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 D3.8

Identity framework in blockchain to support DPM for 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 D3.8

Identity framework in blockchain to support DPM for IoT and SC&C

Summary

The Technical Specification specifies an identity framework in blockchains to support data processing and management (DPM) for IoT and SC&C.

This specification provides support for designing, developing, integrating an identity framework in blockchain to support aspects of data processing and management for IoT and SC&C.

The relevant requirements and technologies that support the identity framework in blockchain are defined in this Technical Specification.

Acknowledgements

This Technical Specification was researched and principally authored by Ning Hu (Onchain) under the chairmanship 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 interoperability; data sharing; identity framework.

Technical Specification D3.8

Identity framework in blockchain to support DPM for IoT and SC&C

Table of Contents

Technical Specification D3.8

Identity framework in blockchain to support DPM for IoT and SC&C

1 Scope

The Technical Specification specifies an identity framework in blockchains to support data processing and management (DPM) for IoT and SC&C.

The scope of this Technical Specification covers several key requirements with respect to an identity framework in blockchain to support DPM for IoT systems and functional features to fulfil these requirements.

The scope of this Technical Specification covers the following:

- Overview of identity framework in blockchain to support DPM;
- Requirements for developing identity framework in blockchain to suppor DPM;
- Functional model of identity framework in blockchain to support DPM;
- Details on identifier model functions;
- Details on ID based DPM runtime and trust audit for IoT system;
- Details on ID based runtime and trust audit for data interoperability cross IoT systems.

NOTE – For data exchange example through blockchain system, see Appendix I.

2 References

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

[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.4050] Recommendation ITU-T Y.4050/Y.2069 (2012), *Terms and definitions for Internet of Things*

3 Definitions

3.1 Terms defined elsewhere

These Technical Specifications use the following terms defined elsewhere:

3.1.1 AAA [ITU-T Y.2703]: The authentication, authorization and accounting service provides the functions by which a user's identity is verified (authentication), is given access to the services (authorization) and a means by which consumption of resources is measured (accounting).

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

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

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

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

3.2.4 identifier [ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.5 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.

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

3.1.7 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

These Technical Specifications defines the following terms:

3.2.1 BCID: Blockchain identity (BCID) framework is a term of identity framework in blockchain.

3.2.2 token: In computing industry, “token” means an object (in software or in hardware) which represents the right to perform some operation; in blockchain, esp., public chain, “token” is used as a form of cryptocurrency to perform decentralized finance business. In object-oriented programming,

one object can be implemented from both token (computing) and token (blockchain) interfaces. A token can be transferred from one to another as a blockchain token and be used as a computing token.

3.2.3 data-token: Data-token (computing) is a term of a sequence of bytes inside blockchain, with cryptographic protection, which is always present in every on-chain event and taken together with the ownership and accessibility (or other privileges if any) of on-chain data identifier, whereas on-chain data identifier is linked with off-chain data instance, these bytes represent a unique data token identifier called a data-token.

3.2.4 utility-token: Utility-token (blockchain) is a term usually used in public chain, which is a tool for value assessment, and digital asset reconciliation for exchanges. Furthermore, in blockchain systems which are providing financial services, utility tokens are used as a form of payment for close loop exchange settlement.

3.2.5 fungible: In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part [b-1]. In cryptocurrency, cryptocurrencies are usually considered to be fungible assets, where one coin is equivalent to another. In the use of data token identifier (data-token), adopt the economic term fungible to describe certain types of data token that can be broken down into interchangeable pieces that are not interdependent on the other pieces, fungible data-token is interchangeable.

3.2.6 non-fungible: In cryptocurrency, a non-fungible token (NFT) is a special type of cryptographic token which represents something unique; non-fungible tokens are thus not interchangeable [b-2]. In the use of data token identifier (data-token), use non-fungible data-token to describe certain types of data token that are unique and not interchangeable.

3.2.7 partially-fungible: In the use of data-token, use partially-fungible data-token to describe certain types of data token are created with interchangeable but can be updated to unique and interchangeable during data processing.

4 Abbreviations and acronyms

These Technical Specifications use the following abbreviations and acronyms:

AAA Authentication, Authorization, and Accounting

BCID Blockchain Identity

DID Decentralized Identifier [b-6]

DLT Distributed Ledger Technology

EID Entity ID

ID Identifier

IoT Internet of Things

5 Conventions

In this technical specification:

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

6 Overview of identity framework in blockchain to support DPM

6.1 Concepts of identity framework in blockchain for DPM

Blockchain enables trusted data transmission and circulation. It can help to guarantee the data security, data privacy, and data access control. Blockchain enables trusted digital asset transferring:

- The blockchain enables 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
- Blockchain can 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.

Identity framework in blockchain provides the capability of trust audit for the following,

- the ownership and accessibility of entities in IoT and SC&C systems;
- full traceable transactions of data processing.

A view of identity framework in blockchain to support DPM is described as below,

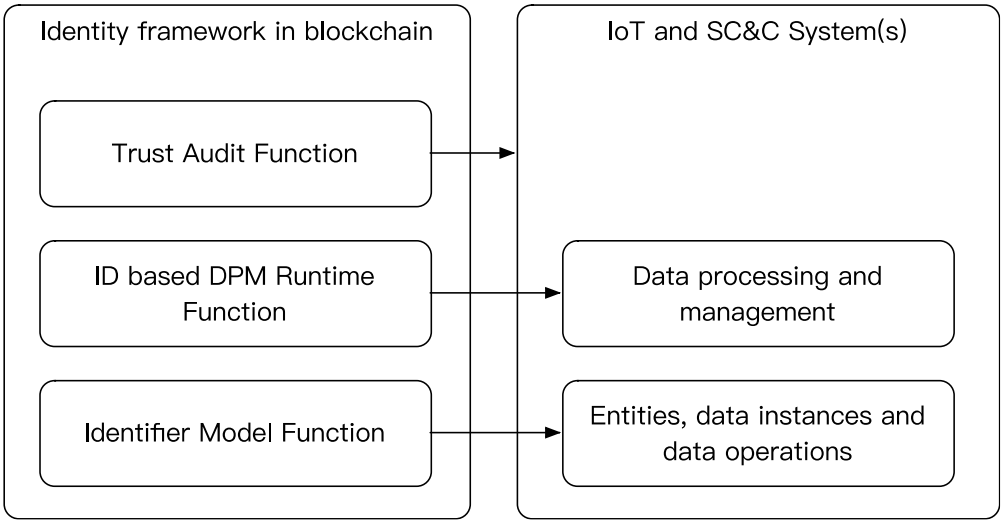

Figure 6-1 A view of identity framework in blockchain to support DPM

In IoT system, a combination of IoT and blockchain identity system is able to support identities of “persons (users)”, “data instances”, “transactions” and “smart devices”.

There are three types of functions in the identity framework in blockchain which work with IoT and SC&C systems, namely, identifier model functions, data processing and management runtime functions and trust audit functions. The details on these functions are elaborated in section 7.

6.2 Dimensions of identity framework in blockchain

- Static identifier model and mapping

IoT system generate data by users, smart devices or platforms, the static identifier model and mapping provides the capability to map entities, data instances and data operations in IoT systems to blockchain.

- Dynamic runtime of identifier generation and updating

The data processing and management in IoT system has got runtime services, the DPM runtime in blockchain provides the capability to trace data processing and control the accessibility for entities accessing data instances.

- Trust functions for audit

Blockchain provides trust endorsement for transactions cross systems, the ledger in blockchain provides audit of the ownership and accessibility of data instances, and the lifecycle of data processing and management.

7 Requirements for developing identity framework in blockchain to support DPM

The blockchain system is to resolve the problem of competitive synergy and construct a credible business execution environment. The close-loop of data generation and processing in IoT system is a "trustworthy" source of blockchain system. Therefore, the combination of IoT system and blockchain system constructs a reliable solution to enable data self-sovereign and traceability of data processing and management.

To support data self-sovereign and traceability of data processing and management in IoT and SC&C, many aspects are required to be considered.

