Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 705 - 712

Research on Decentralized Trusted Data Sharing Technology Based on Blockchain

Jeffrey S. IngosanDionisio R. TandinganJr
University of Cordilleras University of Cordilleras
Gov. Pack Road, Baguio City, PhilippinesGov. Pack Road, Baguio City, Philippines
jsingosan@uc-bcf.edu.ph drtandingan@uc-bcf.edu.ph

Zhu. YuliangJamil Krystyan Beset
Universityof CordillerasUniversity ofCordilleras
Gov. Pack Road,BaguioCity,PhilippinesGov. Pack Road, Baguio City,Philippines
zhuyluc@gmail.com jklbeset@gmail.com

Abstract--In the current information age, having more data means having more information. However, the complete sharing of data will increase the possibility of criminals using relevant data to commit crimes. With the development of cloud computing technology, data sharing can be realized based on the cloud, and the shared data can be stored in the data center. However, this will not ensure the security and privacy of the shared data, and there are security risks such as tampering and counterfeiting of the shared data. The decentralization of the blockchain and the non-tamperable characteristics of the data on the block can safely save data-sharing records without the need for a trusted third party. The paper will discuss the decentralized trusted data sharing technology based on blockchain to enhance the credibility of data sharing.

This paper will use the characteristics of the decentralized trust management of the blockchain to study the decentralized solution of trusted data sharing. Aiming at the storage problem of shared data, the block structure of shared data oriented to the blockchain is proposed, and the design is based on the blockchain, and the information of the shared data is stored in the blockchain; in response to the data access request and service problem in data sharing, a block chain-based, decentralized data sharing mechanism is proposed; usingsmart contracts can adopt data variables as parameters to transfer and store the characteristics.Design a decentralized, trusted data sharing smart contract, form a blockchain-based data sharing prototype system, and finally simulate the real on the Ethereum open source platformScenes.

The data sharing system based on blockchain was simulated and run on the Ethereum blockchain platform, and the data sharing function test was carried out. Experiments have shown that the blockchain-based data sharing technology solution in a decentralized application environment and distributed storage of data to protect data security, to a certain extent, enhance the credibility of data sharing.

Keywords: data sharing, decentralization, blockchain, smart contract

Ⅰ. INTRODUTIONANDBACKGROUND

Data collection has developed from manual operation to record data to automatic data collection, suchasphotoshooting,radiotelemetry,etc.[1].Withtheinnovationanddevelopmentofelectronic technology (miniaturization, battery and transmission technology, satellite navigation, etc.), a large number of digital tracking devices (such as GPS collars and implantable data sensors) have emerged [2]. These devices can be used to collect data. Reducing the error of the data can also prevent the possibility of falsifying data during collection. The sharp drop in the error rate of data collection significantly reduces the possibility of falsifying data. The powerful computing and storage capabilities of the cloud [3] can store or share data, but a large amount of information interaction and highly concentrated computing resources make the cloud face severe security challenges [4], for example, cloud systems may be exposed to malicious users or cloud-provided Business attack.

How to improve the security of data storage and enhance the credibility of data sharing in the process of sharing data has become a new core issue. Research has found that it is uneconomical to query data in a centralized manner [5], not only to solve the problems of huge data and distributed management, but also to solve the problems of data security and privacy [6] [7]. When data is shared, more and more data occur on the web server site related to the owner, that is, between the data owner and the visitor. Both parties have become the smallest scope for datasharing.

Reliable data sharing means that the participating parties can access the data that they are authorized to access each other, and it is also the behavior that can prevent the participating parties or attackers from tampering with the data. The data owner has the right to view the access records, who can view what content is at what time. The data owner can specify that a certain part of the data content can be viewed, or the relevant data can only be viewed with the consent of the data owner. The identities of the two parties sharing the data must be authentic, and also be prevented from being known by any party to avoid attacks by attackers.

Blockchain technology can effectively solve the problem of untrustworthiness between the two parties during data sharing. Blockchain technology can securely record transactions between two parties without the need for a trusted third party. Blockchain technology also provides a way to use a variable public key as an identity to protect privacy. Blockchain technology can efficiently solve the privacy and security issues of data sharing. As a result, blockchain technology has become a focus of decentralization of shared data and enhancement of shared data security [8] and privacy.

