International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4560

(08/2020)

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

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

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

Recommendation ITU-T Y.4560

ITU-T Y-SERIES RECOMMENDATIONS

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

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

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

Recommendation ITU-T Y.4560

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

Summary

Blockchain is an emerging technology, its most important characteristics are traceable, un-erasable, immutable, and time-stamped. It is able to efficiently ensure integrity, authenticity, and auditability for all transactions. Blockchain has important impacts and benefits for data exchange and sharing in support of Internet of things (IoT) and smart cities and communities (SC&C). In most of the IoT and SC&C scenarios, it is necessary to ensure data processing, circulation, sharing and management for all trust operations. Blockchain technologies can meet these needs.

Recommendation ITU-T Y.4560 specifies the requirements, functional models, a platform, and deployment modes of blockchain-based data exchange and sharing for supporting IoT and SC&C.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4560	2020-08-29	20	11.1002/1000/14379

Keywords

Blockchain, data exchange, data sharing, functional mode, Internet of things (IoT), smart cities and communities (SC&C).

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.4560

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

1 Scope

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

The scope of this Recommendation 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.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 blockchain data [b-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 [b-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 [b-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 [b-FG-DPM TR D3.5]: Agreements to confirm the correctness of the blockchain transaction.

3.1.6 data sharing [b-FG-DPM TS D0.1]: The process of data exchange among different parties with specified conditions.

3.1.7 data exchange [b-FG-DPM TS D0.1]: Accessing, transferring, and archiving of data.

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

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

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

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

3.1.10 smart contract [b-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 [b-ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DPM	Data Processing and Management
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of things
IP	Internet Protocol
JSON	JavaScript Object Notation
SC&C	Smart City and Communities
P2P	Peer-to-Peer
TCP	Transmission Control Protocol

5 Conventions

In this Recommendation:

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

6 Overview of blockchain in data exchange and sharing

6.1 Impacts of blockchain in data processing and management

The Internet of things (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 ledgers which contain all transactions executed within their networks, enforced with cryptography, and carried out collectively by peer-to-peer (P2P) workgroups. 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 number of impacts for data processing and management (DPM) to support IoT and smart city and communities (SC&C) application domains:

– Generally, IoT is used in P2P networks. The multi-centre and weak centre characteristics of blockchain are suitable for IoT networks. Additionally, blockchain can help the central structure reducing 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 for supporting device security, and to further 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 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 and protect privacy and identity rights management.

– Blockchain makes data auditable and traceable. 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 cannot allow detection and rejection by the other nodes in the network. In addition, using timestamps, 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. Trust and credit are the basis of all IoT transactions.

Blockchain technologies have the following specific characteristics: trustworthy, 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:

– Trusted transactions between the parties: Blockchain could be used to allow distrusted parties to realize trusted transactions, and finally to attain a trust relationship between the parties.

Whenever 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 becomes trusted: Consensus in blockchain would help to identify illegal nodes and prevent malicious access. Blockchain helps to guarantee that data's terminal device is trusted.

– Data becomes trusted and verifiable: Data becomes trusted and verifiable and can be traced back to the origin based on blockchain.

– Trusted data storage: Blockchain itself is an untampered database storage technology. The data can be recorded directly on blockchain or can be encrypted 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. In addition, based on cryptographic protocols, the blockchain is able to effectively protect the 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 and reasonable in a blockchain network; in addition, the private-key encryption and 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 that it is un-tampered and traceable. Therefore, in multi-parties' cooperation scenarios, they need to rely on a trusted third party to share trusted data information which impacts on the cooperation between parties. However, at times there is no trusted third party, or the costs 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 would help to optimize procedures, improve efficiency and reduce costs, etc.

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

– Blockchain can be used in data exchange and sharing for achieving data asset transaction as well as for safeguarding related rights and interests of data owners.

– Blockchain can be used for sharing trusted information in a multilateral collaboration scenario. It is helpful to optimize procedures, improve efficiency or reduce costs especially 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 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 management process.

– It is required to maintain the identification of participating parties throughout the data 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 the support of trusted data transmission and circulation.

– It is required to keep tamper detection of data.

– It is recommended to use data encryption, digital signatures, and data fingerprints 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 blockchains.

NOTE – It is necessary to address the following attributes of the system, including but not limited to, data structure, data element format, data type, identifier, and data length, etc.

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 platforms.

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 by ensuring that either all executions of data sharing operations during cross-blockchain are successful or that they all 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 secure.

– It is required to enhance the secure control of cross-blockchain operations (e.g., keeping cross-blockchain operations confidential and traceable).

8 Functional model of blockchain-based data exchange and sharing

The functional models of blockchain based data exchange and sharing include a security and privacy function, a trusted data collection function, a distributed data processing function and a data sharing and trading function. Figure 8-1 shows a functional model of blockchain-based data exchange and sharing.