7.1 Requirements of identifier model to support DPM in IoT and SC&C

To ensure the appropriate level of the identifier model in IoT and SC&C following aspects are required:

- Capability of cross IoT and SC&C systems. It is required to support self-sovereign identifier in different systems, regions or organizations;
- Capability to support self-sovereign data management. It is required to provide data management on different type of data owners, e.g., smart devices, end users and/or systems;
- Capability to support traceability of actions on data processing and transferring. It is required to provide the capability of traceability on data processing and transferring;

Due to the capability limitation of "things" in IoT systems, the embedded sub-system of smart devices is tightly coupled with IoT system internally, cannot be integrated with external systems easily. There're multiple ID standards in different IoT solutions, e.g., OID[b-3], Handle[b-4], EPC[b-5].

The identifier model shall be able to integrate with multiple ID resources from existing IT systems. The identifier model shall include the capability to integrate heterogeneous system sources within distributed/decentralized identity systems.

To ensure the identifier protocol is compatible with identifier standard or existing identity frameworks that the IoT system is following, the following aspects are required:

- Capability to be compatible with existing ID standards or identity frameworks, and achieve ID consistency;
- Capability of identity qualification (e.g., Know Your Customer, KYC) from different business system.

7.2 Requirements for ID based DPM runtime to support data processing and management runtime

To ensure the data processing and management runtime of blockchain is able to catch up with IoT systems, the following aspects are required:

- Capability to control the accessibility of data instances. It is required that the id based DPM runtime is able to provide access control from specified entities to data instances;
- Capability to map data processing runtime in time. It is required that the data processing of IoT systems has got fast reaction to blockchain.

7.3 Requirements for trust audit of data processing and management

In IoT systems, the data processing and accessibility of “thing” entities is not clearly defined. During data sharing and exchange, data ownership and data processing right may belong to different entity or person, it is not easy to decouple data processing and data accessibility from some IoT system to blockchain system. So the auditing of data processing and management is difficult.

To ensure the self-sovereign data can be processed or managed by pre-authorized entities, the following aspects are required:

- Strong data accessibility control with security data storing. It is required that the access control and data storage of self-sovereign data provides security and privacy;
- Privacy-preserving data processing. It is required to get data processing result without obtaining original data;
- To separate the work of data processing by IoT system and data accessibility, ownership control by blockchain.

8 Functional model of identity framework in blockchain to support DPM

The functional model of identity framework in blockchain provides the mechanisms to support DPM cross systems. The functional design of this model is shown in figure 8-1, each components of the model provides an individual functionality which are further described as below:

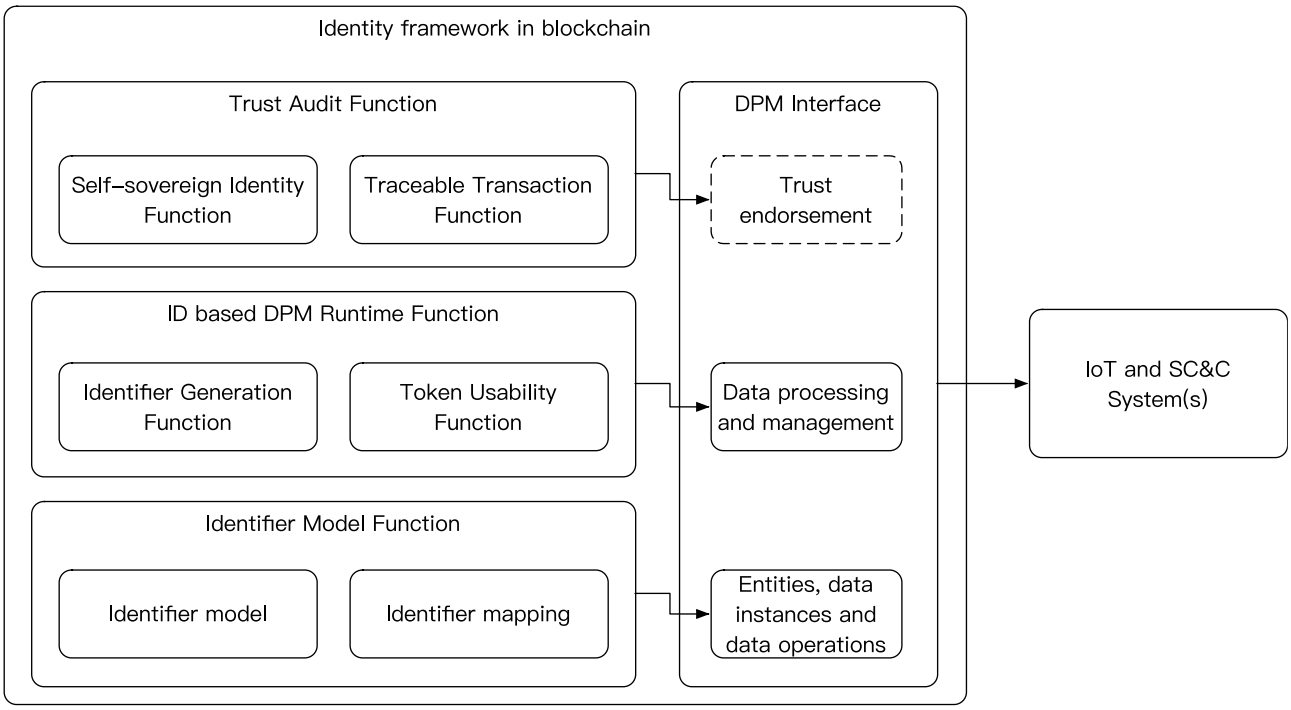

Figure 8-1 Functional model of identity framework in blockchain to support DPM

- Identifier model function: This function offers the mechanisms to map business in IoT systems from off-chain interface with on-chain identifier (see clause 8.1).
- ID based DPM runtime functions: The function provides an on-chain runtime to keep in trace with data processing and management in IoT systems (see clause 8.2).
- Blockchain trust audit function: The function provides the mechanisms to provide trust endorsement and audit for DPM in IoT systems (see clause 8.3).

8.1 Identifier model functions

- Identifier model: The identifier model function provides an identifier model, where the entities, data instances and business actions of off-chain IoT systems are able to be mapped with on-chain identifiers.
- Identifier mapping: The identifier mapping function provides a static identifier mapping capability, where the entities, data instances and business actions of off-chain IoT systems are able to be mapped with on-chain identifiers.

8.2 ID based DPM runtime functions

- Identifier generation function: The identifier generation function provides a mechanism to generate identifiers with access control on data processing and management of IoT systems.
- Token usability function: The token usability function provides a runtime mechanism to do access control on the business actions of entities are taking in IoT systems.

8.3 Trust audit functions

- Self-sovereign identity function: The self-sovereign identity function provides a mechanism to ensure the ownership and accessibility of off-chain data instances in IoT systems.

In IoT and SC&C systems, applications to serve the end users may use services cross systems, platform, and smart devices. Data is generated by smart devices and transferred cross platforms. Due to different business, data could be owned by the smart device, end user or system. Data processing will change the form of data. Self-sovereign identity is to enable data processing without change the ownership and accessibility of the data instances. Which supports further audit for data processing and management.

- Traceable transaction function: The traceable transaction function provides full traceability of the lifecycle of data instances in IoT systems, data generation, data processing and data transferring.

