Blockchain based data trust sharing mechanism in the supply chain

Wang Luya and Guo Shaoyong

December 25, 2018

Blockchain based data trust sharing mechanism in the supply chain

[1]Wang Luya[0000-0002-3722-7642] [2]Guo Shaoyong

Beijing University of Posts and Telecommunications, Beijing 100876, China
wangluyadei@163.com

Abstract. Currently, the trust and privacy problem is an obstacle during data sharing process in supply chain. To solve it, this paper proposes a blockchain based data trust sharing mechanism in the supply chain. Firstly, we design the architecture to introduce the system framework, service process and data model for data trust sharing. Secondly, we implement the blockchain-based supply chain platform, consisting of account management module and data request processing module with open data index name extension (ODINE). At last, we state an use case to analyze this platform.

Keywords: Blockchain Supply chain Data storage and access

1 Introduction

[1] Supply chains are networks with big data attributes that connect providers, manufacturers, operators, retailers and consumers. In the supply chain, information cooperation sharing plays an important role in improving the resource utilization of upstream and downstream enterprises. However, at present, the problem of low efficiency in information access and value mining and privacy leakage limit the sustainable development of the supply chain system [1]. Blockchain is a distributed computing paradigm with features of centralization, trust, collective maintenance, reliable storage, and automatic operation. From this perspective, blockchain is a natural remedy for supply chain system, which can achieve data transparency, form a good transaction order and commercial ecology under the condition of trust, and provide high-level data security protection.

Since Nakamoto took the lead in proposing a set of Internet governance mechanisms [2] based on cryptography and trust in "Bitcoin: A Peer-to-Peer Electronic Cash System", many scholars began to study blockchain technology in the supply chain applications in the field. The rapid development of B2B(Business-to-Business) trading theory and integration platform establishes an efficient and secure supply chain blockchain transaction prototype [3-6], but the current low level of system interoperability lead to high investment costs, which limit the realization of potential benefits [7-8]. Chris et al [9]proposed to improve the digital activities in the internet supply chain finance to achieve commercial operation. Korpela Kari[10] and others developed a

[1] This work was supported in part by the National Natural Science Foundation of China (61702048) and State Grid Corporation of Science and Technology Project (5211DS17002D).

digital supply chain (DSC) conceptual model, but it has limited scalability. Abeyratne et al [11] discuss a blockchain-based manufacturing supply chain system to improve data transparency, but this technology requires some IT infrastructure for all participants. For data governance issue, Azaria A [12], Liu PTS [13] and others based on blockchain technology to give a model for recording and accessing medical big data, but two further exploration is needed to maintain the auditability of the chain. For the problem of data security storage and sharing mechanism [14], Guy zyskind et al[15] proposed to store information and parse it by using bitcoin, but it is very expensive. Ahmed Kosba et al[16] introduced a third party database, and Zhang Ning et al[17] introduced an audit center for system data storage and extended access , but the two models for special cases lacked other models. Aizhan NZ et al[18] used multi-signature technology to protect information security in distributed energy supply chain systems through , but it did not involve data processing integration and industry analysis.

For those problems, we combined encryption technology and named query technology to data sharing processing in supply chain for designing our architecture. And then we implement the blockchain-based supply chain platform, consisting of account management module and data request processing module. In data request processing module, we construct a new open data index name extension for the data index. At last, we state an use case to analyze this mechanism.

2 Data trust sharing architecture

2.1 Blockchain based transaction processing model

The architecture consists of three main parts: Data collection, Data procession and Data storage and access. In the first part, we use intelligent contracts to support data sharing processing between the upstream and downstream of the supply chain to improve the level of data trust. In the second part, we analyze and extract the value of the integrated data. Finally, we use the ODINE name index standard to access data safely and effectively.