Ⅱ. RELATED WORK

In the field of the Internet of Things, the blockchain-based Internet of Things data sharing model [9] sets up a new type of gateway to solve the problem of large heterogeneity in the interfaces of different devices, thereby solving the increasingly complex problems of the Internet of Things structure, effectively the threat of artificial tampering and deletion of data in IoT devices is prevented or combined devices with higher computing power to create apair

Waiting for the network [10], the verification of new blocks no longer uses the proof-of-work mechanism, and the data can be queried by signing the transaction with the verification code, thereby reducing the time for querying the data. The combination of blockchain technology and P2P storage system has promoted the development of privately designed Internet of Things [11]. Sensitive data generated and exchanged between device nodes in the network is stored in this storage system. Its P2P nature can ensure privacy that is robustness and prevention of single point of failure.

In the medical field, the blockchain-based medical data sharing model [12] solves the difficulty of verifying, saving, and synchronizing medical data by improving the Delegated Proof of Stake (DPOS), avoiding spending a lot of resources and time for permissions and dataverification.

Alternatively, using the proxy re-encryption mechanism in cryptography to achieve access control and sharing of medical data [13]. Blockchain technology provides a useful mechanism to support post-incident auditing and accountability [14], which will further improve the effectiveness of medical institutions. The sharing of electronic medical data between the two is of great significance to the accurate treatment of patients, disease tracking, and data analysis. At the same time, it protects patients' privacy and improvessafety.

In addition, the combination of the Internet and cryptographic technology enables data sharing in cloud computing to open up a new useful field for computer networks. The conference key agreement protocol based on Symmetrical Balanced Incomplete Block Design (SBIBD) greatly improves the security and efficiency of data sharing in cloud computing[15].

Ⅲ. METHODLOGY

1. Overall systemdesign

The cloud-based data sharing system is based on a third-party network server for data storage and sharing. This paper removes the third-party network server and uses blockchain as the core. The design is based on blockchain, decentralization, and trusted data sharing. The function implementation architecture. The overall design architecture involves four parts: local data storage equipment, blockchain network built by blockchain nodes, smart contracts, and the front end of the application. The overall design is shown in Figure 3.1 below. Each part is described in detail below.

(1) Localdatabase

From bottom to top, this layer is responsible for the storage of shared data. The shared data of the data owner is stored locally. During the sharing process, no one except the data owner has the ownership of the shared data. The shared data in the local database is not in the blockchain network, but after data processing through metadata, the authenticity data identifier is finally stored in the blockchain, and this identifier is transmitted on the network.

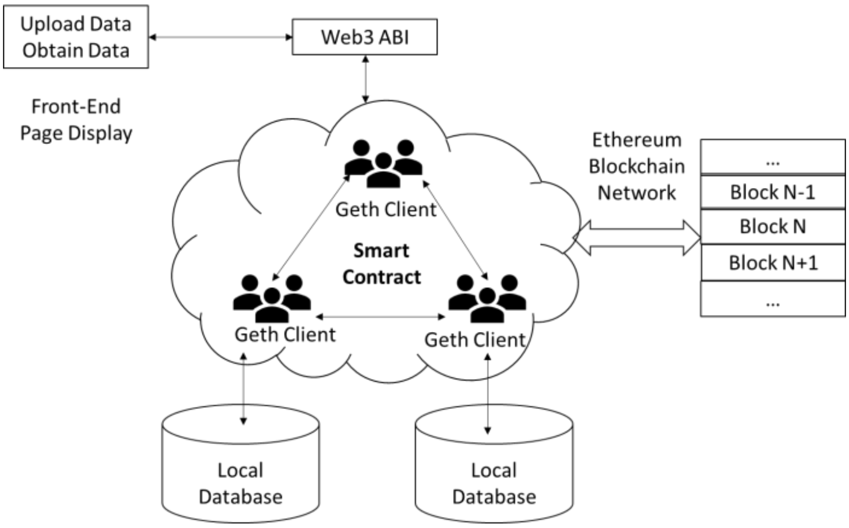


Figure 3.1 Overall design architecture

(2) Smartcontract

This layer is based on the business logic required by the blockchain-based data sharing solution and uses a suitable programming language to flexibly write smart contract scripts for shared data storage and shared data requests and services. This smart contract script is strictly implemented by all nodes in the network.