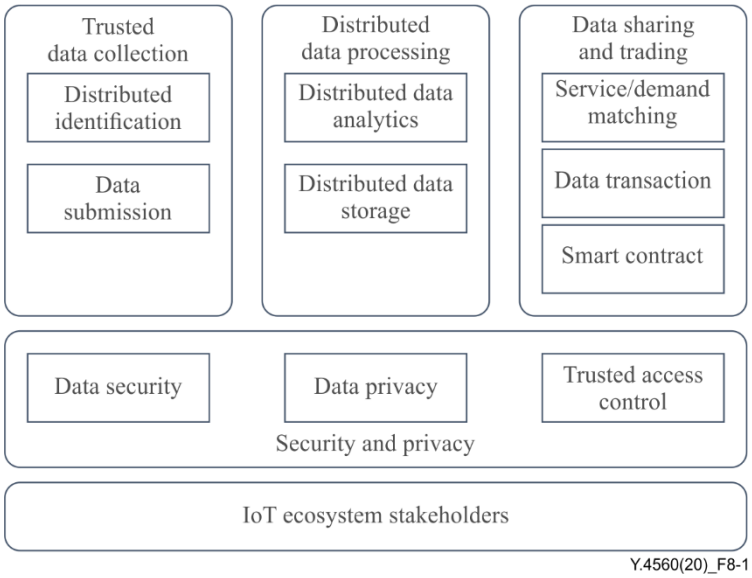


Figure 8-1 – A functional model of blockchain-based data exchange and sharing

8.1 Trusted data collection function

A trusted data collection function provides data from the data source. It includes distributed identification and data submission functions.

– **Distributed identification function**: It provides a 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 a blockchain-based integrated, auditable, and traceable data collection mechanism for IoT devices.

8.2 Distributed data processing function

A distributed data processing function 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

A data sharing and trading function 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 effectively ensures integrity, authenticity, auditability, and consistency of all transactions.

– **Smart contract function**: It enables the exchange of data sharing and trading with rules defined in a code form and 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

A security and privacy protection function 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 and a digital signature to ensure data security.

– **Data privacy function**: It minimizes data exposure according to data rights (the right of ownership, use, and/or profits).

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

9 Blockchain-based data exchange and sharing platform

Figure 9-1 shows a reference platform for blockchain-based data exchange and sharing.

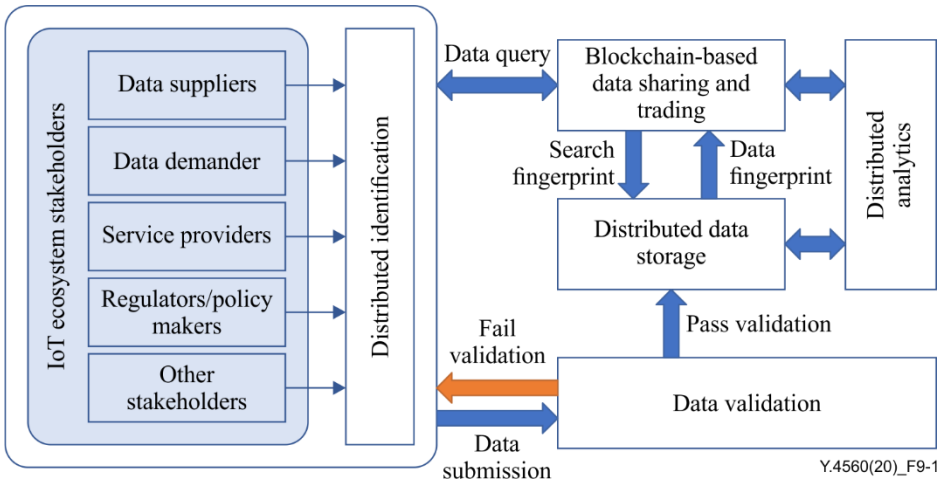


Figure 9-1 – Blockchain-based data exchange and sharing platform

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 other stakeholders.

– **Data suppliers**: Data suppliers send/sell data to data demanders. They either own various IoT devices and are 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 platforms.

– **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 agencies, insurance companies, 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 include approval of the identifier and change of status associated with the identifier.

9.3 Data submission

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

9.4 Data validation

Data validation 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 passes the validation it would be encrypted and sent to distributed data storage. If the data does not 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 a mismatch in the blockchain.

9.6 Distributed analytics

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

9.7 Blockchain-based data sharing and trading

Blockchain-based data exchange and sharing as shown in Figure 9-2 comprises:

– **Trusted supply/demand matching**: It finds matching pairs for data suppliers and data buyers. 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 the blockchain, and then data is retrieved via the distributed storage relating to the data's "fingerprint". Based on this, a data sharing transaction is initialled and the data sharing transaction in the 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 a contract. Once the conditions of the smart contract are met, the smart contract is performed automatedly for data sharing or data trading in blockchain. Especially 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.