In the supply chain system, data is mainly derived from peripheral device acquisition, transaction processing, and personal information input. The process is roughly as follows:

- Step 1: Summarizing data and extracting the transactions and information recorded in the blockchain. Using intelligent contracts for loading, noise reduction and format conversion.
- Step 2: Integrating various industry data and tapping the value.
- Step 3: Classifying the identification objects according to the ODINE naming rules. Storing the acquired industry information sets and user information sets through the blockchain API interface according to the naming rules.
- Step 4: After verifying the identity and permissions, the visitor can send a data request and find the data location through the ODINE parsing library.

Among them, the intelligent contract can be automatically executed when the access condition is satisfied. The timestamp of the tag verifies the authenticity of the original data.

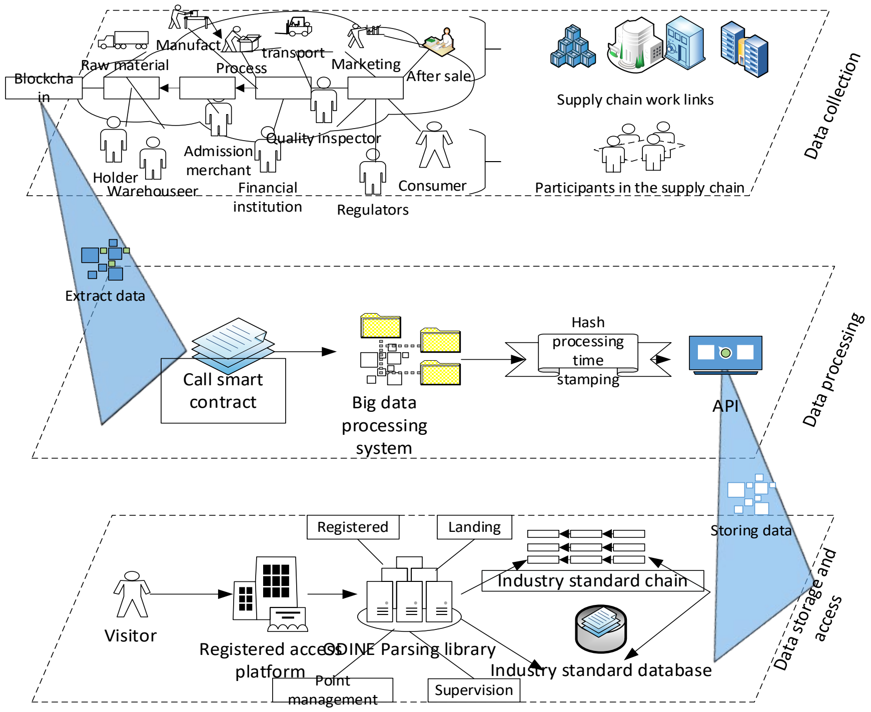

Fig. 1. Overview of the process flow

2.2 Blockchain based data processing

After processing, the data can generate industry value. In the data processing part, the flow of the data is:

- Step 1: The transaction information and industry data are stored in the blockchain through the P2P transaction module.
- Step 2: The node calls the intelligent contract to clean the data for inspection, fault diagnosis, and information specification.
- Step 3: The data is classified, integrated, and reorganized by the big data processing module, and named according to certain rules (In Section 4.3).
- Step 4: The data is restored to the blockchain by calling the API interface of the blockchain system.
- Step 5: When a visitor accesses data information he can obtain data by a certain authority audit (In Section 4.1) and access rules (In Section 4.2).

