characteristics of blockchain are un-tampered and traceable. Therefore, in a multi-parties' cooperation scenarios, they need to rely on a trusted third party to share trusted data information which impacts the cooperation between parties. However, at times there is no trusted third party, or the cost of trusted third-party entities are too high, or the effect of utilizing trusted

third-party entities is not ideal. In this situation, the blockchain would offer a potentially viable optimized solution and it would help to optimize procedures, improve efficiency and reduce cost, etc.

The roles of blockchain in data exchange and sharing in IoT and SC&C are as following:

- Blockchain can be used in data exchange and sharing for achieving data asset transaction as well as safeguarding related rights and interests of data owners.
- Blockchain can be used for sharing the trusted information in a multilateral collaboration scenario. It is helpful to optimizer procedures, improve efficiency or reduce cost specially when there is no trusted third party, or when the cost of trusted third-party entities is too high or the effect is not ideal.

7 Requirements for blockchain-based data exchange and sharing

7.1 General requirements

7.1.1. Scalability

- It is required to enable to support different services for realizing data exchange and sharing in one blockchain or in different blockchains.

7.1.2 Trusted data storage

- It is required that data and records for data exchange and sharing are stored in a secure and tamper-resistant manner with the capability to report on it for audit purposes.

7.1.3 Trusted identification

- It is recommended to provide distributed identification for allowing each stakeholder to participate in the identification manage process.
- It is required to maintain the identification throughout the lifecycle.

7.1.4. Interoperability

- It is required to provide interoperability between different blockchains.

7.1.5 Data security

- It is required to provide data security for support trusted data transmission and circulation.
- It is required to keep tamper detection of data.
- It can optionally use data encryption, digital signature, data’s figureprint to ensure data security.

7.2 Requirements of interoperability

7.2.1 Unified Data format for blockchain-based data exchange and sharing

- It is required to provide unified data format during data exchange and sharing in different blockchain.

NOTE - It needs to address the following attributes of the system, including but not limited to, data structure, data element format, data type, identifier and data length and so on.

7.2.2 Unified cross-blockchain identity

- It is recommended to provide uniform cross-blockchain identity among all blockchains which support cross-blockchain operation in the same IoT platform or between different IoT platform.

7.2.3 Cross-blockchain transaction

- It is required to provide cross-blockchain transaction among all blockchains which support cross-blockchain operation.
- It is required to record data sharing operation between different blockchains in cross-blockchain transaction.

7.2.4 Atomicity between different blockchains

- It is required to keep the atomicity between different blockchains via keeping all executions of data sharing operation during cross-blockchain are successful or all executions fail.

7.2.5 Security on cross-blockchain operation

- It is required to ensure that data exchange and sharing operation of cross-blockchain is trusted and safe.
- It is required to enhance the secure control on operation of cross-blockchain (e.g., keeping operation of cross-blockchain confidentiality and traceability).

8 Functional models of blockchain-based data exchange and sharing

The functional models of blockchain based data exchange and sharing include security and privacy function, trusted data collection function, distributed data processing function, data sharing and sharing function.

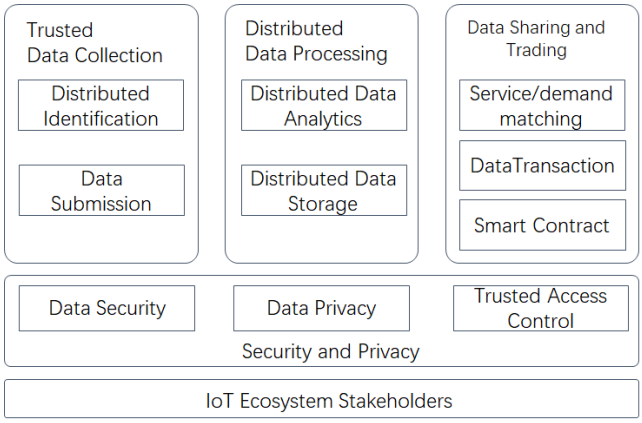


Figure 8-1 Functional models of blockchain-based data exchange and sharing

8.1 Trusted data collection function

It provides trustworthy data from the data source. It includes distributed identification and data submission function.

- **Distributed identification function:** It provides blockchain-based identification mechanism and enables each stakeholder to participate in the trusted identification management instead of traditional centralized authority identity management.
- **Data submission function:** It provides blockchain-based integrated, auditable and traceable data collection mechanism for IoT devices.

8.2 Distributed data processing function

It transfers raw data to meaningful information for reliable decision-making. The sub-functions include:

- **Distributed data storage function:** It provides distributed storage that are hosted by different entities based on blockchain.
- **Distributed data analytics function:** It provides time-efficient computation and analysis, especially for time-sensitive tasks.

8.3 Data sharing and trading function

It provides a mechanism for IoT data sharing and trading with flexible rules and transaction methods. The sub-functions include:

- **Supply/demand matching function:** It provides different rules for the data provider to find a matching data demander.
- **Data transaction function**: It enables trusted micro-payments and automated transfer of data assets between different stakeholders or different devices. It provides effectively protect integrity, authenticity, auditability and consistency of all transactions
- **Smart contract function:** It enables the exchange of data sharing and trading with rules defined in the code form, and it enforces the automatic execution of obligations between different stakeholders or different devices. It defines the rules, penalties, and rewards around the agreement in the same way a traditional contract does, and with higher execution efficiency on a trusted blockchain-based infrastructure.

8.4 Security and privacy protection function

It provides mechanisms for data security and data privacy protection throughout data lifecycle. The sub-functions include:

- **Data security function**: It provides various types of data encryption, digital signature to ensure data security.
- **Data privacy function**: It minimizes data exposure according to data rights (the right of

ownership, use, and/or earning).

- **Trusted access control function**: It enables blockchain-based authentication, authorization and accounting for accessing the data.

NOTE: Details of IoT ecosystem stakeholders are described in clause 9.1.