9 Details on identifier model functions

The general identifier model in blockchain provides the mechanisms to support data processing and management in IoT and SC&C system. The general design of this model is shown in figure 9-1, each identifier of the model provides an individual relationship with IT system(s):

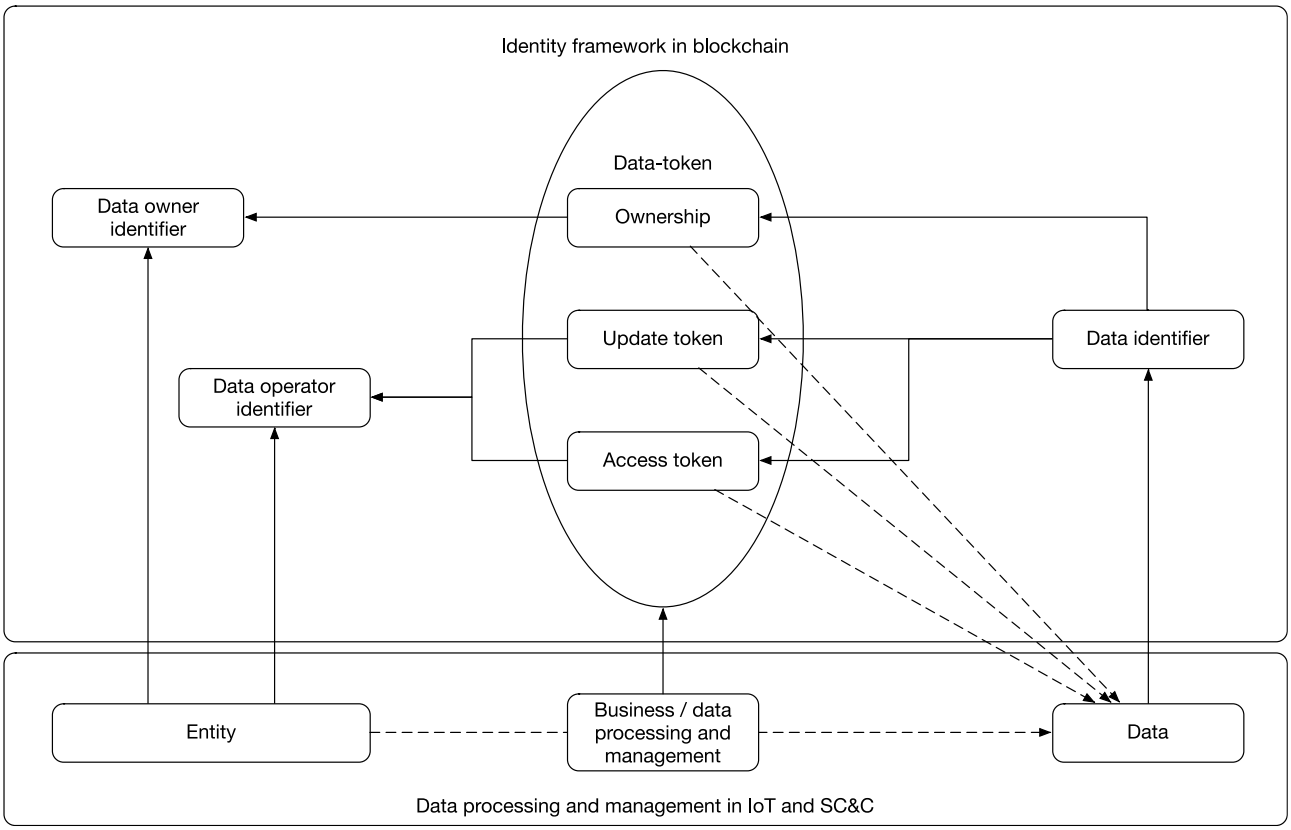

Figure 9-1 General model of identity framework in blockchain

- Entity identifier is mapped with system user of IT system;
- Data identifier is mapped with data instance in IT system;
- Data-token is mapped with business action, esp., in DPM system;

Due to different privileges of data processing and management, entity identifiers can be defined to take multiple privileges of data processing, e.g., data owner identifier of ownership and data operator for data updating and accessing.

- Data instances are stored off-chain and data processing takes place off-chain, while access control of data and data processing is on-chain. The hybrid system is able balance the cost and trust requirement of data resource from on-chain and off-chain;
- All data-tokens are generated based on data identifiers in blockchain system, while data identifiers are mapped to data instances in multiple business systems. Different business systems share the same blockchain system, with entity identifiers hold different data-tokens. The identity model support self-sovereign identifier cross systems with self-sovereign data management;
- Actions entities took will be recorded to blockchain system as transactions of entity identifier using data-tokens, thus the actions on data processing and transferring is traceable.

The blockchain systems are able to save the cost of on-chain storage, by the following steps,

1. Use a predefined structured frame with cryptographic protection as an on-chain identifier , which maps off-chain data instance;
2. Generate data-tokens for different right to perform operations on data instance, based on data identifier;
3. Let data-token travels inside blockchain system.

9.1 Entity identifier model

For the identifier model, both entity identifier and data identifier share the same structure.

Entities take specific actions on data. An entity ID is referring an entity, namely Entity ID (abbr. EID). The entity identifier has got the following structure:

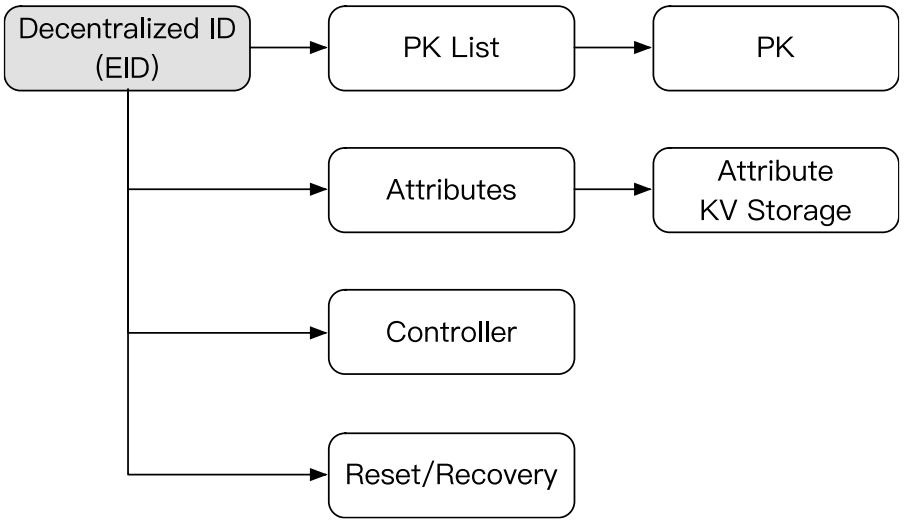

Figure 9-2 Blockchain entity identifier structure

- To save on-chain storage, all blockchain identifier uses simple Decentralized ID (DID [b-6]) model. A blockchain identifier contains a public key list that can make full control to of the DID object;
- A blockchain identifier supports reset (or recovery) of PK list.
  The reset/recovery supports a combination of ID-based operations like threshold method, multi-signature;

- A blockchain identifier contains controller. To satisfy the delegation scenario of IoT and data, that entities other than the object or data the blockchain identifier represents are able to control the object or data. The controller of the identifier can create, modify or delete the identifier, but the controller cannot modify the reset/recovery field. The controller supports ID-based operations;
- To enable self-sovereign identity, blockchain identifier contains an extra key-value storage space for DID extensions or extensible function modules. For example, an index of identity certifications [b-7].

  There are multiple identity frameworks in IoT and SC&C. The entity can manage the attributes of the self-sovereign DID and bind multiple claims of ownership of identifier from other systems.

  Conceptually, a claim is a state or assert that the entity is the case. Technically, a verifiable claim protocol is provided to entity identifier in blockchain. A statement to confirm a claim made by one entity about another (including themselves). The claim is accompanied by a digital signature that can be used by other entities for authentication. The verifiable claim protocol describes in detail the procedures and specifications about issue, store, and verification of verifiable claims.

9.2 Data token

Due to the performance limitation of consensus algorithm and network hypothesis in blockchain system, it is better to use “token” to represent the ownership and/or accessibility (other privileges if any) of data instances, whereas the blockchain data identifiers can represent data instances, so called data-token. In blockchain systems with large network scale, esp., public chain systems, data accessibility update or ownership exchange rely on data-token technology.