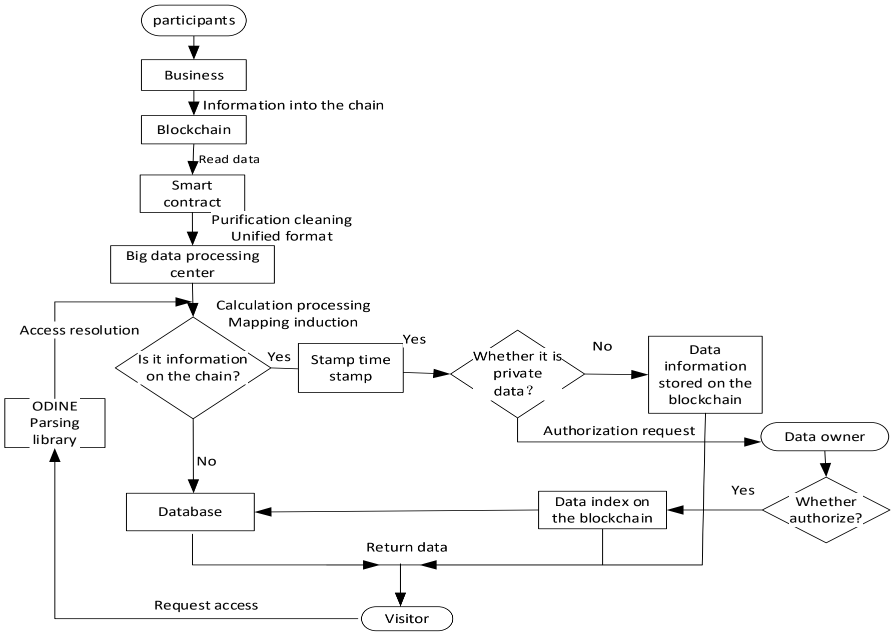

Fig. 2. Data processing flow

2.3 Inter-chain data correlation model of supply chain

Integrating and mining the potential value of data is one of the keys to this paper, so data correlation analysis is required.

The value of the data is gradually tapped and aggregated. When business partners conduct business activities directly or indirectly between supply chains, they generate a large amount of industry data that can be used as a data source for big data processing after purification. By arranging messy data into industry data sets or personal information sets, we can further analyze the intrinsic connection of abstract data for market analysis. In order to achieve secure storage and privacy protection of the integrated data, the data is stored in different modes. The key data is stored in the blockchain, the common data is put into the database, and the private data is set access rights.

Table 1: Meaning of model parameters

function	definition		
TxHash .Hash	The root hash of the transaction tree	Extra []byte	Block additional data
ReceiptHash .Hash	The root hash of the receipt tree	MixDigest .Hash	Hash value, combined with Nonce for workload calculation
Difficulty *Big.Int	The difficulty of this block	Nonce BlockNonce）	Random value when the block is generated
Number *Big.Int	Block number of this block	Datai.Int	Transaction data corresponding to

			each initial hash
Time *big.Int	Timestamp	Datacategory.Int	Data category
[SCHEME]	Data ODINE identification string	Databelong.Int	Data attribution account
Accountneed*Big.Int	Account demand information	Datatype.Int	Data transaction
Accounttrade*Big.Int	Account transaction information	Datachange.Int	Data rate of change
Authority.Int	Access permission	MerkleRoot .Hash	Block root hash value