(3) Blockchain

This layer is the core part. Nodes participate in the blockchain network through the geth client, responsible for the generation of blocks and maintaining the operation of the blockchain. The storage of shared data is completed before the data is shared. In addition, the service of shared data request and response is also provided. Each node on the blockchain can have two roles at the same time, namely, the data owner and the data requester.

(4) Front-end page displaypart

This layer allows each participant to implement shared data storage and shared data requests and services based on the front-end page, and finally complete the data sharing interaction, provided that the blockchain network is running normally and the contract is successfully deployed.

2.Functional design of the system

According to the application requirements of data sharing based on blockchain, the decentralized data sharing system based on blockchain mainly involves five functions: local data storage function, shared data storage function, shared data retrieval function, block Consensus function, data sharing request and service function. The detailed function module design is shown in Figure 3.2 below.

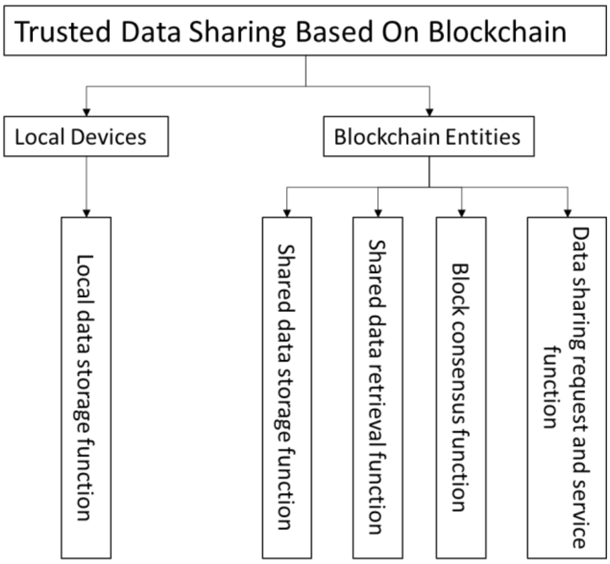

Trusted Data Sharing Based On Blockchain
Local Devices
Blockchain Entities
Local data storage function
Shared data storage function
Shared data retrieval function
Block consensus function
Data sharing request and service function

Figure 3.2 Design and implementation of system functions

Among them, the storage function of shared data, the retrieval function of shared data, and the request and service function of data sharing are the three main functions. In the implementation diagram of the system function design, the local data storage function refers to storing the original data of the shared data locally. The data can be any type of data, but the premise is that it can be processed with metadata. In order to facilitate the subsequent experiments, different types of data are selected for local storage, or the data from the local server can be used directly.

3. System functionrealization

Based on the data sharing interaction model, this article mainly uses the Ethereum blockchain as the blockchain deployed by the smart contract. Each function is also realized through the smart contract.Thethreefunctionsofdatasharingbasedontheblockchainaremainlyrealized.Theyare: :

Shared data storage function, shared data retrieval function, and shared data request and service function. The functional structure of the solution is shown in Figure 3.3.