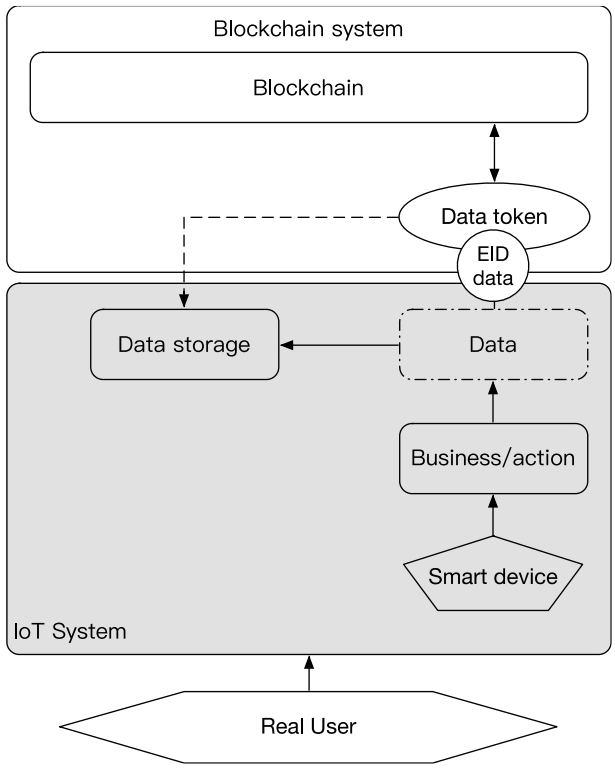

Figure 9-3 Data token for resource integration of IoT and blockchain system

The data identifier represents data instance generated by IoT systems; any cross-systems data processing is related to access control of the data identifier in blockchain. The access control is represented by data-token in blockchain. Any use of the data-token can access off-chain data instances, by on-chain control.

9.3 Identifier model

The identifier model in blockchain is formed upon entity identifier model and data token.

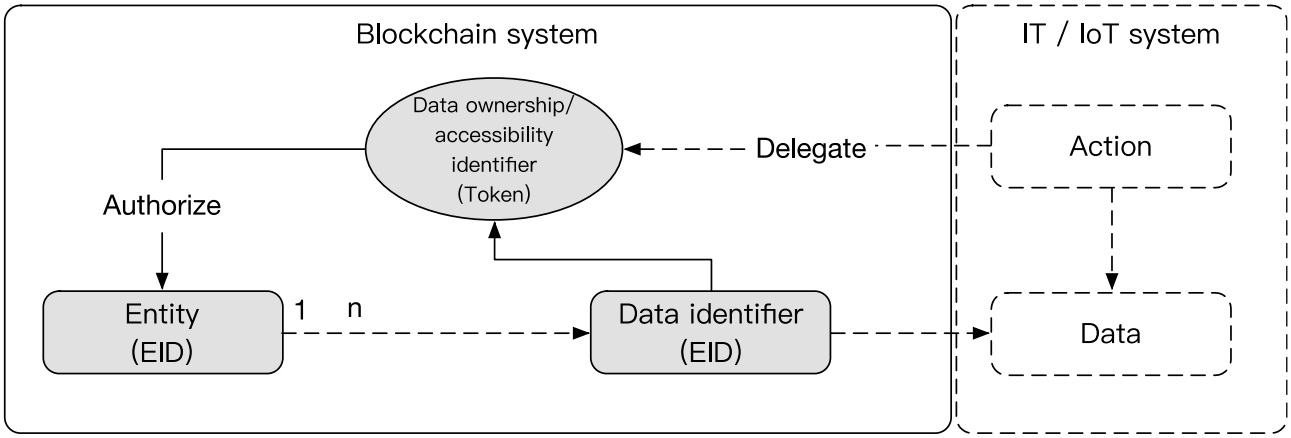

Figure 9-4 Identities in blockchain

- Entity (EID-entity) is related to multiple data instances (EID-data), tokens are bound to data instances (EID-data).

Tokens are representing the ownership/accessibility of data instances; data instances are mapped with EID (with controller) from off-chain to on-chain. Esp., digital assets are referring to valuable data.
This structure is to resolve the requirement of data sharing and exchange in SC&C.

- Smart devices can delegate certain set of actions in form of data token in blockchain and authorize to entities (EID).

Smart devices are entities in blockchain.
This structure is to resolve the requirement of data processing traceability in SC&C.

9.4 Data-token mapping

In general, token is a tool to substituting a sensitive data element with a non-sensitive equivalent.

Blockchain identifier is able to represent off-chain data instance, with non-sensitive equivalent. Data-token technology is used for the access control of on-chain data identifier, results to control its off-chain data instance. Data-token is generated along with the token to access off-chain data instance with limitations, e.g., time expiration, access limitation, count limitation of data-token transferring.

Integrate blockchain technology into IoT system is to provide trust data processing traceability and data validation services. To map data to token, focuses on data processing and data validation.

	Create per instance	**Batch create**

Update per instance	Non-fungible data-token	Partially-fungible data-token
Batch update	-	Fungible data-token

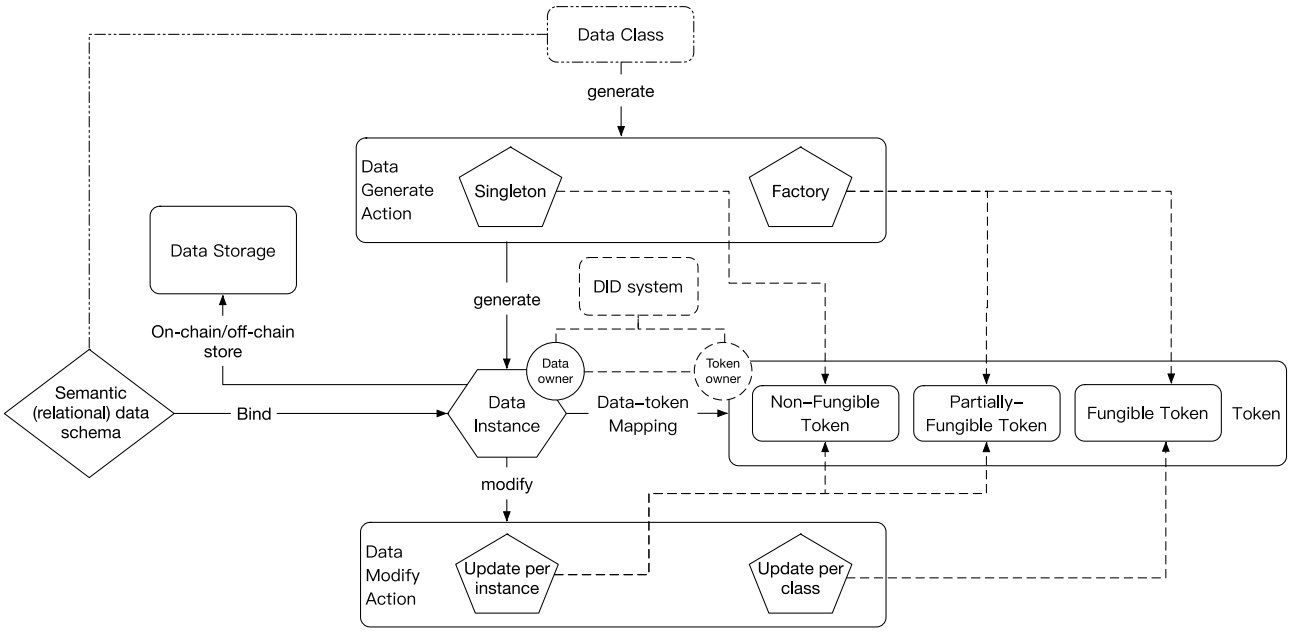

Figure 9-5 Data-token in blockchain

Data processing and accessibility focuses on generation, accessing, updating and deletion of data. Any data class has its own data schema, data processing is based on the schema. Data-token, as token identifier of data instance in blockchain system, focuses on the ownership and accessibility of data instance, and updated with data processing accordingly.

- If the data schema/class is interchangeable, data instance is mapped to fungible data-token;
- If the data instance is unique, data instance is mapped to non-fungible data-token;
- If the data schema/class is interchangeable, but the data instance can be updated to unique instance during the data processing, data instance is mapped to partially-fungible data-token.