9 Blockchain-based data exchange and sharing platform

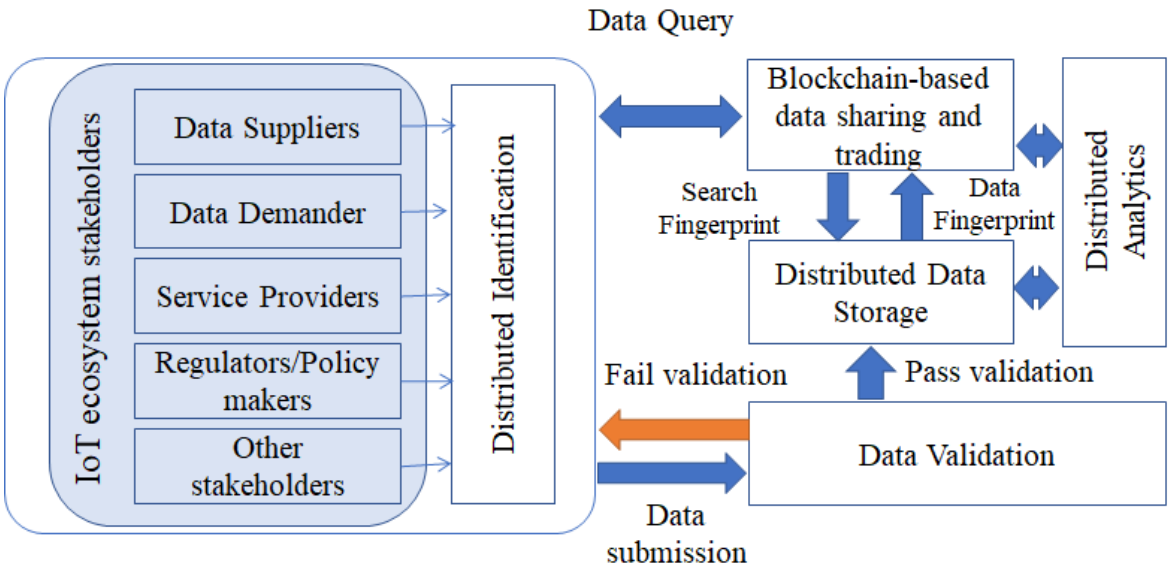


Figure 9-1 Blockchain-based data exchange and sharing platform

9.1 IoT ecosystem stakeholders

A typical IoT ecosystem usually consists of multiple stakeholders with different roles and interests, and each of them can provide different types of data to the ecosystem. It includes data suppliers, data buyers, services providers, regulators/policy makers and others.

- **Data suppliers**: Data suppliers send/sell data to data demander. They either own various IoT devices and collecting data from their devices, or they are authorized to access and share/sell the data to data demanders.
- **Data demanders**: Data demanders receive/purchase data from data suppliers.
- **Service providers**: Service providers support the operations of blockchain-based IoT data exchange and sharing platform.
- **Regulators/Policy makers**: Regulators/policy makers are usually government agencies that supervise regulation compliance and issue certificates (e.g. operation permission, quality assurance, etc.).
- **Other stakeholders**: Other stakeholders may include consulting agency, insurance company, etc.

9.2 Distributed Identification

Every stakeholder may own a number of IoT devices and each device is uniquely identified. All stakeholders participate in the distributed identification management activities, which includes approval of the identifier, change of status associated with the identifier.

9.3 Data submission

Data which is generated by device, is submitted to a data validation module. Every data entry submitted is associated with its unique identifier.

9.4 Data validation

It checks and validates submitted data from stakeholders' devices. When data are submitted from one stakeholder, other stakeholders in the system will be incentivized to check the conformance. The regulators and policy makers can validate the submitted data and issue certification that will be packed with the data into the blockchain system. If the data that passes the validation would be encrypted and sent to distributed data storage. If the data doesn't pass the validation, it will be sent back to the submitter and can be submitted again after self-correction. The re-submission operation will also be recorded in blockchain.

9.5 Distributed data storage

Data which is successfully validated is stored among participating nodes and the hash of the data (also known as its fingerprint) will be stored in blockchain. The "fingerprint" is calculated with the data, any tampering to the data will alter its fingerprint, which leads to mis-match in the blockchain.

9.6 Distributed analytics

Data analytics extracts important knowledge from raw data in order for stakeholders' decision-making.

9.7 Blockchain-based data sharing and trading

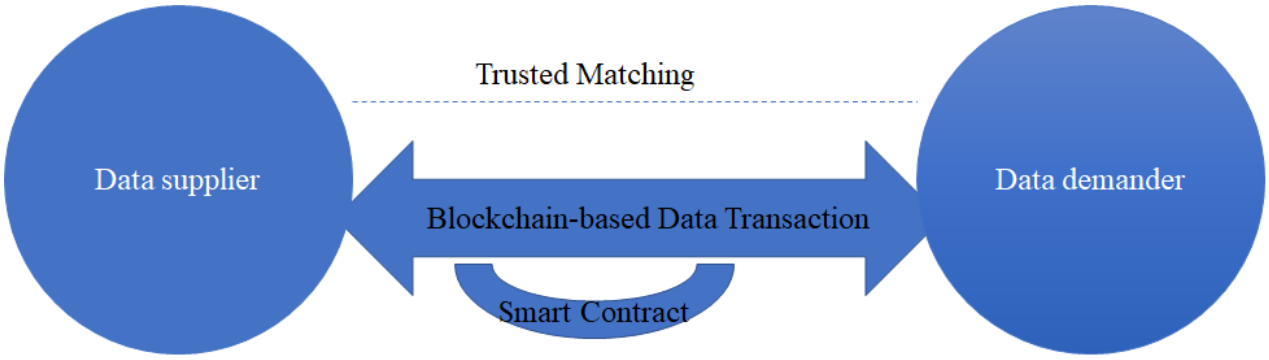


Figure 9-2 Data sharing interaction between data supplier and data demander

In blockchain-based data exchange and sharing, it contains:

- **Trusted Supply/demand matching:** It finds matching pairs for data supplier and data buyer. When a matching pair is found, they can become two parties in a blockchain-based transaction or a smart contract. The blockchain can implement a number of services' scheduling policies to optimize the matching process.

- **Blockchain-based data transaction:** It performs the data sharing or data trading process for a supplier-demander pair. The data demander queries data in the blockchain with the identifier related to data. Data's "fingerprint" is found in blockchain, and then data is retrieved via the distributed storage regarding to the data 's "fingerprint". Based on this, a data sharing transaction is initialed. And the data sharing transaction in blockchain is recorded as soon as the data sharing or data trading in completed between the demander and supplier.

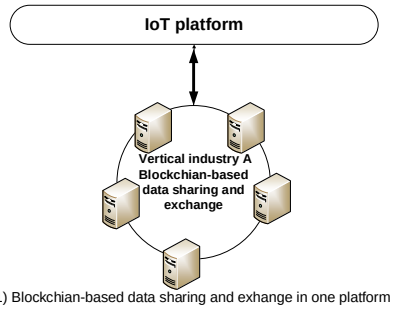
- **Smart contract:** It includes a series of pre-defined rules as contract. once the condition of the smart contract is met, smart contract is performed automatedly for data sharing or data trading in blockchain. Specially for data trading, the associated fees can be transferred from the data demander to the data supplier safely without a trusted third party in the blockchain-based data sharing platform.