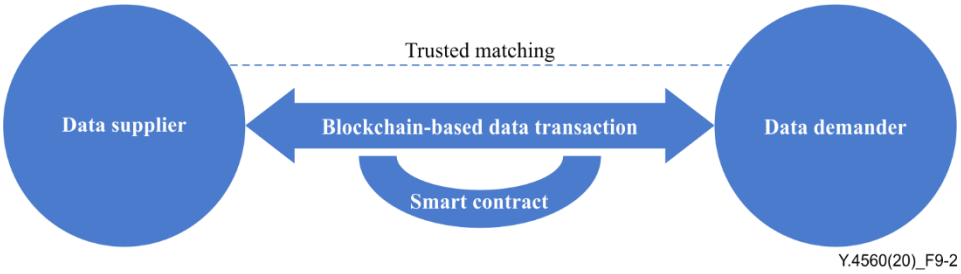


Figure 9-2 – Data sharing interaction between data supplier and data demander

10 Deployment modes for blockchain-based data exchange and sharing

10.1 General deployment modes

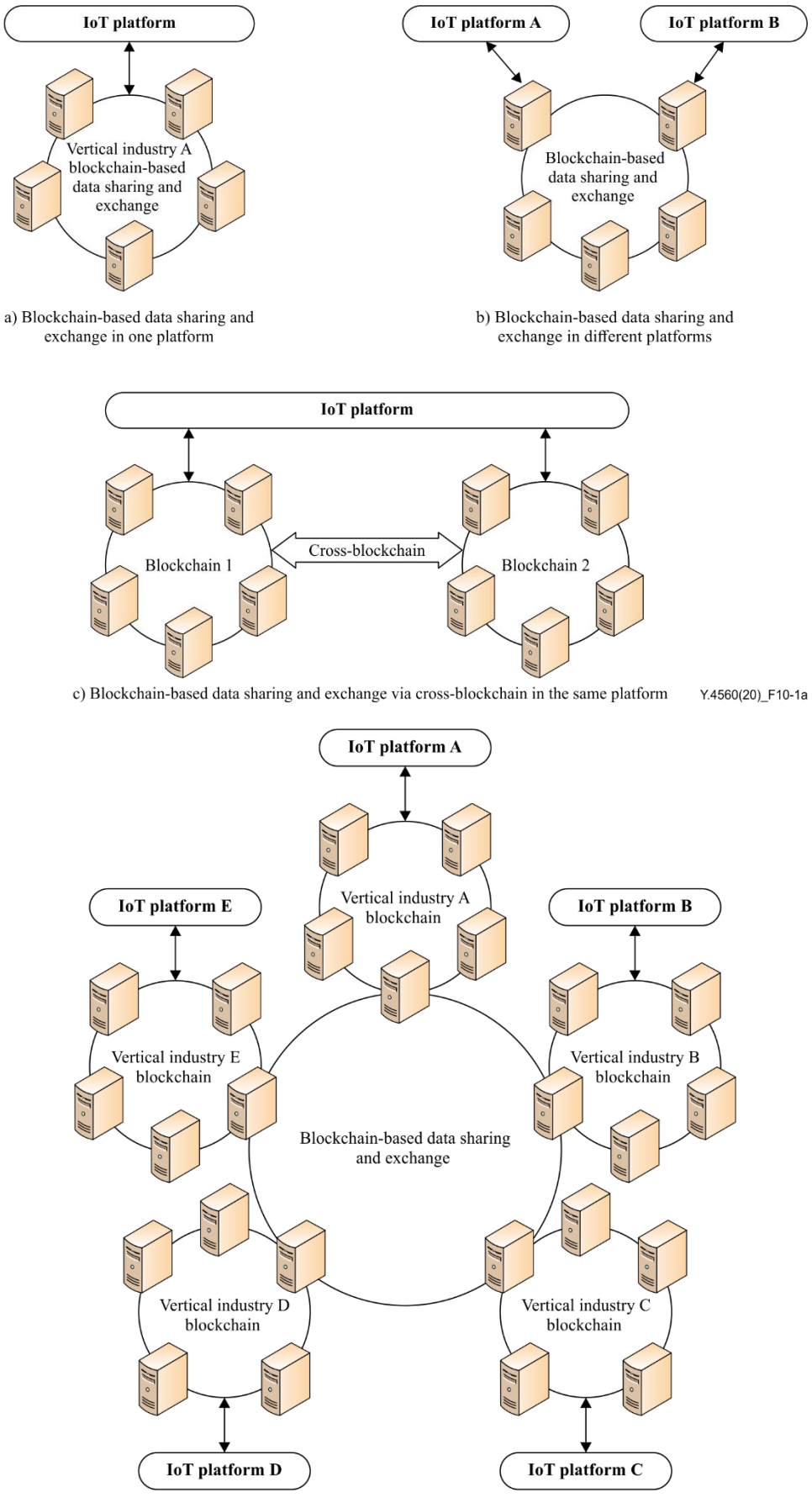
The potential deployment modes of blockchain-based data exchange and sharing, as shown in Figure 10-1, are as follows:

– **One blockchain in one platform**: One blockchain connects an 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 one 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 a cross-blockchain. Different blockchains may respectively have different kinds of data.

– **Cross-blockchain in different platforms**: Different blockchains connect to different IoT platforms. Data exchange and sharing among different platforms is realized via different cross-blockchains.



a) Blockchain-based data sharing and exchange in one platform

b) Blockchain-based data sharing and exchange in different platforms

c) Blockchain-based data sharing and exchange via cross-blockchain in the same platform

Y.4560(20)_F10-1a

d) Blockchain-based data sharing and exchange via cross-blockchain in the different platform

Y.4560(20)_F10-1b

Figure 10-1 – General deployment modes of blockchain-based data exchange and sharing

10.2 Cross-blockchain deployment modes

Figure 10-2 shows blockchain-based data exchange and sharing via cross-blockchains in the same platform or in different platforms. Relating to cross-blockchains, the cross-blockchain deployment modes are shown as follows:

– Deployment mode 1: The nodes in Blockchain 1 are independent of the ones in Blockchain 2. The two different blockchains exchange data via smart contract.