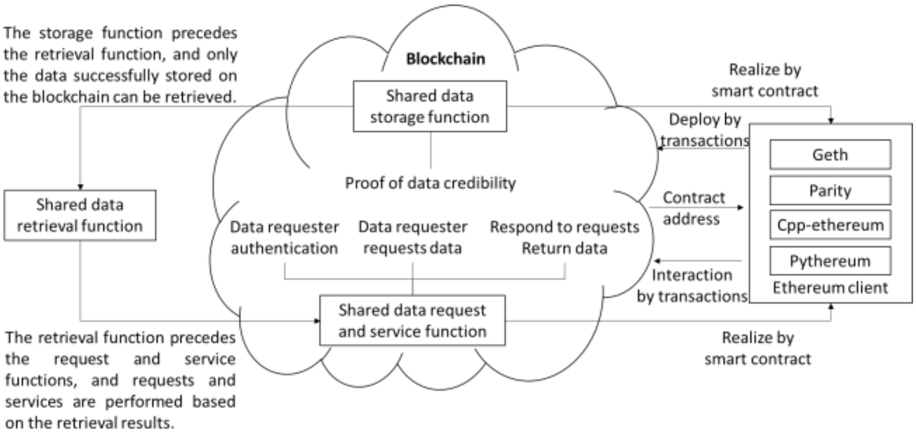

The storage function precedes the retrieval function, and only the data successfully stored on the blockchain can be retrieved.
Blockchain
Shared data storage function
Realize by smart contract
Deploy by transactions
Geth
Parity
Cpp-ethereum
Pythereum
Ethereum client
Shared data retrieval function
Proof of data credibility
Contract address
Data requester authentication
Data requester requests data
Respond to requests Return data
Interaction by transactions
Shared data request and service function
Realize by smart contract
The retrieval function precedes the request and service functions, and requests and services are performed based on the retrieval results.

Figure 3.3 Realization function structure diagram

First, start an Ethereum node Geth, and use the Solidity programming language to write smart contract files with .sol of the suffix. Compile the smart contract file, convert the smart contract into bytecode recognized by the Ethereum virtual machine, and obtain the binary interface ABI for the interaction between the account and the smart contract. When creating a contract, the account will use bytecode as the transaction parameter and broadcast it to the entire network for verification. After valid verification, the contract is created successfully, and the transaction is recorded on the blockchain. When the contract is called, the execution of the smart contract also exists in the form of a transaction. The account obtains the running result of the contract through the ABI interface, and records this process as a transaction and stores it in the blockchain. Whether it is to compile or deploy a smart contract, it needs to consume a certain amount of fuel, and the initiator of the contract is required to sign the contract with its own private key. After the proof of work is verified, the contract code is successfully stored on the Ethereum blockchain. Up. The information contained in the smart contract for data sharing is shown in Figure3.4

DataSharing

+ struct Data {
bytes name;
bytes hash;
bytes dsign;
uint256 timestamp;
address owner;
}

+ store(bytes32 name, bytes hash, uint256 timestamp, bytes dsign) public returns(bytes) + query(address owner) public return (bytes32, bytes32, uint256, address, bytes)

Figure 3.4 Smart contract for data sharing

The above smart contract contains the following properties and functions.

name, a keyword selected from the shared data stored locally and stored on the blockchain.

hash, the hash value of the shared data link entry.

dsign, a digital signature based on decentralized timestamp.

timestamp, the local time when the data is stored on the blockchain, that is, the timestamp.

owner, the public key address of the data owner.

The store() function performs the storage function of shared data. Every time the storage of shared data updates the global state of the smart contract, it is regarded as a transaction.

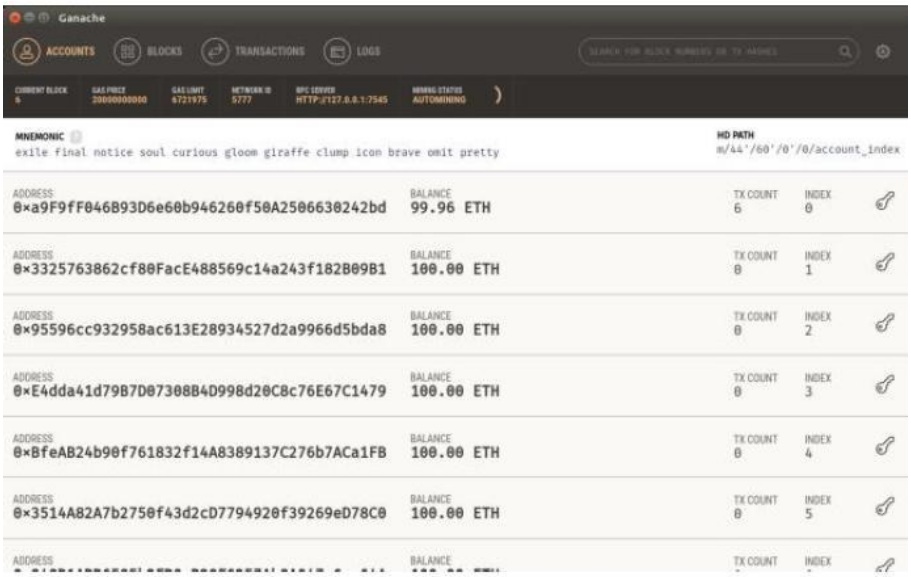
The query() function executes the request and service functions of shared data, makes a specific data access request to the blockchain network, and responds according to the identity of the visitor. This function will also update the global state of the smart contract and execute the transaction.