10 Deployment modes for blockchain-based data exchange and sharing

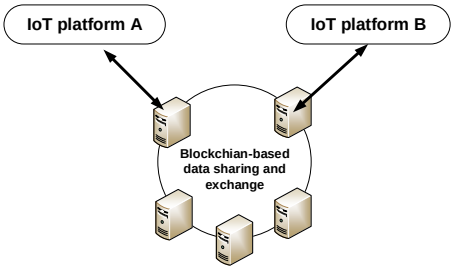
10.1 General deployment modes

The potential deployment modes of blockchain-based data exchange and sharing are as following:

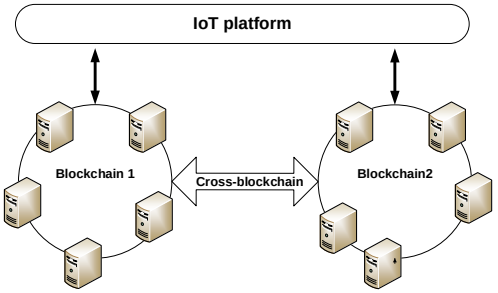
- **One blockchain in one platform:** One blockchain connects IoT platform independently for sharing data in this IoT platform.
- **One blockchain between or among different platforms:** Data exchange and sharing between/among different platforms is realized by using on blockchain. Different platforms act as one partner in this blockchain.
- **Cross blockchain in the same platform:** In the same platform, different blockchains exchange and share data via cross-blockchain. Different blockchains may respective different kind of data.
- **Cross blockchain in different platforms:** Different blockchains connect to different IoT platforms. Data exchange and sharing among different platforms is realised via cross different blockchains.



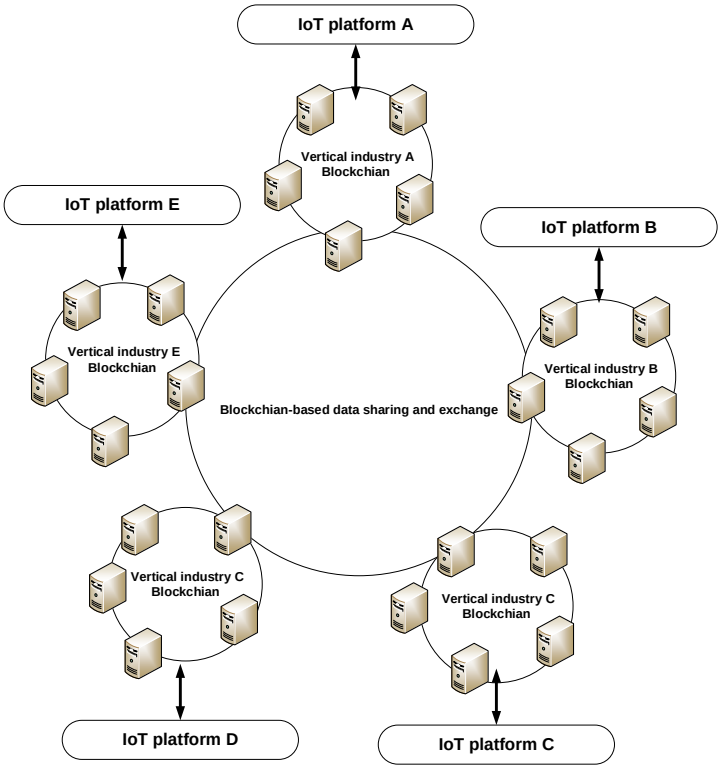
(1) Blockchian-based data sharing and exhange in one platform



(2) Blockchian-based data sharing and exhange In defferent platforms



(3) Blockchian-based data sharing and exhange via cross-blockchain in the same platform



(4) Blockchian-based data sharing and exhange via cross-blockchain in the different platform

Figure 10-1 Four general deployment modes of blockchain-based data exchange and sharing

10.2 Cross-blockchain deployment modes

In clause 10.1, Figure 10-1 shows blockchain-based data exchange and sharing via cross blockchains in the same platform or in different platforms. Regarding to cross-blockchain, the cross-blockchain deployment modes are shown as follows:

- Deployment mode 1: The nodes in blokchain1 are independent of the ones in blockchain2. The two different blockchains exchange data via smart contract.
- Deployment mode 2: Blokchain1 connects with blokchain2 via one trusted node.
- Deployment mode 3: Several nodes of blockchain1 are the nodes of blockchain2.