– Deployment mode 2: Blockchain 1 connects with Blockchain 2 via one trusted node.

– Deployment mode 3: Several nodes of Blockchain 1 are the nodes of Blockchain 2.

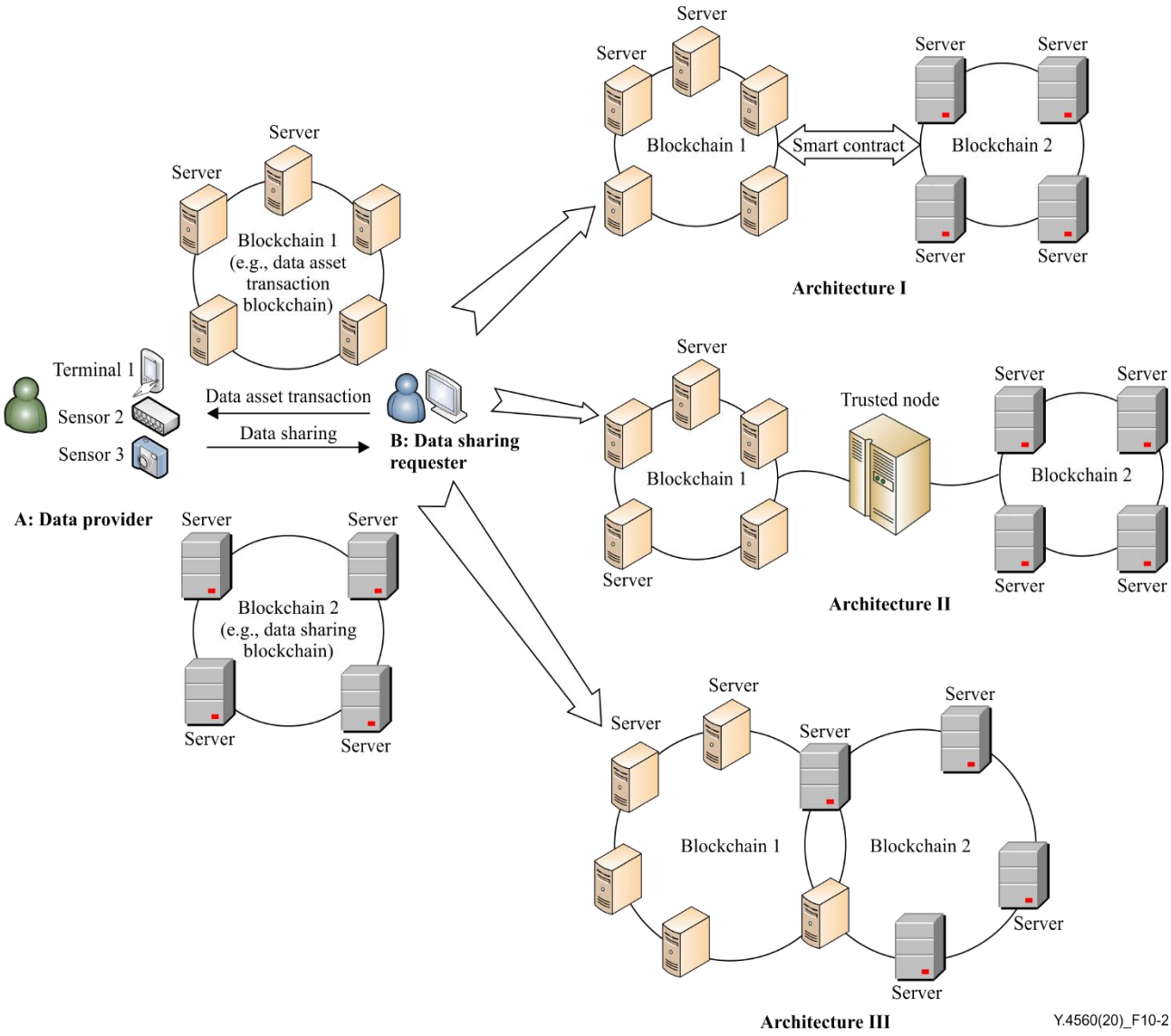


Figure 10-2 – Deployment modes of cross-blockchain for blockchain-based data exchange and sharing

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 illustrates supply chain traceability based on the blockchain. By taking full advantage of blockchain's un-erasable, immutable, and time-stamped characteristics, data is effectively traceable and thus could help to maintain trust relationships among different parties in supply chain applications and services. However, there are several challenges to blockchain-based supply chain traceability when using blockchain in data information sharing and exchange for providing supply chain applications and services:

– **A mechanism for setting data access control rights is lacking**. In a supply chain system that consists of manufacturer, distributor, retailer, and customer etc., different roles have different requirements and different access control rights for the data. For the supply chain's data, it needs different multilevel confidential policies in the enterprise, and needs different access rights for different participants in the supply chain. For example, different government sectors, such as customs and the quality supervision department, have different requirements for data governance in a supply chain. The customer however is only concerned with the quality and authenticity of the product regarding the supply chain data. Thus, it is imperative to provide a mechanism that could protect commercial privacy and personal privacy and provide the access control rights of data by blockchain-based data exchange and sharing.