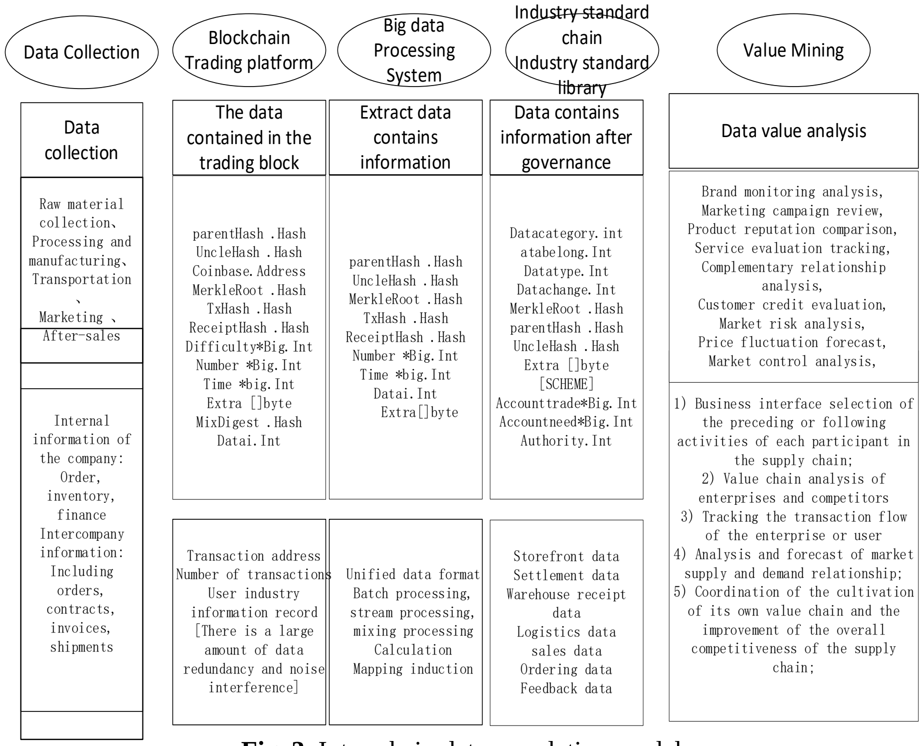
Data Collection
Blockchain Trading platform
Big data Processing System
Industry standard chain Industry standard library
Value Mining
Data collection
The data contained in the trading block
Extract data contains information
Data contains information after governance
Data value analysis
Raw material collection、Processing and manufacturing、Transportation、Marketing 、After-sales
parentHash .Hash
UncleHash .Hash
Coinbase.Address
MerkleRoot .Hash
TxHash .Hash
ReceiptHash .Hash
Difficulty*Big.Int
Number *Big.Int
Time *big.Int
Extra []byte
MixDigest .Hash
Datai.Int
parentHash .Hash
UncleHash .Hash
MerkleRoot .Hash
TxHash .Hash
ReceiptHash .Hash
Number *Big.Int
Time *big.Int
Datai.Int
Extra[]byte
Datacategory.int
atabelong.Int
Datatype.Int
Datachange.Int
MerkleRoot .Hash
parentHash .Hash
UncleHash .Hash
Extra []byte
[SCHEME]
Accounttrade*Big.Int
Accountneed*Big.Int
Authority.Int
Brand monitoring analysis,
Marketing campaign review,
Product reputation comparison,
Service evaluation tracking,
Complementary relationship analysis,
Customer credit evaluation,
Market risk analysis,
Price fluctuation forecast,
Market control analysis,
Internal information of the company: Order, inventory, finance Intercompany information: Including orders, contracts, invoices, shipments
Transaction address
Number of transactions
User industry information record
[There is a large amount of data redundancy and noise interference]
Unified data format
Batch processing, stream processing, mixing processing
Calculation
Mapping induction
Storefront data
Settlement data
Warehouse receipt data
Logistics data
sales data
Ordering data
Feedback data
1) Business interface selection of the preceding or following activities of each participant in the supply chain;
2) Value chain analysis of enterprises and competitors
3) Tracking the transaction flow of the enterprise or user
4) Analysis and forecast of market supply and demand relationship;
5) Coordination of the cultivation of its own value chain and the improvement of the overall competitiveness of the supply chain;

Fig .3. Inter-chain data correlation model

After registering, the users can drive the value realization. They can implement business transactions, access information and decide how to respond to other people's access requests.