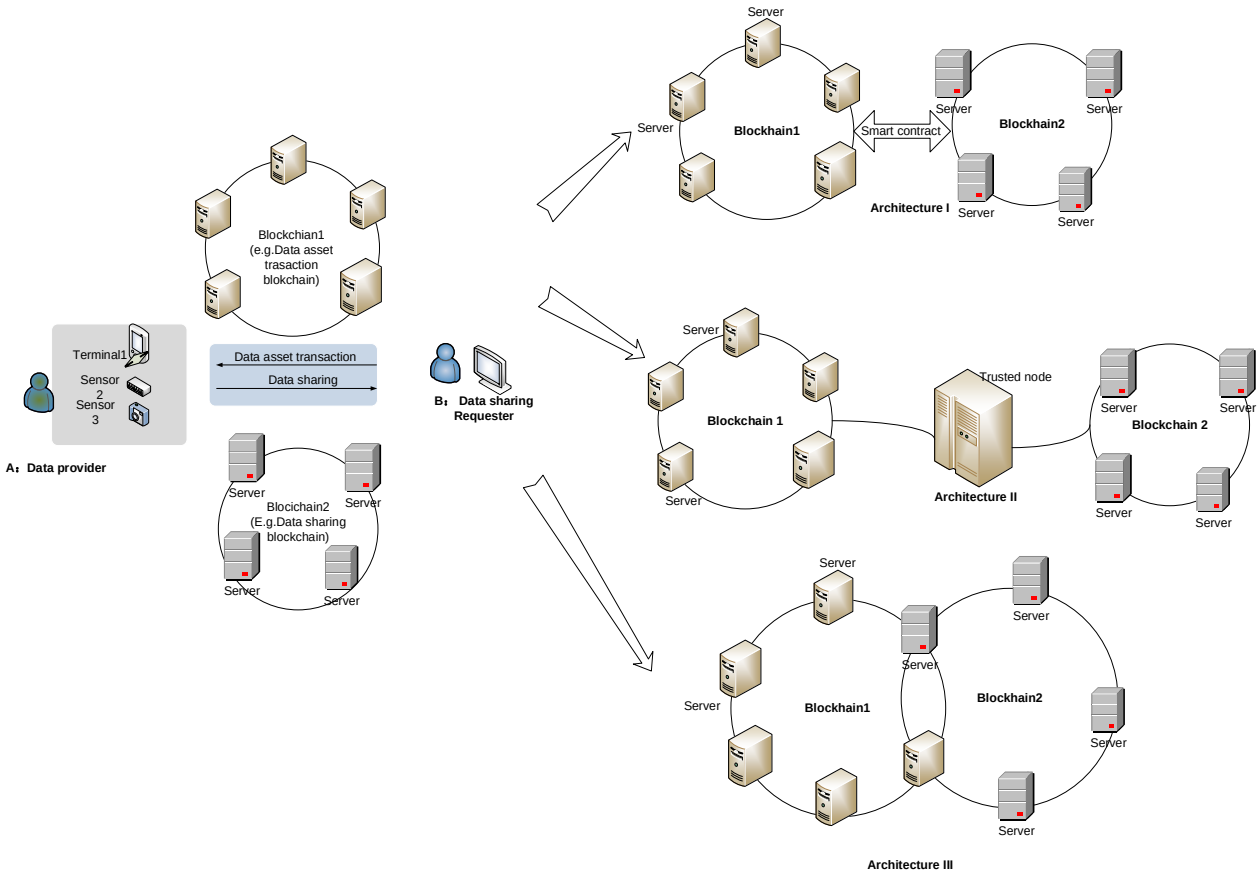


Figure 10-2 Deployment modes of cross-blockchain for blockchain-based data exchange and sharing

Appendix I

Data exchange and sharing approaches based on blockchain

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

I.1 Blockchain-based IoT data sharing in supply chain traceability

I.1.1 Challenges of blockchain-based supply chain traceability

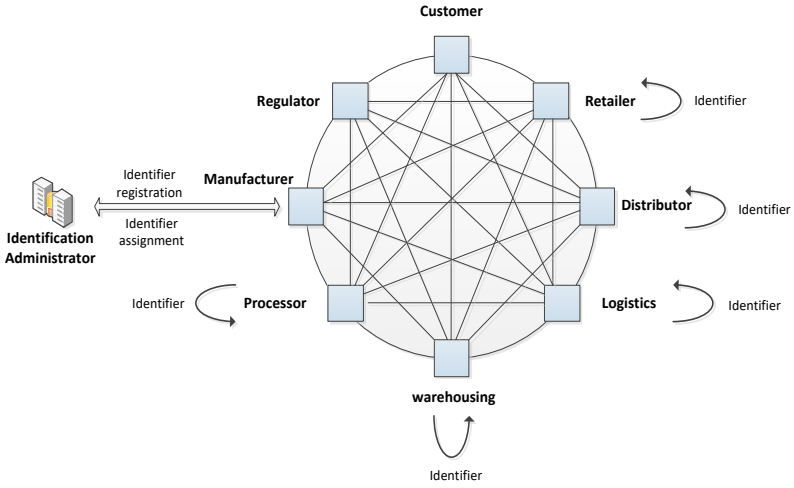


Figure I.1-1 The blockchain-based supply chain traceability

By taking full advantage of blockchain's un-erasable, immutable, and time-stamped characteristics, it would be would effectively realize the data traceable, keep trust relationship among different parties in supply chain application and service. However, there are several challenges by using blockchain on data information sharing and exchange for providing supply chain application and service.

- **The mechanism of setting data access control right is lacking.** In the supply chain system, it consists of manufacturer, distributor, retailer, and customer and so on. Different roles have different requirements and access control rights for the data. For the supply chain's data, it needs different multilevel confidential policy in the enterprise, and needs different access rights for different participants in the supply chain. For example, different government sectors, e.g. custom, quality supervision department, they have different requirements for the data governance in supply chain. Besides, the customer only concerns the quality and authenticity of the product by regarding the supply chain data. Thus, it's imperative to provide a mechanism that could protect the commercial privacy and personal privacy, and provide the access control right of data by blockchain-based data exchange and sharing.

- **The storage capacity and efficiency in public blockchain is insufficient.** Storing the data from different procedure of the supply chain in the public blockchain is reliable and visible, and it ensures the data trackable and immutable. However, this has some disadvantages for the enterprise, e.g. low efficiency, small data capacity, high cost. The data cannot be stored directly and quickly. Thus, the enterprise prefers to store the data which contains more detail in the private blockchain or information server, and only register the corresponding address of information server or the address of private blockchain to the public blockchain. How to

guarantee the data stored in the private blockchain is not tampered, and how to retrieve the data in private blockchain, becoming a vital problem.

- **Iintegrating blockchain in current supply chain systems in not quite easy**. The supply chains system is not easy to change and adapt. How to integrate the blockchain technology inside existing supply chain is very important.
- **It's difficult to guarantee the validity and legality of the traceability information.** Various participants need to reach consensus on the validity the product traceability information which is recorded and shared in the blockchain, and ensure the authenticity and legality of these traceability information in supply chain. It is important to provide an appropriate and effective algorithm to verify it.

I.1.2 Requirements of blockchain-based supply chain traceability

Blockchain could be used in the supply chain to exchange and share the dynamic and static information among the manufacture, processor, warehousing, logistics, distributor, retailer, customer, and regulator in different procedure of supply chain.

The Figure I.1-1 illustrates the supply chain traceability based on the blockchain.

Different partner and different enterprises in supply chain, need to access and obtain the information of the entire supply chain in real time. The requirements for blockchain-based supply chain traceability are as following:

- Currently most of the traceability data is stored in the public block chain, which is inefficient and slow in data storage. Especially for the case of huge historical data, the requirement of efficient data storage capacity is need to guarantee in blockchain-based supply chain system.
- By considering the efficiency of data storage and cost issues, some traceability data is stored in the private server or private blockchain, however, this is difficult to ensure whether the data has been tampered or not. So, it requires the traceability of data for guaranteeing the data has not been tampered.
- During the production, distribution and retail procedure of supply chain, it has a lot identifiers c corresponding one product. So, it needs to consider how to manage the identifiers in the blockchain-based supply chain traceability. It is necessary to consider different identifiers mapping relationship with each other. For example, a piece of labelled raw material is divided into different containers during processing and assigned new identifiers respectively. When more than one product is packaged into the same container. The nesting between these container identifiers and raw material identifiers or product identifiers should be considered.
- In the circulation, distribution, and retail procedure of supply chain, the manufacturers may reassign new identifier to the products, then the new identifier is generated corresponding the original product identifier. Therefore, it is necessary to record and maintain the mapping relation between the identifiers are used in all procedure of supply chain.