Data token share the same technology of "token" in blockchain.

- Fungible data-token: fungible token. Ref., ERC-20[1], OEP-4[2];
- Non-fungible data-token: non-fungible token. Ref., ERC-721[3], OEP-5[4];

[1] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md .

[2] See https://github.com/ontio/OEPs/blob/master/OEPS/OEP-4.mediawiki .

[3] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md .

[4] See https://github.com/ontio/OEPs/blob/master/OEPS/OEP-5.mediawiki .

- Partially-fungible data-token: partially-fungible token. Ref., ERC-1155[5], OEP-506[6].

10 Details on ID based DPM runtime and trust audit for IoT system

The blockchain system provides components for data privacy, while the identifier model functions is able to map data ownership and data processing, all business actions will be recorded and traced by blockchain system. In IoT system, data instances will be generated, and modified by different entities.

Therefore, blockchain system is required to make full trace on data processing and management of off-chain data instances.

10.1 Data sharing and exchange with data-token

Data exchange (data ownership transfer) in ID based DPM runtime includes,

- on-chain data-token exchange;
- cross-chain data-token exchange;
- on-chain data-token and off-chain data exchange (hybrid data exchange mode).

There are altogether two different ways to do data sharing and exchange by then,

1. From off-chain data sharing and exchange to map with on-chain record,
    a. Data sharing, to create the access data-token of on-chain identifier and transfer the data-token to target;
    b. Data exchange, to transfer the ownership data-token/token to target, in each side;
2. From on-chain data-token sharing and exchange to map with off-chain data sharing and exchange[7].

In blockchain system, token exchange action has got trust endorsement and supports atomic transactions, both for cross-chain and inter-chain.

Blockchain provides trust audit for data sharing and exchange.

Data-token share the same technology of token, data sharing and data exchange is mapped to token sharing and token exchange in blockchain technically, e.g., ERC-823[8], OEP-8[9].

10.2 Decouple data accessibility, ownership with data processing

The entity identifier, data identifier and data-token framework decouples data accessibility and ownership after the data is generated.

---

[5] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1155.md .

[6] See https://github.com/ontio/OEPs/blob/67f6c537ecfe0d7c52aece55be4b182f146f50a3/OEPS/OEP-506.mediawiki .

[7] See section 11.

[8] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-823.md .

[9] See https://github.com/ontio/OEPs/blob/master/OEPS/OEP-8.mediawiki#transferMulti .

In IoT systems, smart device is able to generate and modify data, while the data ownership may be assigned to different roles, e.g., real users, systems, or other devices.

In ID based DPM runtime, data identifier is generated the time data instance is created, the data-token to access data instance will be generated on demand of data processing. The generation and using of data-token is post to blockchain system as transactions. The blockchain system provides trust endorsement of all the transactions, which are able to be audit.

The blockchain system provides the traceability of data processing, and the capability of decoupling data accessibility, ownership with data management.

10.2.1 Integrate ID based DPM runtime into IoT system

An IoT system is a system for smart device network to connect, interact and exchange data. Smart devices are able to execute certain interactions and generate/modify data.

IoT user uses the system with AAA management.

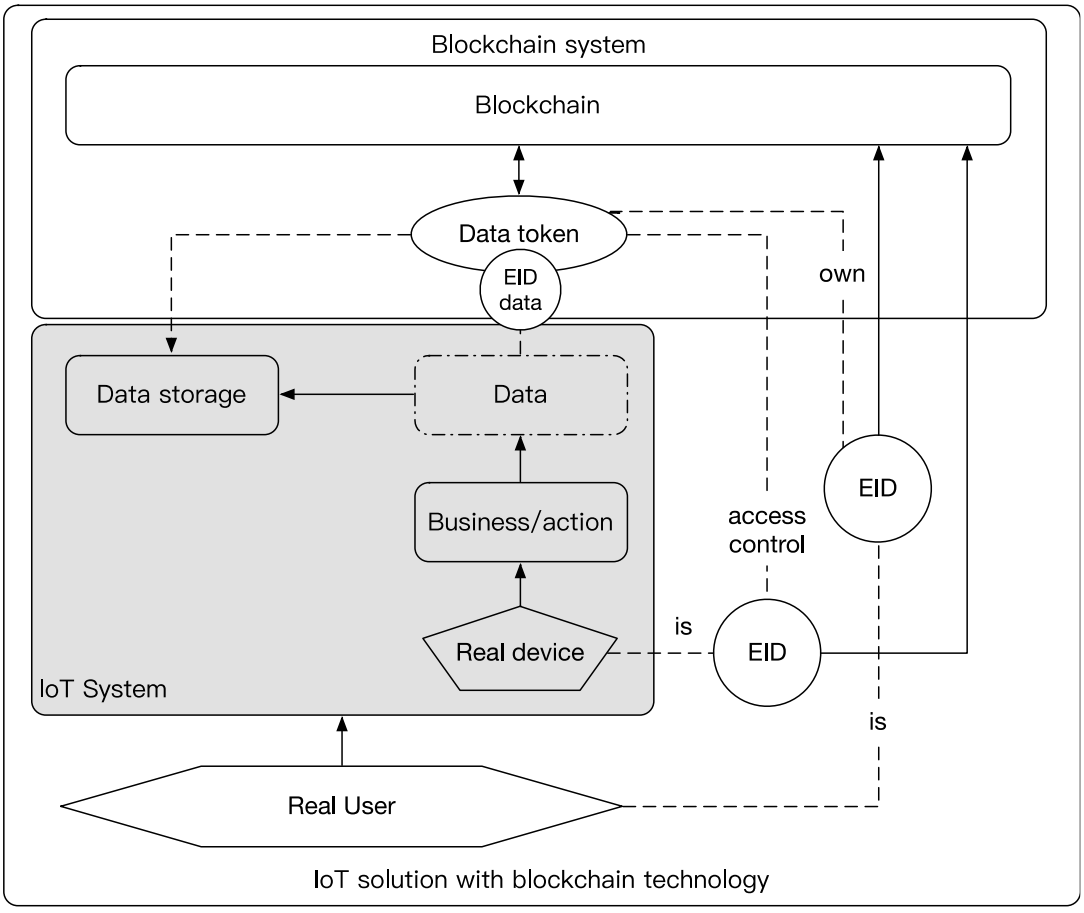

Figure 10-2 Integrate blockchain identity system into IoT system

To integrate IoT system into blockchain system,

- Users and/or smart devices are mapped to EID, to have IoT system share its user/device with common account in blockchain system;

- Data can be mapped to data identifiers in blockchain systems, with the form of entity identifiers. With the technology of data privacy and data protection provided by blockchain system, any business action taken by smart device will not reveal data privacy;
- The accessibility and ownership of data can be mapped to data-token of data identifier in blockchain system, and data token is owned by entities;
- Data token can access data instance directly, with action recorded on-chain;
- Any data processing will be traced with on-chain transactions.

To integrate IoT system into blockchain system, IoT system can be benefit from the following items,

- Provide data processing traceability
- Provide services for data protection and data privacy with trust
- Decouple data processing with data accessibility, ownership

To decouple the accessibility, ownership with data processing can satisfy various of IoT and SC&C scenarios.

10.2.2 Data sharing and transferring (exchange) in SC&C

The typical scenario of data transfer is to change the ownership of data-token.

- For data exchange, encapsulate a set of token transfer from both directions in one atomic transaction, on-chain token swap/exchange represents off-chain data exchange.
- For data sharing, generate multiple access tokens and transfer to target users.

In data sharing scenario, multi-signature or threshold-signature can be used to control the authentication of data processing.

Furthermore, if the tokens are in different blockchain instances, there are cross-chain protocols for atomic token swaps, e.g., hashlock [b-8].