Ⅳ. FINDINGSAND DISCUSSION

According to the application requirements of the blockchain-based decentralized trusted data sharing program, the test program for the authenticity of the shared data and the trusted data sharing interaction was determined, and specific test cases were designed. The selected test environment is consistent with the hard and soft environment of experimental development. Record the results of the experiment in time, judge whether it meets the expected results and analyze them, and finally draw a conclusion.

1. Test results and analysis of shared data storage

According to the test methods and test cases in the test plan, the shared data storage function is tested first. Figure 4.1 is the running interface of ganache. The 10 users automatically assigned by the system are displayed in the interface. Each user has the following information: ADDRESS refers to the account address, BALANCE refers to the remaining amount currently owned by the user, and TXCOUNT refers to the number of transactions. In addition, you can also view the log output of the Ganache internal blockchain through the LOGS field, including In response to other important debugging information, check all blocks and transactions to obtain information about related issues.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
6	20000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

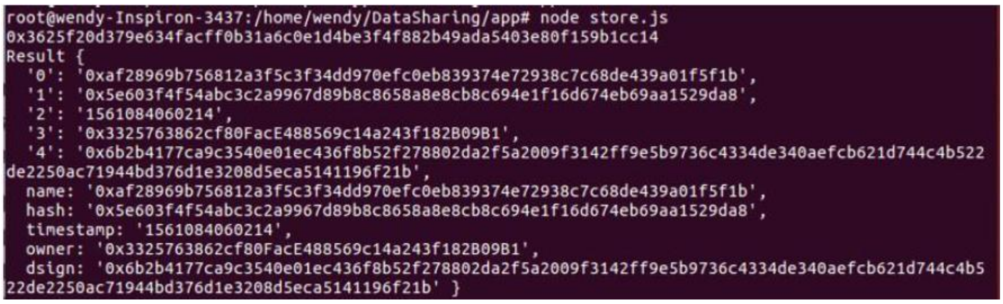
MNEMONIC
exile final notice soul curious gloom giraffe clump icon brave omit pretty

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×a9F9fF046B93D6e60b946260f50A2506630242bd	99.96 ETH	6	0
0×3325763862cf80FacE488569c14a243f182B09B1	100.00 ETH	0	1
0×95596cc932958ac613E28934527d2a9966d5bda8	100.00 ETH	0	2
0×E4dda41d79B7D07308B4D998d20C8c76E67C1479	100.00 ETH	0	3
0×BfeAB24b90f761832f14A8389137C276b7ACa1FB	100.00 ETH	0	4
0×3514A82A7b2750f43d2cD7794920f39269eD78C0	100.00 ETH	0	5
[illegible]	[illegible]	[illegible]	[illegible]

Figure 4.1 The running interface of ganache

After completing a series of preparations, run the store storage script file to store the hash value, timestamp, digital signature, and data owner address in the blockchain to form a transaction record. The running result is shown in Figure 4.2.