I.1.3 Framework of blockchain-based supply chain traceability

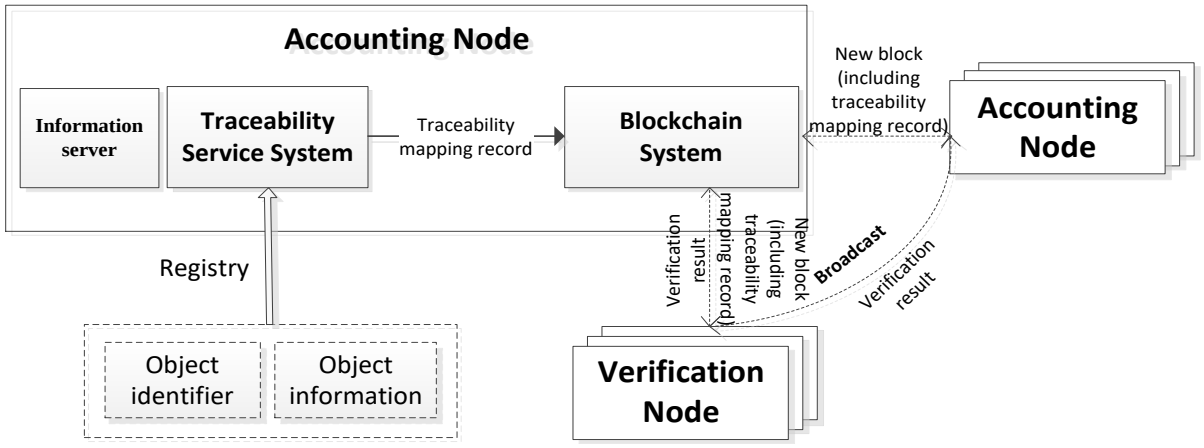


Figure I.1-2 Framework of supply chain traceability

Figure I.1-2 illustrates the architecture of supply chain traceability based on blockchain. The figure defines the participating nodes in the supply chain traceability, and the interaction mode between nodes, as well as the interaction information. The definitions of nodes and systems are as follows. Accounting node: One accounting node represents a participant in the supply chain, for example, a manufacturer, a retailer, a wholesaler, a distributor, or customs. The accounting node can broadcast the traceability mapping records to the blockchain and participate in synchronization of traceability mapping records.

- Verification node: The verification node is a regulator organization, for example, inspection and quarantine, food and drug supervision. It is responsible for verifying the new blocks that contain the traceability mapping record. It participates in the synchronization of traceability mapping records.
- Traceability service system: The traceability service system can be built in the accounting node and the verification node. It is responsible for recording the entire data of traceability event, and it provides the interface to assist blockchain system for the traceability data acquisition of the object identification query. In the case of authorization, it can supervise and audit the traceability data submission of certain real service identities.
- Blockchain system: The blockchain system can be built in the accounting node and the verification node, it is based on the underlying blockchain basic services. It is mainly responsible for consensus management, network communication, traceability mapping record storage, interface adaptation, etc. The traceability mapping records is stored by using blockchains structure.
- Information server: The information server is an enterprise private server, and responsible for object identifier and its associated traceable data storage, maintenance and management.

The key information transmitted in the system are as follows:

- Traceability mapping record: mainly includes the object identifier, the information server address identifier, the hash value of traceability data, the transfer-out blockchain account address, the transfer-in blockchain account address, timestamp and other information.
- Traceability data: mainly includes the data of the business link where the accounting node is located (e.g., commodity origin, date, environmental data, etc.), and the corresponding

relationship between the user's real business identity and the blockchain account address, and the business relationship between the users' real identities.

- Object identifier: The IoT identifier directly identifies the entity object, and the object identifier has a corresponding relationship with the entity object, for example, the IoT related commodity code.
- Object information: information related to the object identifier, for example, the origin of the object, date of manufacture, expiration date, production environment information, location, etc., it is the main information that constitutes traceability data.

I.1.4 Blockchain-based supply chain traceability interface

The interface between the traceability service system and the blockchain system is mainly used to implement data exchange between the traceability service system and the blockchain system. The traceability service system submits traceability mapping records to the blockchain system through this interface, and cooperates with the blockchain system to obtain traceability data of object identification query.

The interface uses HTTPS or HTTP protocol (based on TCP/IP) to submit data using POST and GET methods. Interface messages are transmitted in the JSON format via HTTPS or HTTP.

I.1.5 Technical solution of blockchain-based supply chain traceability

(1) Blockchain-based supply chain data sharing procedure

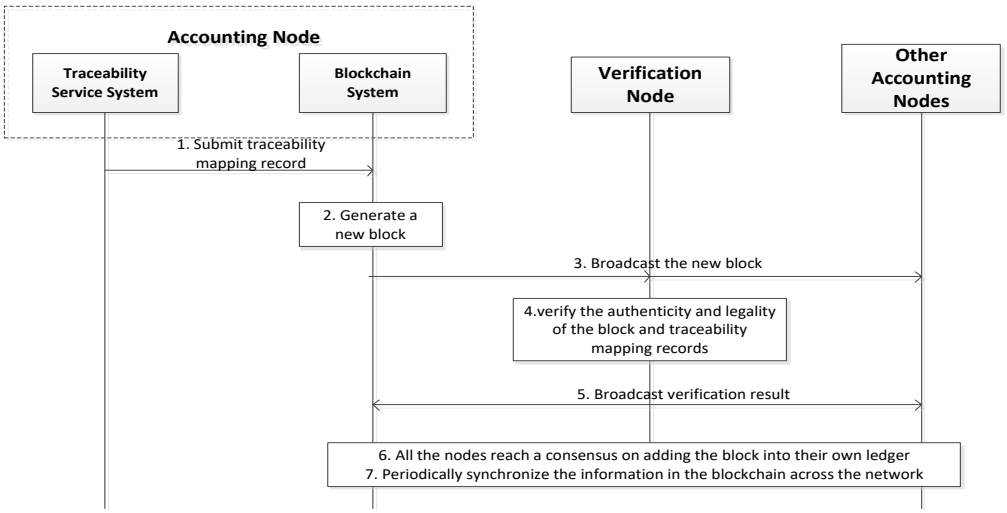


Figure I.1-3 Blockchain-based supply chain data sharing procedure

Figure I.1-3 shows the flow of announcing the data sharing transaction which is noted as "traceability mapping record" in this procedure. The steps are as follows:

- Step1: The traceability service system sends the traceability mapping record to the blockchain system, which mainly includes: the object identifier, the information server address identifier, the hash value of the traceability data, the transfer-out blockchain account address, the transfer-in blockchain account address, timestamp;
- NOTE: The transfer-out blockchain account address or the transfer-in blockchain account address may represent the downstream and upstream enterprise of supply chain.