According to the data processing of IoT and SC&C systems, the generation, removal and updating of data instance is managed by on-chain data-token of related on-chain data identifier, e.g., any sharing and transferring of data instance is traced by the sharing and transferring of access-token of data identifier. With cryptographic protocols built upon data systems, data processing executors can update data instances without access the origin data source, e.g., zero-knowledge proof, multi-party secure computing, homomorphic encryption。

By manage the belonging of data-token, data accessibility, ownership is decoupled with data processing.

11 Details on ID based runtime and trust audit for data interoperability cross IoT systems

The runtime to support data interoperability satisfies two basic requirements,

1. cross-community and cross-application data sharing;
2. data transformation information and knowledge, achieving information alignment cross system.

11.1.1 Trust data processing and management

Blockchain system provides solutions for data processing traceability and data validation.

The ID based DPM runtime provides the capability of trust data processing and accessibility for data interoperability in IoT and SC&C,

- data processing traceability;
- on-chain data-token sharing and exchange[10].

The trust audit of data communicates directly with data interoperability systems, usually with architectural design as a hub.

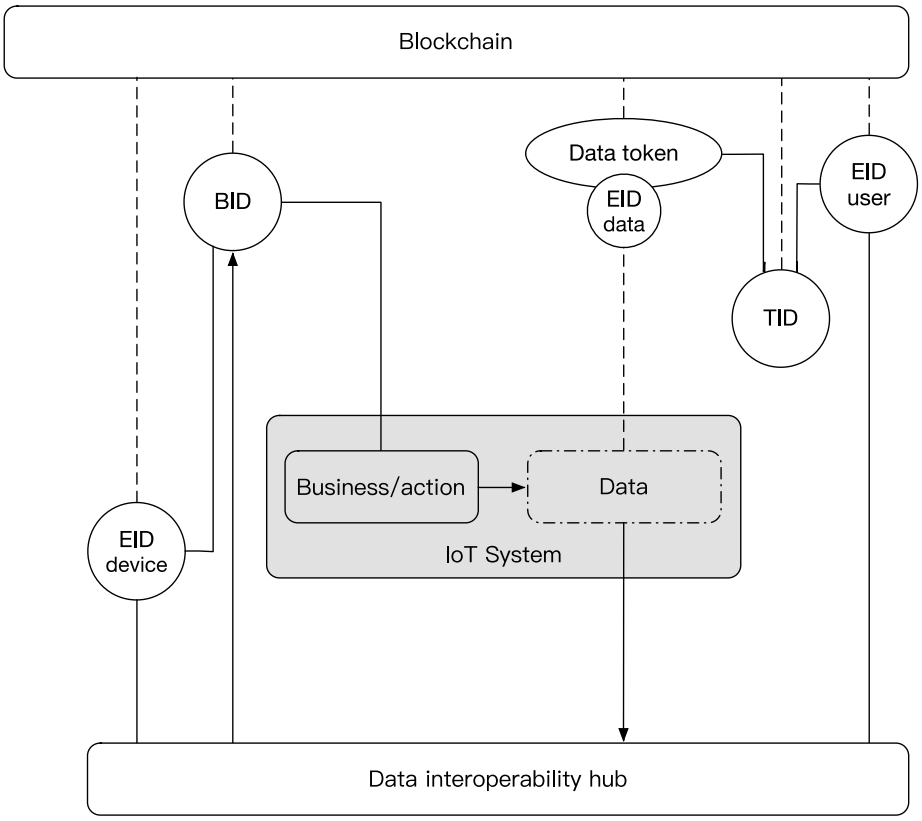

Figure 11-1 BCID framework to provide “trust audit” for data interoperability cross IoT systems

The diagram demonstrates the way to integrate blockchain framework in blockchain with IoT and SC&C interoperability systems and provide trust audit of data processing and management.

- All entities inside system has got its own EID and saved to blockchain. The EID is self-sovereign;
- All data instances generated/updated in the off-chain system are mapped to on-chain data identifier;
- To make use of on-chain data identifier, BCID generates data-token for ownership and different privileges on demand. Use data-token as a token to access off-chain data instance;
- All data-tokens are owned by entities, the state of entity-“data-token” is saved to blockchain;

[10] See Appendix I.

- Any data process actions that cause the change of data instance can be synced to blockchain as an upgrade of data identifier if necessary;
- Any changes of data ownership shall be synced to blockchain for the ownership change of data-token, and update controller in data identifier.

The trust audit is based on the blockchain system as a black box ledger, which just focuses on "what" action is taken and been logged with trust endorsement, which does not focus on "how" the data interoperability is formed. Data interoperability hub sync the "what" information from interoperable system to with blockchain trust endorsement and provide ownership and accessibility lookup service from trust auditing to interoperable system.

11.1.2 Integrate identity framework in blockchain to support data interoperability

All roles in data interoperability for IoT systems is mapped with blockchain identifiers, and data access control can be handled by data-token in blockchain.

The data interoperability hub is to handle off-chain data interoperable actions with the use of on-chain data-token.

In IoT environments, users call IoT services cross platforms, data management is traced by on-chain entity identifiers and data identifiers, data interoperability is controlled by on-chain data token and passed through blockchain ledger system, which provides trust endorsement for auditing.

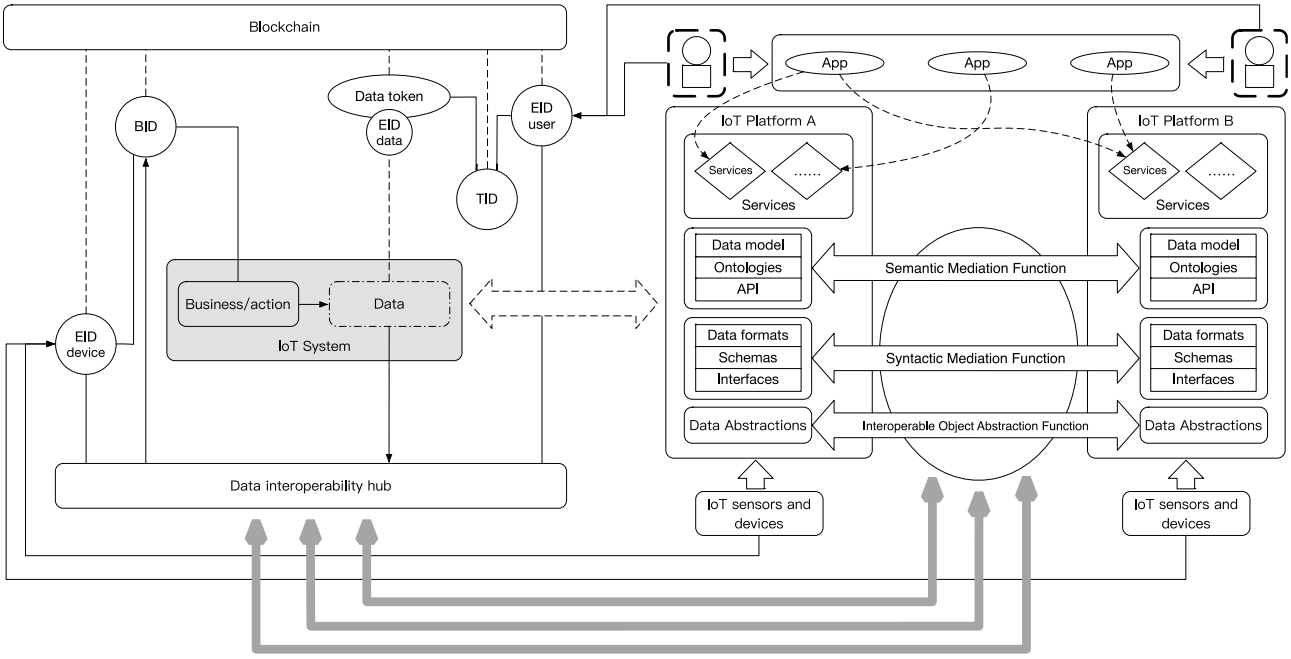

Figure 11-2 BCID framework to support data interoperability framework for IoT and SC&C

11.1.3 Hybrid model to support data interoperability

Furthermore, it is required to provide the following services to extend the capability of data interoperability

- cross-chain data sharing and exchange;

- on-chain and off-chain data sharing and exchange (hybrid data sharing and exchange mode).