– **The storage capacity and efficiency in public blockchains is insufficient**. Storing data from different procedures of a supply chain in a public blockchain offers reliability and visibility and ensures that the data is traceable and immutable. However, this has some disadvantages for the enterprise, such as low efficiency, small data capacity and high costs. The data cannot be stored directly and quickly. Thus, enterprises prefer to store more detailed data in a private blockchain or information server, and only register the corresponding address of the information server or the address of the private blockchain to the public blockchain. How then to guarantee that the data stored in the private blockchain is not tampered with, and how to retrieve the data in a private blockchain, becomes a significant problem.

– **Integrating blockchain in current supply chain systems is not easy**. The supply chains system is not easy to change and adapt. The question of how to integrate the blockchain technology inside existing supply chain systems is very important.

– **It is difficult to guarantee the validity and legality of the traceability information**. Various participants need to reach consensus on the validity of the product traceability information that is recorded and shared in the blockchain and ensure the authenticity and legality of this traceability information in the supply chain. It is important to provide an appropriate and effective algorithm to verify the traceability information.

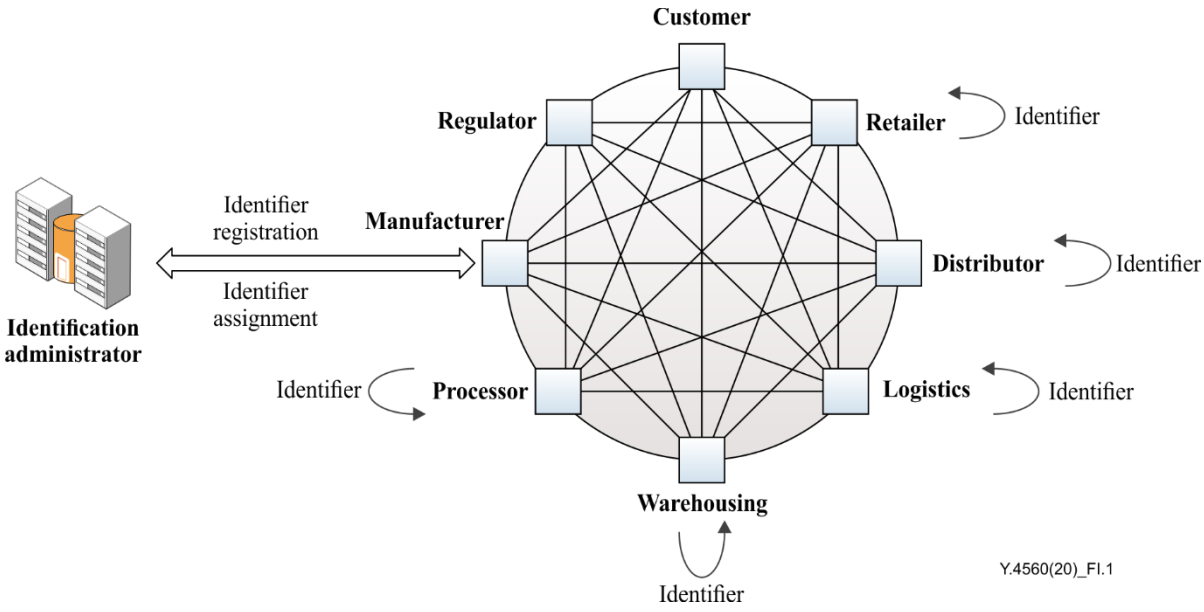


Figure I.1 – Blockchain-based supply chain traceability

I.1.2 Characteristics of blockchain-based supply chain traceability

Blockchain could be used in the supply chain to exchange and share dynamic and static information among manufacturers, processors, warehousing operators, logistics, distributors, retailers, customers and regulators in different procedures of the supply chain.

Various partners and various enterprises in a supply chain, can access and obtain the information of the entire supply chain in real time. The characteristics for blockchain-based supply chain traceability are as follows:

– Most of the traceability data is stored in the public blockchain, which is inefficient and slow in data storage. This is especially the case for large scale historical data. The efficient data storage capacity can be guaranteed in a blockchain-based supply chain system.

– Considering the efficiency of data storage and cost issues, some traceability data is stored in the private servers or in a private blockchain, however, in this case it is difficult to ensure that the data has not be been tampered with. Usually, traceability of data is used to guarantee that the data has not been tampered with.

– During the production, distribution and retail procedures of a supply chain, there may be several identifiers corresponding to a single product. Usually, there is a need to consider how to manage the identifiers in blockchain-based supply chain traceability. It is necessary to consider the various 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 will be considered.

– In the circulation, distribution, and retail procedures of a supply chain, manufacturers may reassign new identifiers to products, then a new identifier is used to generate the corresponding e original product identifier. Usually, it is necessary to record and maintain the mapping relationship between the identifiers that are used in all procedures of the supply chain.