- Step2: The blockchain system generates a new block. The new block includes: object identifier, information server address identifier, hash value of traceable data, transfer-out blockchain account address, transfer-in blockchain account address, timestamp, and digital signature. The composition of the block is shown in Figure I.1-4;
- Step3: The blockchain system broadcasts the new block to the entire network;
- Step4: After the verification node receives the information of new block, it verifies the authenticity and legality of the block and traceability mapping records according to the timestamp, digital signature, transfer-out blockchain account address, transfer-in blockchain account address, the number of commodities, and the location of commodity circulation, event time, and user identity. For example, based on verifying the correctness of the information according to the digital signature (whether the traceability record is broadcasted by the accounting node), and querying the object identifier and the information server address identifier in the traceability mapping record, the complete traceability data which is recorded in the corresponding information server could be queried.
- Step5: The verification node broadcasts the verification result to the entire network;
- Step6: Other accounting nodes monitor that a certain number of verification nodes broadcast the confirmation that they accept the traceability mapping record as a blockchain transaction in the block. It means that the block has obtained the consensus of most of the verification nodes, and then other accounting nodes add the block into their own ledger;
- Step7: Periodically synchronize the information in the blockchain across the network. For example, P2P technology is used to synchronize blockchain data from neighboring nodes.

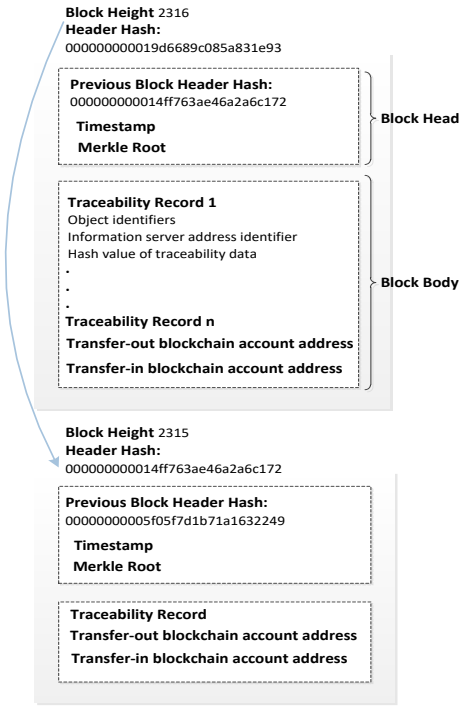


Figure I.1-4 Composition of the block in Blockchain-based supply chain

(2) Blockchain-based supply chain data query procedure

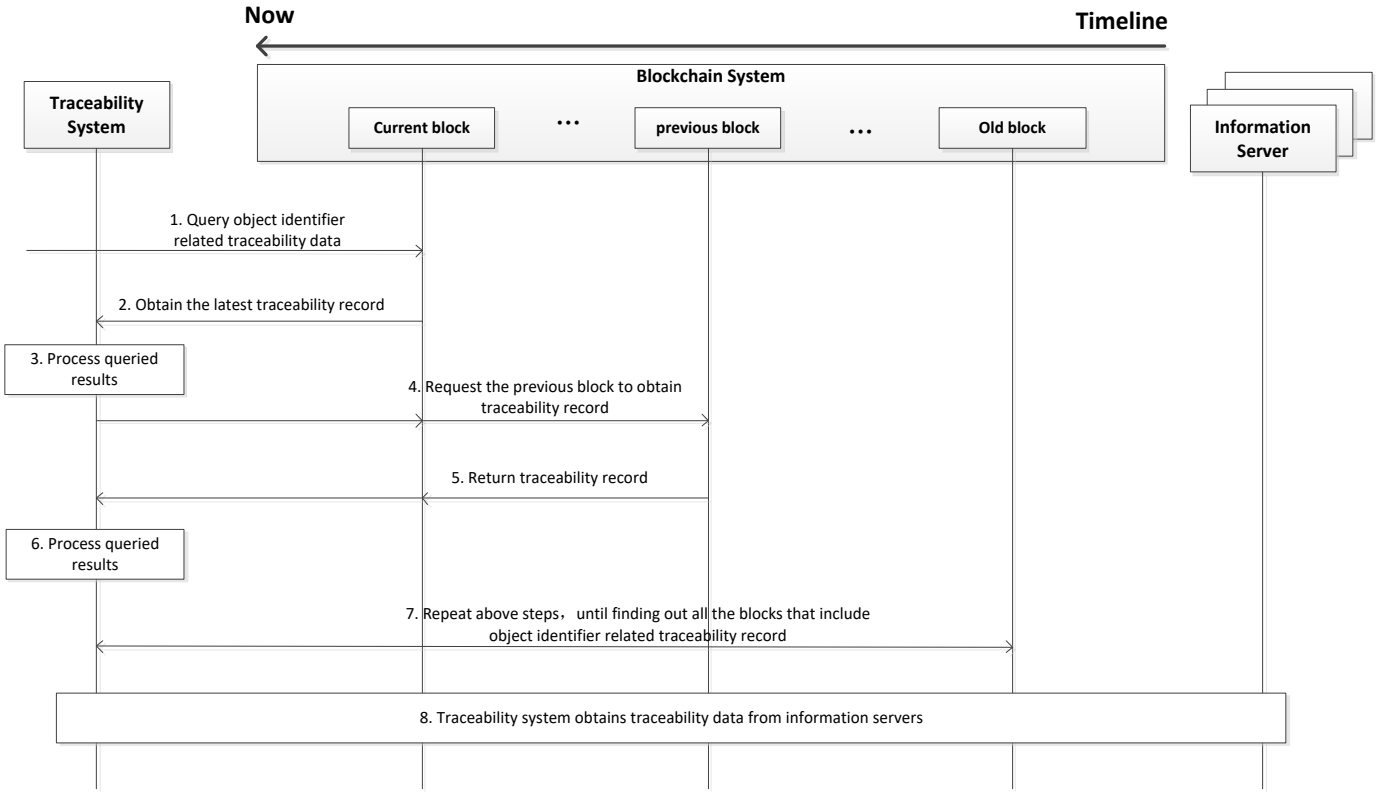


Figure I.1-5 Data Query procedure

Figure I.1-5 depicts the flow of querying traceability data based on object identifier. The steps are as follows:

- Step1: The blockchain system is received a query request for requesting traceability data based on object identifier;
- Step2: The blockchain system queries from the latest blocks in the blockchain system according to the timestamp, and obtains the current block that includes the latest traceability mapping record of the object identifier.
- Step3: According to the transfer-out blockchain account address, the traceability service system queries out the latest block (previous block) that includes the object identifier, and the transfer-in blockchain account address is the same as the transfer-out blockchain account address of current block;
- Step4: The traceability service system sends a request to the previous block to obtain the traceability mapping record that includes the information server address identifier, the hash value of traceability data, and the transfer-out blockchain account address;
- Step5: The block system returns the traceability mapping record;
- Step6: According to the transfer-out blockchain account address, the traceability service system queries out the next block that includes the object identifier and the blockchain account address of transfer-in is the same as the blockchain account address of transfer-out of current block;

- Step7: Repeating the above steps until finding out a block that includes the object identifier and no transfer-out blockchain account address. Therefore, all blocks include object identifier related traceability mapping record have been found out;
- Step8: Then original traceability data would be obtained in the traceability service system according to the set of information server address identifiers and hash values of traceability data found above. In addition, the traceability service system will verify the authenticity of the traceability data. For example, by verifying the hash value of the traceability data in each piece of information. The hash value is generated again according to the generation method of the hash value of the traceability data in the information, and comparing it with the hash value of the traceability data in the transmitted information. If these two are the same, the data in the traceability system is not tampered, on the contrary, it indicates that the data has been tampered with or is false.