Which will satisfy complex scenarios.

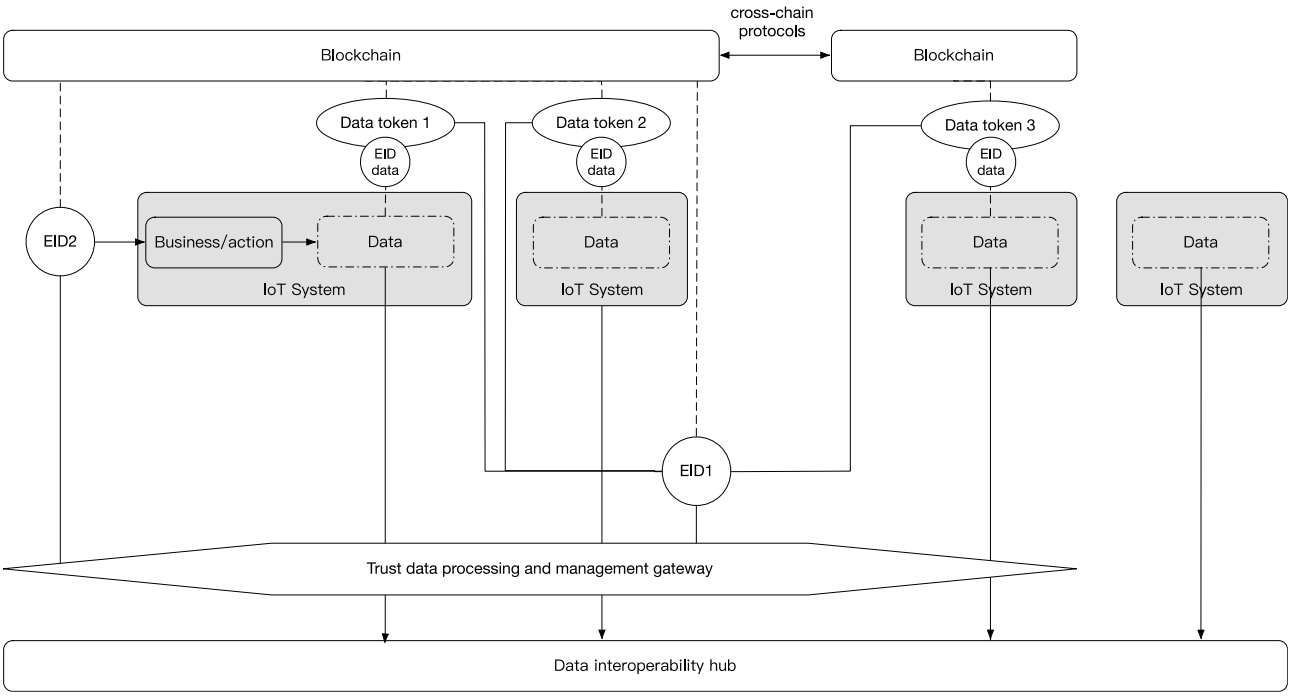

Figure 11-3 Complex data interaction scenario

An example diagram describes an open system for data interoperability.

- Cross-chain scenario to prove trust audit of data interoperability;
  - Use cross-chain protocols to sync ID system;
- Traditional IoT system without trust audit can also be involved;
  - Any data interoperable action taken has not trust endorsement and no record in blockchain ledger (DLT system);
  - Data transferred from non-DLT system to DLT system will trigger a “generation” action in the DLT system and got the data-token.

Appendix I
Data exchange with BCID framework

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

Data interoperation in BCID framework includes common data operation, data-token mapping, data token value assessment and token-data exchange.

I-1 Data operation

Data generation and modifications.

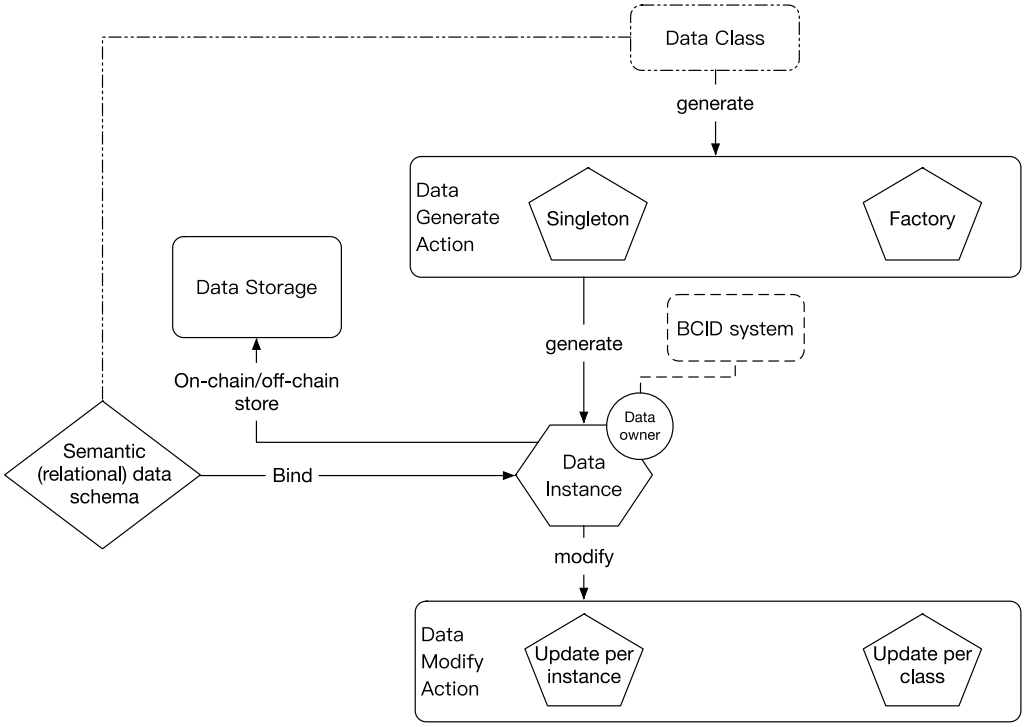

Figure I-1. BCID – data operation

Data operation in every IT system includes data generation and data modification. Data management is required to resolve the problem of data storage.

For data interoperability cross systems, data alignment is required, where semantic (relational) data schema is used.

The preparation work to integrate BCID framework with IT systems is to define data schema and data processing model.

I-2 Data token mapping

Map data to token.

	Create per instance	**Batch create**
Update per instance	Non-fungible token	Partially-fungible token
Batch update		Fungible token

In general, token is a tool to substituting a sensitive data element with a non-sensitive equivalent.

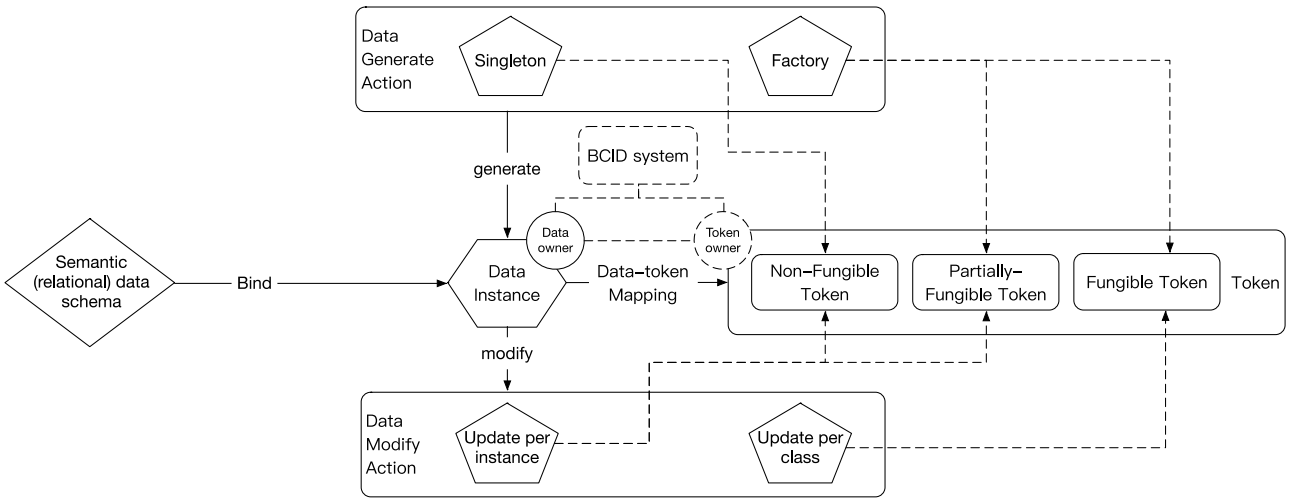

Figure I-2. BCID based data token mapping in blockchain system

In BCID system, the on-chain data identifier is generated for each off-chain data instance. Data token is generated for multiple privileges for the data instance, e.g., ownership, accessibilities, and modifiability.