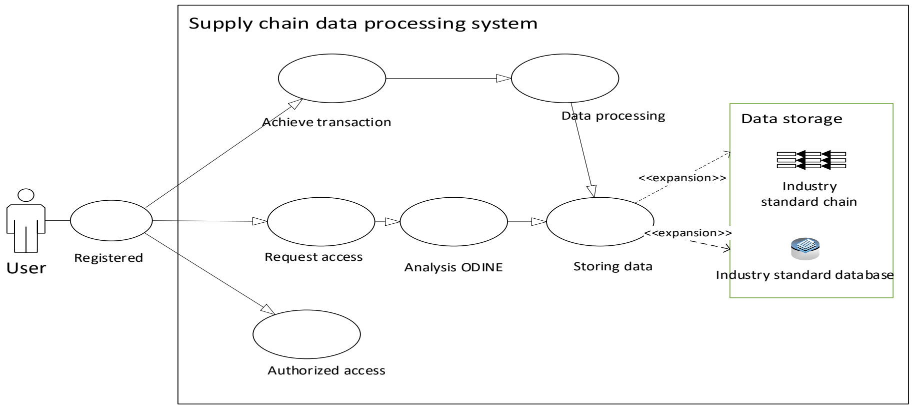

Fig. 4. Value extraction

3 Blockchain-based supply chain platform implementation

3.1 Account Management Module

To ensure secure and efficient access to information, an account management module has been established. When an account is being registered, some corresponding information must be submitted. When a user logs in, the client can authenticate. The registration process includes:

- Step 1: The applicant initiates a registration request and sends his personal ID.
- Step 2: If the initialization ID is legally registered, the calculated parameters will be issued and sent to the application account.
- Step 3: Registrant sends his personal information and public key.
- Step 4: The platform generates the user's private key according to the user's public key and parameters.
- Step 5: The user inputs personal information encrypted by the private key into the registration platform, and the platform executes the corresponding access authority setting flag according to the identity information.

When data is requested, the visitor sends the information encrypted by private key, and the authentication platform matches the information to identify the visitor's permissions. Finally, the access platform sends the user request and user account address to the ODINE parsing library for data request processing.

Table 2: Participants, Run functions, and Parameter definitions

Participating object	Abbreviation		
User (participants)	U	Registration certification platform	(R)
Database	D	Certification Platform	(C)
Named resolution library	ODINE	Integration Platform	(I)
operating	meaning		

U wants to access its visitor record in D	Data1	Modify information in the industry standard library chain	Data3
Access information in the industry standard library chain	Data2	Delete information in the industry standard library chain	Data4
Have access	Token1	Have the right to delete	Token3
Have the right to draft	Token2		

Function	Definition		
Permission type tag	Authority( )	Blockchain address (identity)	Address
Generating a public key	Generate( )	Non-blockchain address (identity)	ID
Generate access parameters	Calculate( )	Direct insertion transaction	Input( )
Match verification	Match( )	Create index	Create( )
Query by index	Find( )	Identity legality verification	Legal( )
Insert key-value pairs	Insert( )	Pre-inserted key value	Preinsert( )

The registration process is as follows:

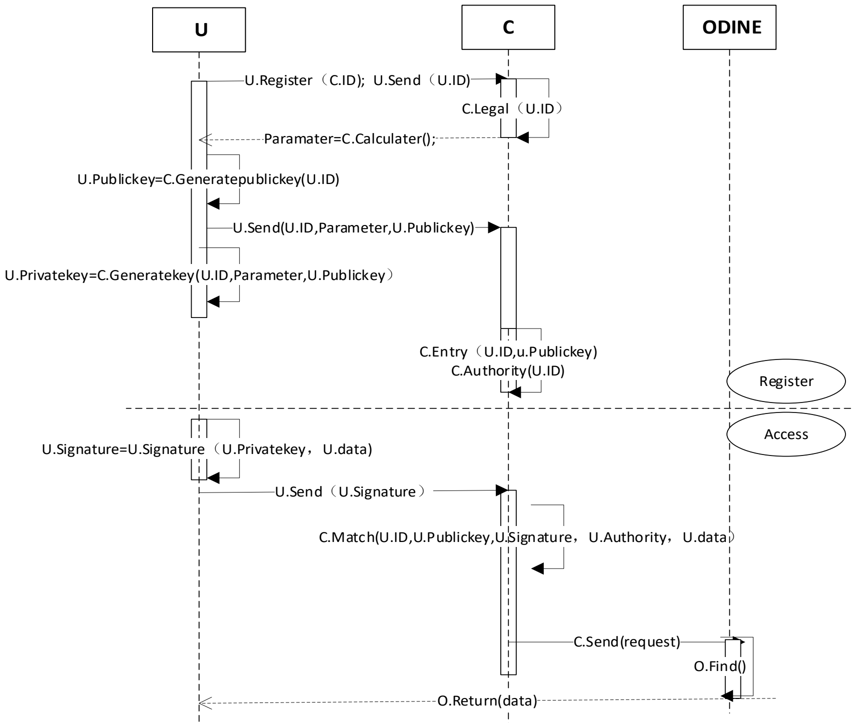
U
C
ODINE
U.Register（C.ID); U.Send（U.ID)
C.Legal（U.ID）
Paramater=C.Calculater();
U.Publickey=C.Generatepublickey(U.ID)
U.Send(U.ID,Parameter,U.Publickey)
U.Privatekey=C.Generatekey(U.ID,Parameter,U.Publickey）
C.Entry（U.ID,u.Publickey)
C.Authority(U.ID)
Register
Access
U.Signature=U.Signature（U.Privatekey，U.data)
U.Send（U.Signature）
C.Match(U.ID,U.Publickey,U.Signature，U.Authority，U.data）
C.Send(request)
O.Find()
O.Return(data)

Fig. 5.: User Registration and Access Sequence Diagram

3.2 Data Request Processing Module

When making data access, certain naming rules are required to improve efficiency. In this paper, a new big data information access naming rule (ODINE Open Data Index Naming Extension)is applied to the supply chain system by combining the URI (Uniform Resource Identifier) specification and the ODIN [19] naming convention. It is an index name and identification of the data resource, which will become part of the data resource. It is independent of the actual address and makes the data unique and traceable. The specific naming rules are:

[1] Data in the block:
[WHETHER_VIP][IF_PRI]/[BLOCK_SN].[TRANS_INDEX]/[AUTHORITY]RESOURCE_ID#[DATA_SN].[CHUNK_INDEX]
[2] Access restricted data in the block:
[WHETHER_VIP][IF_PRI]/[BLOCK_SN].[TRANS_INDEX]/[AUTHORITY]RESOURCE_ID.OWNER_ID#[DATA_SN].[CHUNK_INDEX]
[3] Subject information in the database:
[WHETHER_VIP][IF_PRI]/ [AUTHORITY]RESOURCE_ID[FORM]#[KEY]

[WHETHER_VIP] is used to distinguish whether the data is important industry data stored in the block; [IF_PRI] is used to identify whether the data needs special authentication by the ODINE owner; SN is the serial number； [AUTHORITY] is access rights identification; RESOURCE_ID is the resource identifier; OWNER_ID is the point resolution of the ODINS owner; [DATA_SN] is in the industry standard chain The block number; [CHUNK_INDEX] is the index of the subdata in the block; [FORM] is the database header; [KEY] is the primary key value of the data accessed in the data base. The ODINE, metadata, and URL information of the open data resource can be stored in the ODINE parsing library or the ODINE owner's database in the form of Json encoding.

When a visitor sends a data access request, the ODINE parsing library resolves the location and finds the data location. The corresponding processing of the above three cases is as follows:

[1] The analysis result of the data maps the blockchain to acquire data.
[2] The parsing library sends the access request to the ODINE owner for information confirmation, and accesses the industry data after obtaining the permission.
[3] Acquire the requested data according to the URL of the metadata obtained by the ODINE string and the actual data address.

This access rule not only enables efficient storage and access to supply chain integration information, but also protects data security and respects personal privacy data.