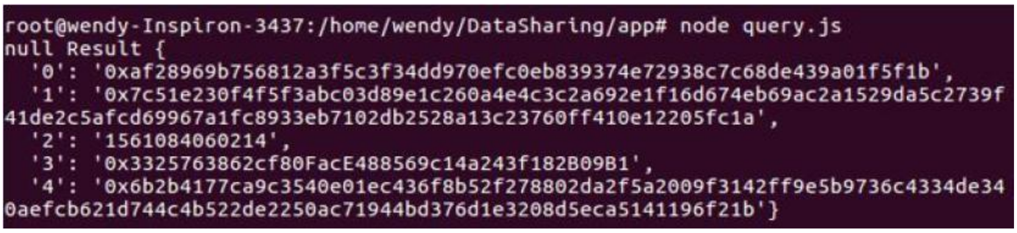
```
root@wendy-Inspiron-3437:/home/wendy/DataSharing/app# node store.js
0x3625f20d379e634facff0b31a6c0e1d4be3f4f882b49ada5403e80f159b1cc14
Result {
  '0': '0xaf28969b756812a3f5c3f34dd970efc0eb839374e72938c7c68de439a01f5f1b',
  '1': '0x5e603f4f54abc3c2a9967d89b8c8658a8e8cb8c694e1f16d674eb69aa1529da8',
  '2': '1561084060214',
  '3': '0x3325763862cf80FacE488569c14a243f182B09B1',
  '4': '0x6b2b4177ca9c3540e01ec436f8b52f278802da2f5a2009f3142ff9e5b9736c4334de340aefcb621d744c4b522
de2250ac71944bd376d1e3208d5eca5141196f21b',
  name: '0xaf28969b756812a3f5c3f34dd970efc0eb839374e72938c7c68de439a01f5f1b',
  hash: '0x5e603f4f54abc3c2a9967d89b8c8658a8e8cb8c694e1f16d674eb69aa1529da8',
  timestamp: '1561084060214',
  owner: '0x3325763862cf80FacE488569c14a243f182B09B1',
  dsign: '0x6b2b4177ca9c3540e01ec436f8b52f278802da2f5a2009f3142ff9e5b9736c4334de340aefcb621d744c4b5
22de2250ac71944bd376d1e3208d5eca5141196f21b' }
```

Figure 4.2 Experimental results of shared data storage

2.Test results and analysis of shared data access requests and services

In the access request, the data owner must first verify the identity of the visitor, that is, check whether the visitor is authorized in the AuthoroList. If it is authorized, return the corresponding shared data information stored in the block, where the link entry of the complete data is used to access the public key of the person is output after being encrypted by an asymmetric encryption algorithm. When visitors get information about the block, they use theirown

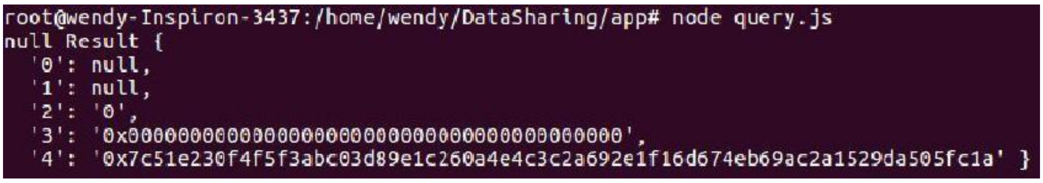
The private key to decrypt the encrypted complete data link entry. Otherwise, it must be authorized first, and then authorized through the verification and approval of the nodes of the entire network. The implemented smart contract contains a query request function. The successful completion of data sharing is shown in Figure 4.3below.



```
root@wendy-Inspiron-3437:/home/wendy/DataSharing/app# node query.js
null Result {
  '0': '0xaf28969b756812a3f5c3f34dd970efc0eb839374e72938c7c68de439a01f5f1b',
  '1': '0x7c51e230f4f5f3abc03d89e1c260a4e4c3c2a692e1f16d674eb69ac2a1529da5c2739f
41de2c5afcd69967a1fc8933eb7102db2528a13c23760ff410e12205fc1a',
  '2': '1561084060214',
  '3': '0x3325763862cf80FacE488569c14a243f182B09B1',
  '4': '0x6b2b4177ca9c3540e01ec436f8b52f278802da2f5a2009f3142ff9e5b9736c4334de34
0aefcb621d744c4b522de2250ac71944bd376d1e3208d5eca5141196f21b'}
```

Figure 4.3 Experimental results in the request phase

It can be seen from the above experiment that the link entry of the shared data is no longer the original value, and its byte length is the same as the length of the public key address. This is because the link entry data of the shared data is encrypted with the visitor's public key and formed. In the case of authorization, the requesting party's data request message can obtain the shared data information stored in the block, and it is also confirmed that the blockchain technology can be applied to data sharing, so as to achieve the purpose ofdecentralization.



```
root@wendy-Inspiron-3437:/home/wendy/DataSharing/app# node query.js
null Result {
  '0': null,
  '1': null,
  '2': '0',
  '3': '0x0000000000000000000000000000000000000000',
  '4': '0x7c51e230f4f5f3abc03d89e1c260a4e4c3c2a692e1f16d674eb69ac2a1529da505fc1a' }
```

Figure 4.4 Experimental results after data tampering

Modify the data in the local database, and any other script data will not change, and the obtained experimental results can still successfully obtain the shared data information. Changing the key words of the data stored in the script or the entry information of the complete data will get the experimental results in Figure 5.7. This is because the data stored on the blockchain has not changed at all, even if the local database is changed multiple times, it will not affect Successfully obtain the shared data entry, but once the data keyword in the script or the link entry of the shared data is changed,thevisitordatarequestwillfail.Atthistime,thedataownerneedstoperformthesharedstorage function again, otherwise the data cannot be shared. This experimental comparison strongly confirms that blockchain-based data sharing can achieve credible data sharing and prevent data from being tampered with by others.