I.1.3 Framework of blockchain-based supply chain traceability

Figure I.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: An 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 note is a regulator organization, for example, inspection and quarantine or food and drug supervision. The verification node 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 the blockchain system for the traceability data acquisition of the object identification query. In the case of authorization, the traceability service system 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 are stored by using a blockchains structure.

– Information server: The information server is an enterprise private server and is responsible for object identifiers and their associated traceable data storage, maintenance and management.

The key information elements transmitted in the system are as follows:

– Traceability mapping record: This 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: This 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.

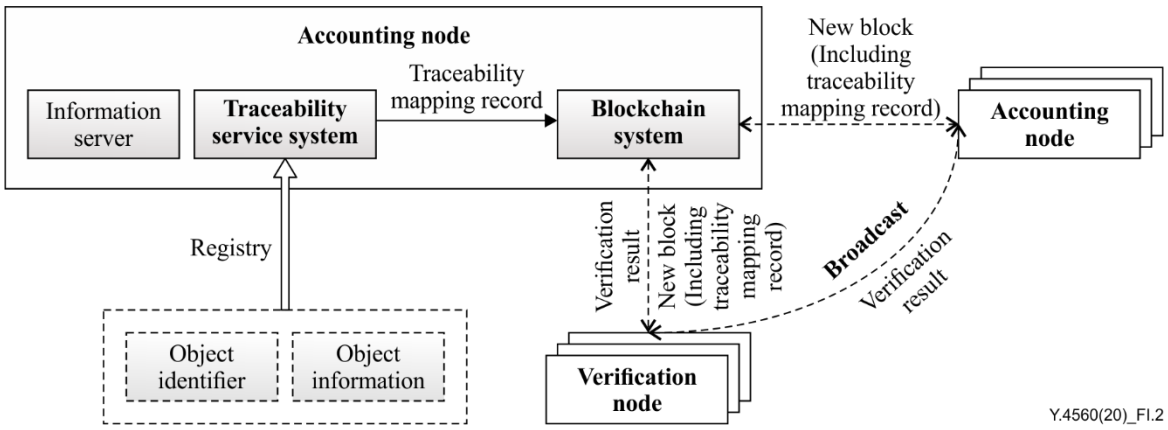


Figure I.2 – Framework of supply chain traceability

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 the object identification query.

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

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

(1) Blockchain-based supply chain data sharing procedure

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

Step 1: 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 enterprises of supply chain.

Step 2: 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.4.

Step 3: The blockchain system broadcasts the new block to the entire network.

Step 4: 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.

Step 5: The verification node broadcasts the verification result to the entire network.

Step 6: Other accounting nodes monitor that a certain number of verification nodes broadcast the confirmation and that they accept the traceability mapping record as a blockchain transaction in the block. This 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.

Step 7: Periodically synchronize the information in the blockchain across the network. For example, P2P technology is used to synchronize blockchain data from neighbouring nodes.