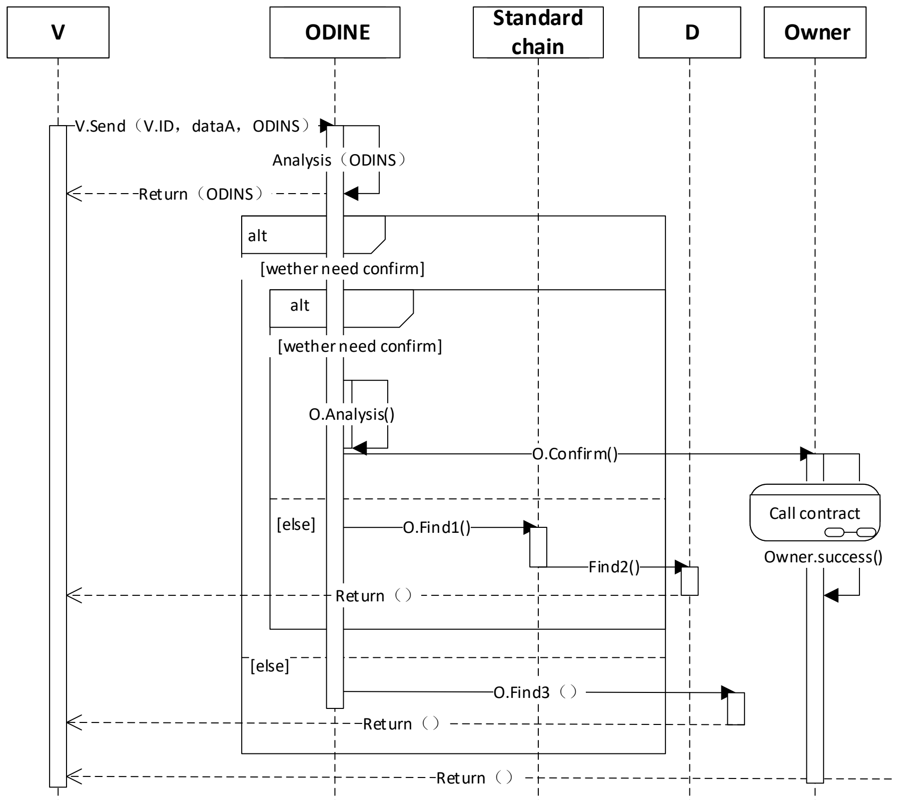

Fig. 6. Data Request Processing Flow

3.3 Use Case Analysis

We take the energy-saving and environmental protection enterprise as an example to realize the application analysis of this architecture.

Based on this mechanism, enterprises can register and access the API interface of the system to obtain effective industry reference for product design, raw material procurement, sales and other aspects. Sewage treatment and recycling can be recorded in the blockchain for national supervision. When the core data of the supply chain is obtained, the competitiveness of the enterprises will be greatly improved.