V.REFERENCES

[1] Valentina Gattesch, Fabrizio Lamberti ,ClaudioDemartini ,Chiara Pranteda ,Víctor Santamaría. ToBlockchain or Not to Blockchain: That Is the Question[C]//IT PROFESSIONAL. IEEE.2018:62-74.

[2] Remo Manuel Frey, Thomas Hardjono, Christian Smith, Keeley Erhardt, Alex 'Sandy' Pentland. SecureSharing of Geospatial Wildlife Data[C]//In Proceedings of the Fourth International ACM Workshop onManaging and Mining Enriched Geo-Spatial Data,Chicago, Illinois. ACM. May14,2017:1-6.

[3] Ravi Kiran Raman ; Lav R. Varshney. Dynamic Distributed Storage for Blockchains[C]//In 2018 IEEEInternational Symposium on Information Theory (ISIT). Vail, CO, USA. IEEE.2018:2619-2623.

[4] Yan Guixu, Liu Bei, Cheng Hao, et al. Research on Data Sharing Security Framework[J]. Information Security Research, 2019,4:309-317.

[5] Wu Zhaoli. Key technologies of shared data centers in colleges and universities[J]. Electronic Technology and Software Engineering,2018,145(23):168-168.

[6] Bin Li, Yijie Wang, Peichang Shi, Huan Chen, Li Cheng. FPPB: A Fast and Privacy-Preserving MethodBased on the Permissioned Blockchain for Fair Transactions in Sharing Economy[C]//In 2018 17th IEEEInternational Conference On Trust, Security And Privacy In Computing And Communications/12th IEEEInternational Conference On Big Data Science And Engineering (TrustCom/BigDataSE). New York, NY,USA. IEEE.2018:1368-1373.

[7] Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han, Paul Sarda.Blockchain as a Notarization Service for Data Sharing with Personal Data Store[C]// In 2018 17th IEEEInternational Conference On Trust, Security And Privacy In Computing And Communications/12th IEEEInternational Conference On Big Data Science And Engineering (TrustCom/BigDataSE). New York, NY,USA. IEEE.2018:1330-1335.

[8] Li Shanqing, Zheng Yanning, Xing Xiaozhao, et al. Research on the safety management of scientific data sharing[J]. China Science and Technology Resources Guide. 2019,3:11-17.

[9] Yu Jingang, Zhang Hong, Li Shu, etc. Blockchain-based IoT data sharing model [J]. Small microcomputer system, 2019(11): 2324-2329.

[10] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. Towards an Optimized BlockChain for IoT[C]//In Proceedings of The 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA. IEEE. 18-21 April 2017:173-178.

[11] Marco Conoscenti , Antonio Vetro , Juan Carlos De Martin. Blockchain for the Internet of Things: aSystematic Literature Review[D]//2016 IEEE/ACS 13th International Conference of Computer Systems andApplications (AICCSA),Agadir, Morocco. IEEE.2016:1-6.

[12] Xue Tengfei, Fu Qunchao, Wang Cong, et al. Research on medical data sharing model based on blockchain[J]. Acta AutomaticaSinica, 2017(09): 73-80.

[13] Zhou Hui, Wang Lidan, Zhong Chengyue. Blockchain helps electronic medical data sharing[J]. Journal of PLA Hospital Management,2019(7).

[14] Yan Ying, Zheng Kai, Guo Zhongxin. Ethereum technology detailed explanation and actual combat [M]. Beijing: Machinery Industry Press,2018.

[15] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, Yang Xiang. Block Design-based KeyAgreement for Group Data Sharing in Cloud Computing[C]//Transactions on Dependable and SecureComputing.IEEE.2017.