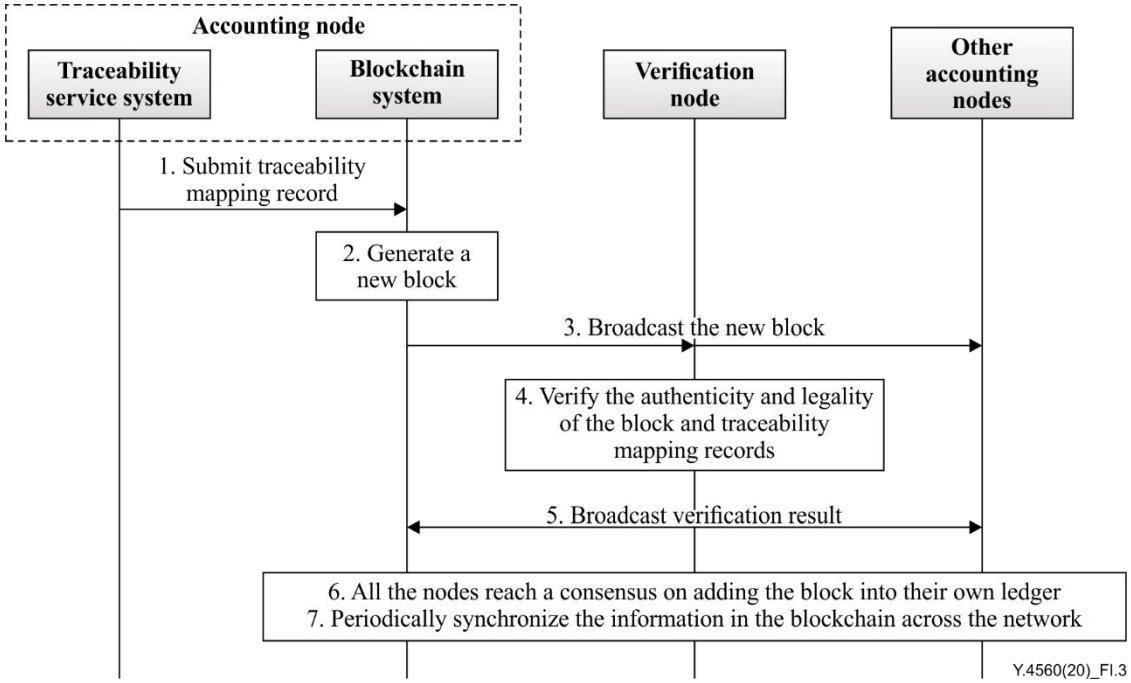


Figure I.3 – Blockchain-based supply chain data sharing procedure

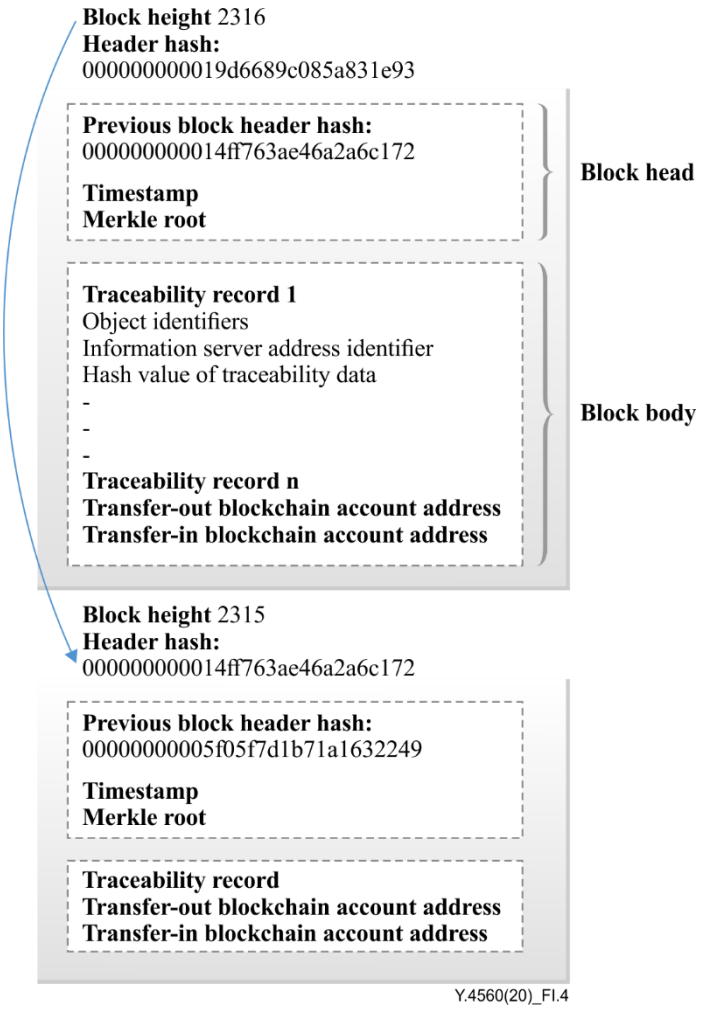


Figure I.4 – Composition of the block in blockchain-based supply chain

(2) Blockchain-based supply chain data query procedure

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

Step 1: The blockchain system receives a query request for requesting traceability data based on an object identifier.

Step 2: 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.

Step 3: 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.

Step 4: 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;

Step 5: The block system returns the traceability mapping record.

Step 6: According to the transfer-out blockchain account address, the traceability service system queries out the next block that includes the object identifier and that the blockchain account address of transfer-in is the same as the blockchain account address of transfer-out of current block.

Step 7: The above steps are repeated until a block is found that includes the object identifier and no transfer-out blockchain account address. Therefore, all blocks include object identifier related traceability mapping records that have been found out.

Step 8: 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, if on the contrary they are different, it indicates that the data has been tampered with or is false.