- If the data instance is created in a singleton pattern, implies the data shall be updated per instance, non-fungible token is generated for data processing;
- If the data instance is created in a factory pattern, and the data instances are to be updated per class (all by once), fungible tokens are generated for data processing;
- If the data instance is created in a factory pattern, and the data instances are to be updated per instance, partially-fungible tokens are generated for data processing.

The fungible, non-fungible and partially fungible token is used in the generation of data accessibility tokens.

I-3 Data token value assessment

Value assessment based on data characteristics evaluation (with semantic technique).

Most public chains, which are using tokenomics as trust endorsement of blockchain system, usually use valuable tokens, e.g., utility token.

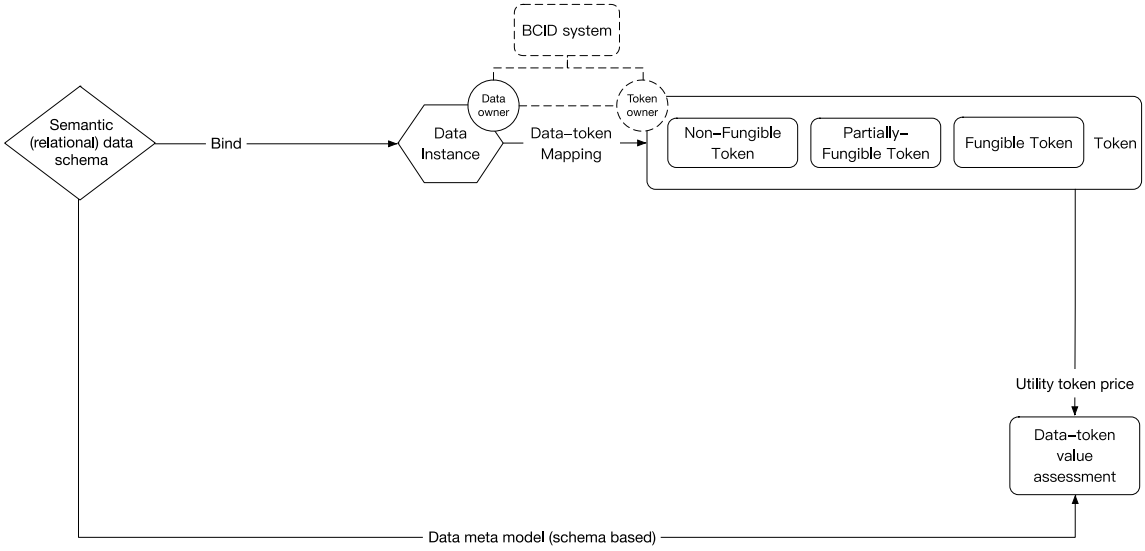

Figure I-3. Blockchain based token assessment

Data-token share the same technology of token in blockchain. Value assessment of data-token is a binding of data-token with certain amount of utility token, technically.

I-4 Token-data ownership exchange

Data ownership transfer/exchange based on token transfer/exchange.

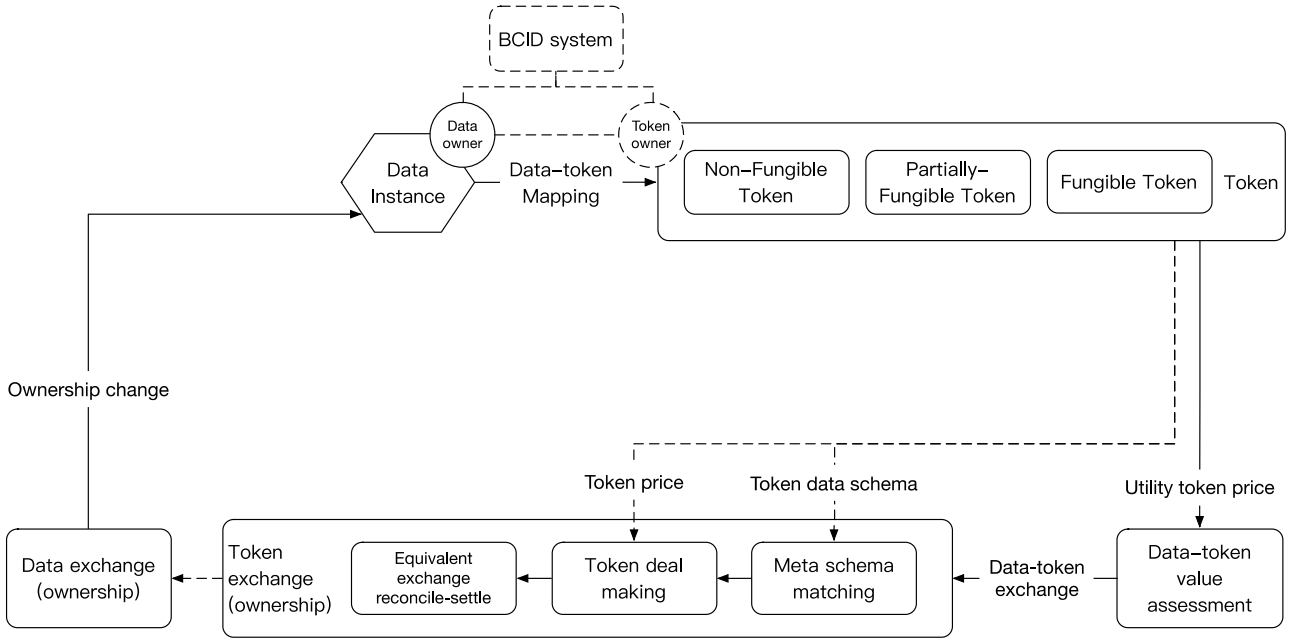

Figure I-4. Blockchain based data- token exchange with BCID framework

Data-token and utility token exchange, the ownership of data-token is transferred, meaning the data ownership is transferred accordingly.

Bibliography

[b-1] “Fungible Synonyms, Fungible Antonyms.” *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/thesaurus/fungible.

[b-2] Schroeder, Stan. “Crypto Trading Card Game 'Gods Unchained' Looks Pretty Sweet in First Gameplay Trailer.” *Mashable*, Mashable, 16 Nov. 2018, mashable.com/article/gods-unchained-trailer/.

[b-3] “OID Repository - Home.” *OID Repository - Home*, www.oid-info.com/.

[b-4] Sun, et al. “Handle System Overview”, *RFC Editor*, http://www.rfc-editor.org/rfc/rfc3650.txt.

[b-5] “EPC/RFID.” *GS1*, 14 Jan. 2015, www.gs1.org/standards/epc-rfid.

[b-6] Reed, Drummond et al. "Decentralized Identifiers (DIDs)" W3C, Credentials Community Group, 2017, https://w3c-ccg.github.io/did-spec/.

[b-7] “Overview.” *ONT ID Document*, Ontology Document, pro-docs.ont.io/#/docs-en/ontid/overview.

[b-8] “Hashlock.” *Hashlock - Bitcoin Wiki*, en.bitcoin.it/wiki/Hashlock.