I.2 Blockchain-based data sharing and data tracking during data asset circulation

Because the blockchain is decentralized, secure, tamper-proof and traceable, so it can help to build trust among participants and promote the sustainable growth of data exchange. With information on data ownership, exchange and verification scope recorded in the blockchain, the data ownership can be confirmed, and a clearly defined scope of verification can also regulate use of data. Each step from data collection to distribution is also recorded in the blockchain. Therefore, data is traceable, and the quality of the data can be enhanced by limiting data sources. Decentralized data exchange platforms based on the blockchain can promote global large-scale data exchange.

Based on Blockchain data Exchange& Sharing Authentication procedure is as following:

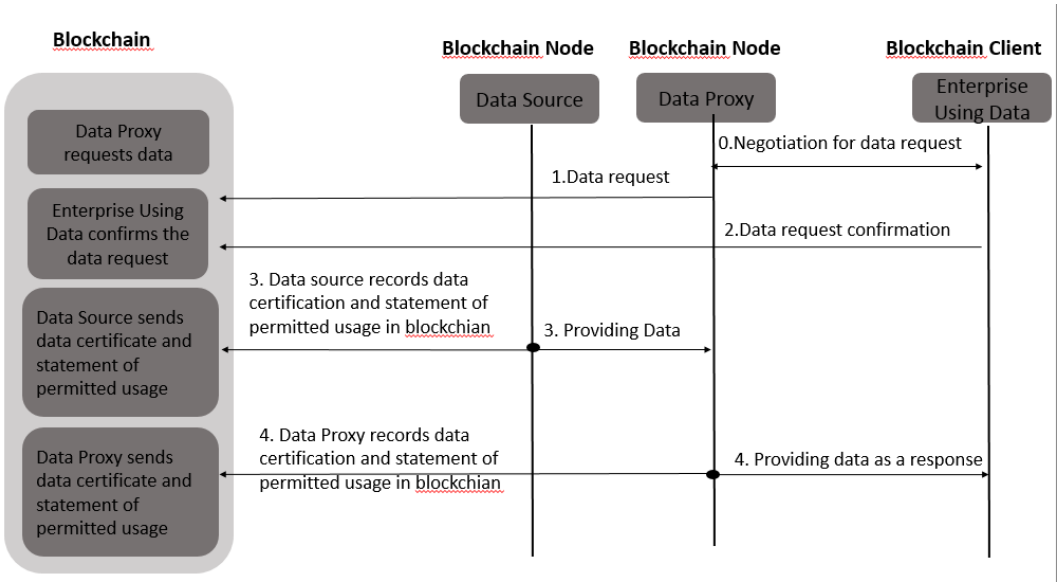


Figure I.2-1 Based on Blockchain data Exchange& Sharing Authentication

- Step0: Enterprise Using Data acts as the data requester, it makes negotiation with Data Proxy acts as the data intermediary for requesting data.

- Step1: Data Proxy requests data via blockchain in which Data Source and intermediary are both participant node in the blockchain.
- Step2: Enterprise Using Data send data request confirmation in the blockchain responding Data Proxy's data request.
- Step3: Data Source provides data to Data Proxy, as well as it records this data asset transaction certification and statement of permitted data usage in blockchain.
- Step4: Data Proxy provides data to Enterprise Using Data, as well as it records this data asset transaction certification and statement of permitted data usage in blockchain.

The figure above shows that all online data asset transactions are recorded in the blockchain. It cannot avoid data leakage specially during offline data asset trading. However, it could be mainly used to guarantee data provider's rights and responsibilities. The blockchain is a distributed ledge, and its transitions are the result of consensus among all the participants. If there is data leakage, it can be used for attesting whether the data leakage is caused by data provider's responsibility.

Especially in IoT domain where a wide range of IoT devices and sensors collect a large amount of data, serving as a medium for data exchange, blockchain-based decentralized data exchange and sharing networks can support the distribution of data and record real-time detailed data exchange. They can also build trust, maintain transparency, and support IoT participants in the data exchange ecosystem during the processes of data collection, storage, exchange, distribution, and data services. However, breakthroughs are still needed in scalability, exchange cost, and exchange speed in the decentralized data exchange networks to accelerate the commercialization of the IoT data market.

I.3 Blockchain-based data sharing for highly dependable IoT device sharing system