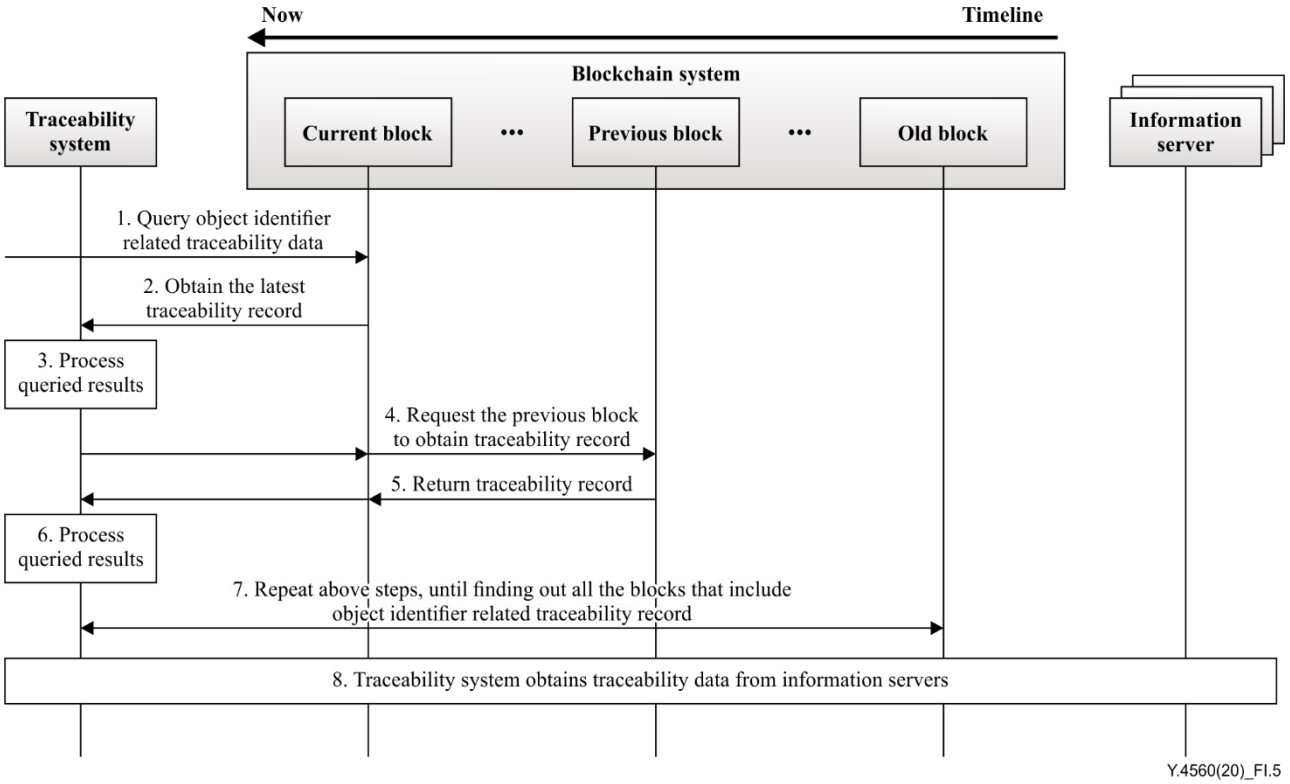


Figure I.5 – Traceability data query procedure

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

As the blockchain is decentralized, secure, tamper-proof, and traceable, it can be used to help 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.

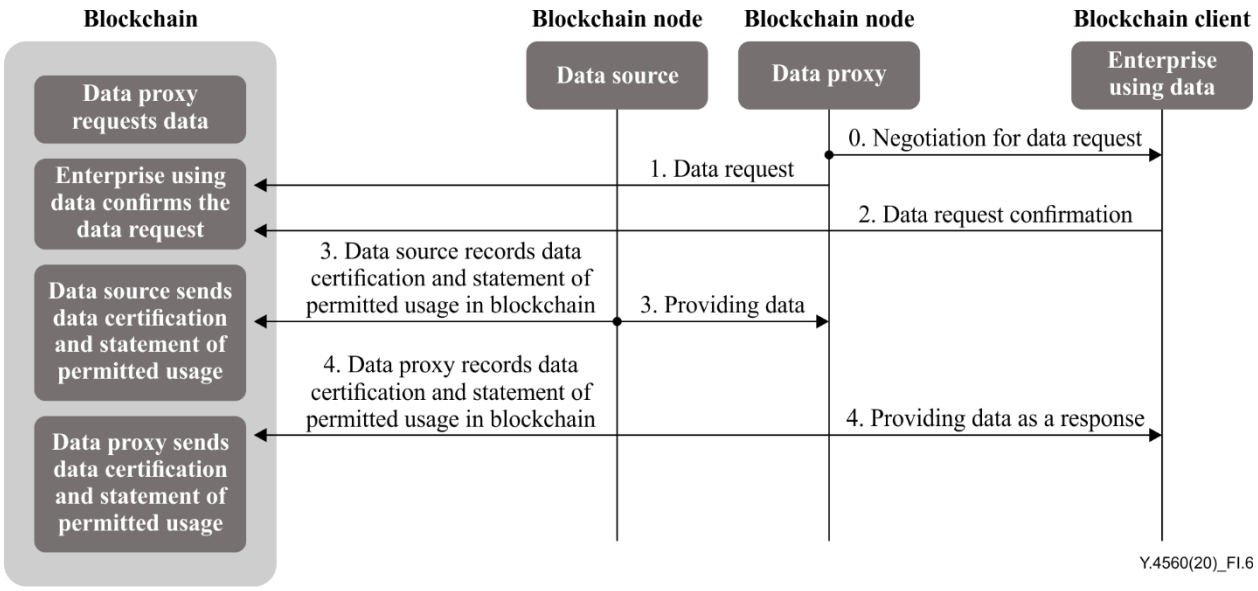


Figure I.6 – Authentication based on blockchain data exchange and sharing

The authentication procedure, shown in Figure I.6, based on blockchain data exchange, and sharing, is as follows:

Step 0: The enterprise using data acts as the data requester, it negotiates with the data proxy and acts as the data intermediary for requesting data.

Step 1: The data proxy requests data via blockchain in which data source and intermediary are both participant nodes in the blockchain.

Step 2: Enterprise using data send data request confirmation in the blockchain responding data proxy's data request.

Step 3: Data source provides data to data proxy and records this data asset transaction certification and statement of permitted data usage in blockchain.

Step 4: Data proxy provides data to enterprise using data and records this data asset transaction certification and statement of permitted data usage in blockchain.

Figure I.6 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 the data provider's rights and responsibilities. The blockchain is a distributed ledger, 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 the 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 costs, and exchange speed in the decentralized data exchange networks to accelerate the commercialization of the IoT data market.

Bibliography

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

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

[b-FG-DPM TS D0.1] Technical Specification D0.1 (2019), *Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary.*

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

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2020