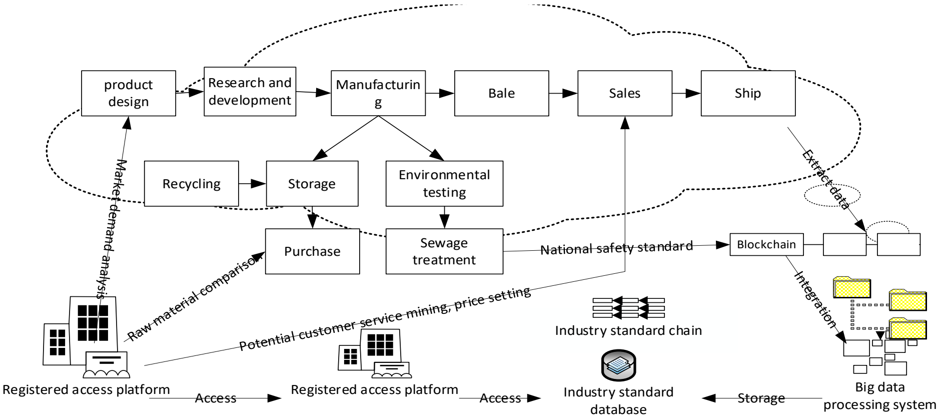

Fig. 7. Use case analysis

4 Summary

Aiming at the problem of information processing and trust sharing in supply chain system, this paper proposes a data processing model based on blockchain technology. We explain the operating principle of the mechanism by giving the overall framework and interpreting the main model. We design the ODINE naming rules for accessing to data effectively and safely. Some algorithms in the mechanism still require further innovation and optimization to increase efficiency. In the next study, we will continue to research the potential relationship analysis of data between different industries.

References

[1] Beth S, Burt D N, Copacino W, et al. Supply chain challenges. building relationships[J]. Harvard business review, 2003, 81(7): 64-73, 117.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL] https://bitcoin.org/bitcoin.pdf.

[3] Hazen, B.T. and Byrd, T.A., 2012. .Toward Creating Competitive Advantage with Logistics Information Technology. International Journal of Physical Distribution & Logistics Management, Vol. 42 No 1, pp. 8-35.

[4] Jeffers, P.I., Muhanna, W.A. and Nault, B.R., 2008.Information Technology and Process Performance: An Empirical Investigation of the Interaction between IT andNon-IT Resources. Decision Sciences, Vol. 39 No. 4, pp.703-735.

[5] Ordanini, A. and Rubera, G., 2008. Strategic Capabilities and Internet Resources in Procurement: A Resource-Based View of B-to-B Buying. International Journal of Operations & Production Management, Vol. 28 No. 1, pp. 27-52.

[6] S. R. Croom, "The impact of e-business on supply chain management: an empirical study of key developments," International Journal of Operations & Production Management, vol. 25, pp. 55-73, 2005.

[7] Evangelista, P. & Kilpala, H. 2007, "The perception on ICT use among small logistics service providers: a comparison between Northern and Southern Europe", 2007.

[8] Murphy, P.R. & Daley, J.M. 1999, "EDI benefits and barriers: Comparing international freight forwarders and their customers", International Journal of Physical Distribution & Logistics Management, vol. 29, no. 3, pp. 207-217.

[9] CHRIS SKINNER. Blockchain is Fintech's real gamechanger[J].Americanbanker，2016（55）：1.

[10]Korpela K, Hallikas J, Dahlberg T. Digital supply chain transformation toward blockchain integration[C]//proceedings of the 50th Hawaii international conference on system sciences. 2017.

[11] Abeyratne S A, Monfared R P. Blockchain ready manufacturing supply chain using distributed ledger[J]. 2016.

[12]Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management[C]//Open and Big Data (OBD), International Conference on.
IEEE, 2016: 25-30.

[13]Liu P T S. Medical record system using blockchain, big data and tokenization[C]//International Conference on Information and Communications Security. Springer, Cham, 2016: 254-261.

[14] Rouibah K, Ould-Ali S. Dynamic data sharing and security in a collaborative product definition management system[J]. Robotics and Computer-Integrated Manufacturing, 2007, 23(2):217-233.

[15]ZYSKIND G, NAYHAN O, PENTLAND A ’. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]//IEEE Security and Privacy Workshops. IEEE, 2015:180184.

[16] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// Security and Privacy. IEEE, 2016:839-858.

[17] ZHANG Ning, ZHONG Shan. Personal privacy protection mechanism based on blockchain[J]. Journal of Computer Applications, 2017, 37(10): 2787-2793.

[18]Aitzhan N Z, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840-852.

[19] Wang Jiye,Gao Lingchao,Dong Aiqiang et al. Research on Data Security Sharing Network System Based on Blockchain[J].Journal of Computer Research and Development,2017,54(4):742-749.DOI:10.7544/issn1000-1239.2017.20160991.