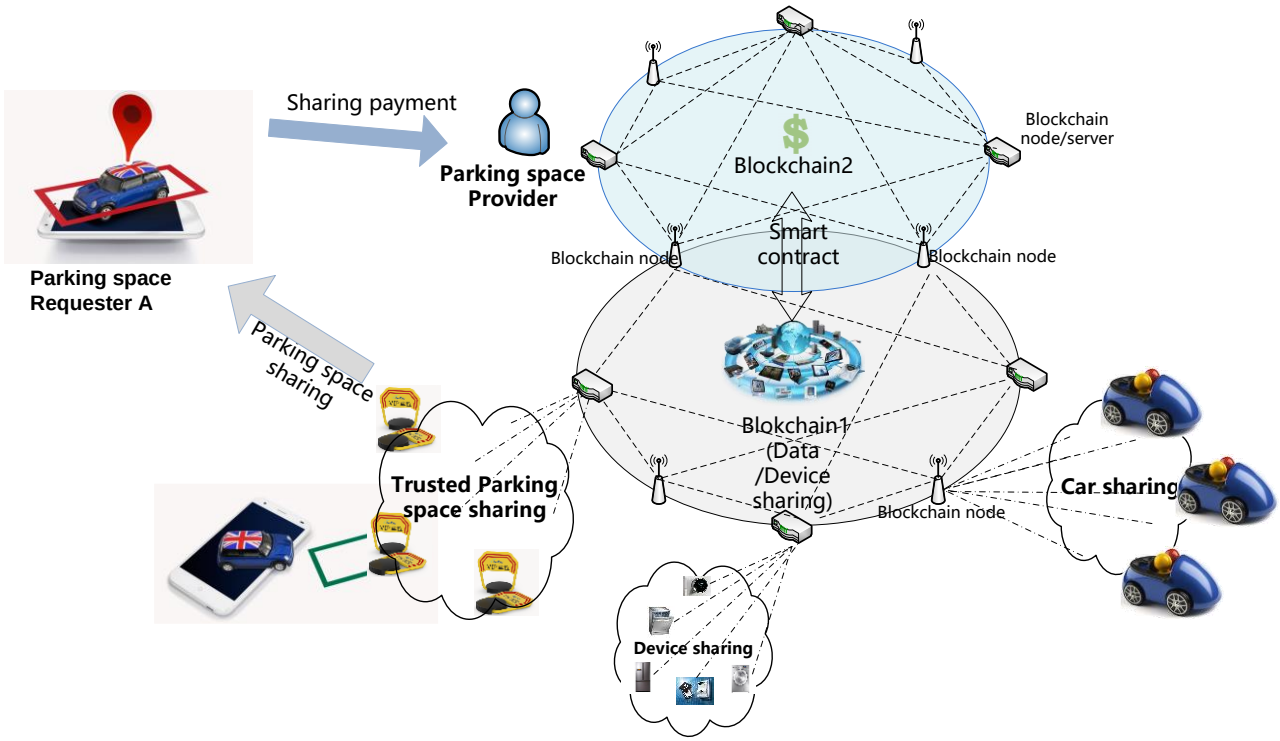


Figure I.3-1 Architecture for highly dependable IoT device sharing system

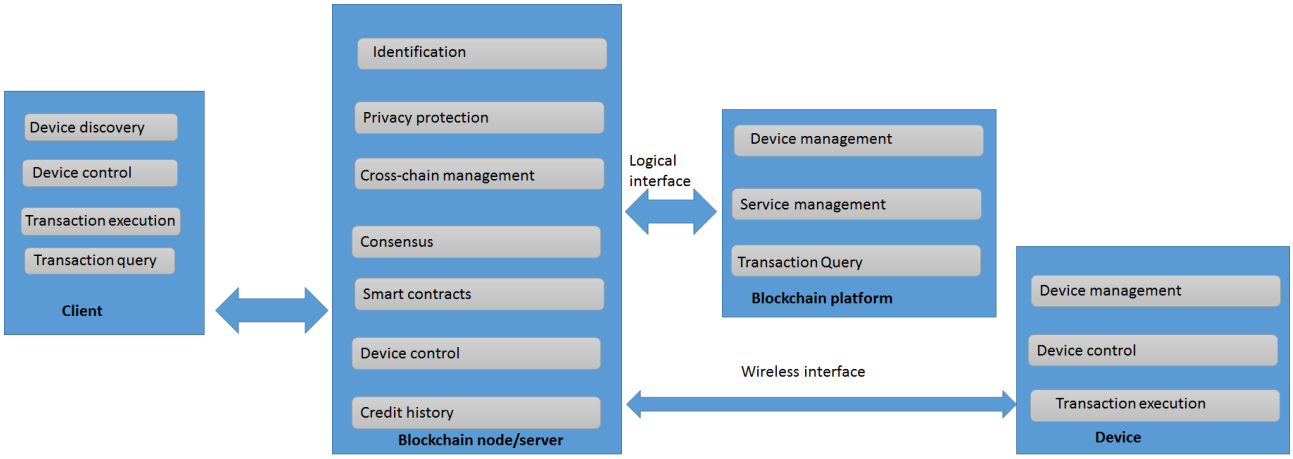


Figure I.3-2 Functional models for highly dependable IoT device sharing system

I.3.1 Client (requester)

The client needs to support the following functions:

- Device Discovery: The client is able to discover the surrounding smart locks that can be used, including:
  - Owner information of blockchain smart locks, as well as attribute information inherent to other devices
  - Location information such as blockchain smart locks and other variable attribute information
  - Service information provided by the blockchain smart lock, and service cost information
- Device Control: The client can control the opening or closing of the device smart lock and support the ability to reserve the blockchain smart lock in advance. (optional)
- Transaction execution: The client can initiate, complete or cancel a transaction with the smart lock
- Transaction Query: The client can query historical transaction information and so on.

I.3.2 Server

The blockchain server acts as a billing server for the blockchain network and acts as a proxy miner for smart locks for billing related transaction information. In the highly trusted IoT intelligent shared prototype, the blockchain server needs to support the following functions:

- Identification: The blockchain server identifies and manages users and smart locks accessing the blockchain network.
- Privacy protection: Blockchain servers provide security and privacy protection for transactions between clients and smart locks, as well as security and privacy protection for users and smart lock devices.
- Cross-blockchain management: Blockchain servers support mutual management between blockchains across two different attributes, such as cross-blockchain trading between cross-

transaction chains and payment chains, between payment chains and identity chains. Cross-blockchain management. Here, the blockchain server performs inter-chain management by executing certain smart contracts.

- Consensus: The blockchain server uses the consensus authentication mechanism. Here, the consensus authentication function, in particular, the blockchain server can perform the consensus authentication on the joining of the blockchain smart lock, the leaving process, and the consensus authentication of each transaction of the client and the smart lock. The blockchain server supports consensus authentication for multiple different blockchains, and different blockchains can use different consensus authentication mechanisms.
- Smart Contracts: Blockchain servers support cross-blockchain management or cross-blockchain transactions by executing relevant smart contracts.
- Device Control: The blockchain server can control the opening and closing of the blockchain smart lock by wireless transmission.
- Credit history: The blockchain server credits the client that completed the transaction. The blockchain server can grant a certain client credit score and the credit score granted in the blockchain for consensus authentication.

I.3.3. Blockchain platform

The blockchain platform refers to a blockchain operation platform composed of various blockchain servers, which is convenient for users to query related information on the platform through a visual interface. The following functions are supported in the blockchain platform:

- Device Management: The information of the blockchain smart lock is displayed in the blockchain platform, which allows the client to discover the surrounding smart lock information. Specifically includes:
  - Owner information of blockchain smart locks, as well as attribute information inherent to other devices
  - Location information such as blockchain smart locks and other variable attribute information
  - Service information provided by the blockchain smart lock, and service cost information
  - Blockchain smart lock real-time status information, i.e. idle, use, and lock (for specific users, such as the owner's own use) information display.
- Transaction Query: The blockchain platform can support the client to request historical transaction records from the blockchain platform in real time.
- Service Management: The blockchain platform supports multi-service coexistence. In the blockchain platform, the client can obtain information about blockchain smart locks that support different services. (convenient to expand later)

I.3.4 Device (e.g. Smart lock)

In the highly trusted IoT intelligent shared prototype, the smart lock needs to implement the following functions:

- Device Management: The smart lock initiates the device to join the blockchain to register the device to record the blockchain smart lock device information in the blockchain. Device information includes related locations, cost information, and more.
- Transaction execution: After receiving the relevant instruction sent by the blockchain server or the client, the smart lock determines that the smart lock and the client execute the transaction.
- Device Control: The smart lock receives the relevant instructions of the blockchain server through the wireless interface, or the relevant instructions of the client completes the opening and closing of the smart lock.
