Automation, Control and Intelligent Systems
2022; 10(1): 8-13
http://www.sciencepublishinggroup.com/j/acis
doi: 10.11648/j.acis.20221001.12
ISSN: 2328-5583 (Print); ISSN: 2328-5591 (Online)

Research on Data Sharing Access Control Based on Blockchain Technology

Zhang Zichen, Yan Changshun*

Faculty of Information Technology, Beijing University of Technology, Beijing, China

Email address:
zzc365021002@163.com (Zhang Zichen), yuewuxing@bjut.edu.cn (Yan Changshun)
*Corresponding author

To cite this article:
Zhang Zichen, Yan Changshun. Research on Data Sharing Access Control Based on Blockchain Technology. *Automation, Control and Intelligent Systems*. Vol. 10, No. 1, 2022, pp. 8-13. doi: 10.11648/j.acis.20221001.12

Received: March 19, 2022; **Accepted**: April 11, 2022; **Published**: April 20, 2022

Abstract: Blockchain is now widely used in various industries due to its openness, transparency, autonomy, imtamability, decentralization, and traceability. With the wide application of blockchain technology, its security problems have also brought significant challenges, seriously affecting the implementation of blockchain applications. Data on the traditional blockchain is open to the entire network node. The update operation of data records is also transparent, accompanied by the leakage of user information. Although blockchain has the characteristics of anonymity and privacy, with its development, it has not been easy to meet users' needs. How to effectively protect user data privacy, realize data sharing on the blockchain, and ensure the security of data integrity, transmission efficiency, storage efficiency, and application is very important to break through the bottleneck of the development of blockchain technology and promote its application. This paper proposes a traffic data resource access control scheme based on blockchain technology by combining the attribute encryption access control system based on ciphertext strategy based on blockchain's distributed ledger technology and the openness and imtamability it brings. In this scheme, the task of attribute encryption is to ensure the security involved in the process of plaintext and ciphertext conversion and the efficiency of data sharing, and to implement a one-to-many access sharing policy, to enhance the safety of the access sharing system and improve the efficiency of the access control module. This paper introduces the access control mechanism from two aspects of system architecture and the access sharing process. Then the attribute encryption mechanism is designed. The design process includes symbol description, primary structure, algorithm design idea and algorithm construction. Finally, the functionality and security of the access control mechanism are analysed.

Keywords: Blockchain, Cryptography, Access Control

1. Introduction

In the era of big data, data resource sharing has become an essential part of people's lives and a necessary part of smart cities. People should pay critical attention to sharing efficiency and privacy protection. Since the emergence of cloud computing, secure data sharing in distributed environments has always been a hot and challenging topic. Users and cloud providers often belong to different management or security domains. The difficulty of cloud-based data sharing lies in how many trusted users can be deployed on the cloud provider side. A blockchain is a distributed database ledger in which the data stored on the blockchain cannot be changed. Since the birth of blockchain in 2008, blockchain technology and architecture have developed rapidly and are now widely used in many fields. With the development of technology, as the transaction information on the blockchain is open to the nodes joining the blockchain system, data privacy, key protection, cryptographic algorithm security, and many other aspects of blockchain are facing challenges. Based on blockchain's distributed ledger technology and its openness and imtamability, this paper proposes a traffic data resource access control scheme based on blockchain technology by combining the attribute encryption access control system based on ciphertext strategy. In this scheme, the task of attribute encryption is to ensure the security involved in the process of plaintext and ciphertext conversion and the efficiency of data sharing, and to implement a one-to-many access sharing

policy, to enhance the safety of the access sharing system and improve the efficiency of the access control module [1-4]. According to the decentralized characteristics of the blockchain system, the communication between the data-sharing visitors and data owners can be completed safely and smoothly without the participation of a third party [5-7]. At the same time, the hybrid consensus mechanism can be used as conditional judgment to realize access requests [8, 9].

2. Access Control Mechanism

This section focuses on two modules, including the system architecture and flow of traffic data resource access control mechanism based on blockchain technology.

2.1. System Architecture

This paper will design the access control system from the following four modules: access requester, information owner, alliance node group, and blockchain network. The essential functions of the four modules are designed in detail as follows:

(1) Access requester: the user applying for access to a shared data resource. This node can be any user node in the system. The access requester can obtain access permission by using the current representative node of the information owner.

(2) Information owner: it is mainly responsible for three tasks: the first is to encrypt the original information in the system; the second is to pre-set the access and to share the structure of the data; the third is to initiate the chain request to the server group of the transportation union, to store the ciphertext. If the request visitor wants to obtain the key to parse the ciphertext, the condition of sharing access structure permission must be met. Only when the state is completed can the key be used to decrypt the ciphertext and obtain the original data transmitted by the information owner, that is, plaintext information.

(3) Union group of nodes: its function is mainly responsible for the information shared by the owner store and broadcast, encrypted file implementation chain, and transaction, and the ability to encryption ciphertext based on the structure of the information owner Shared access to access the requester's attributes in judgment, then to access the requester sends ciphertext, the ciphertext is based on the requester with public key encryption and information access structure of the owner.

(4) Blockchain network: receive the attribute encrypted ciphertext with access structure broadcast by the server node of the union.

The traffic data resource access control architecture based on blockchain has five main parts, including the access requester, the information owner, the alliance nodes, the blockchain network and the blockchain chain storage structure. The so-called information owner can also be regarded as the owner of data resources. It encrypts data on the client-side and can customise access policies, thus realising fine-grained access control. The access control mechanism based on CP-ABE (Ciphertext policy attribute-based Encryption) and proxy re-encryption technology combine to enable users to achieve one-to-many or one-to-one access to the share, which improves the flexibility of access control. Users can obtain encrypted files only after obtaining the permissions specified by the information owner through the personalised access control policy to access shared data. This improves access control security.

2.2. Share Access Process

The process of access sharing mainly consists of six stages: access request initiation, file encryption, consensus completion, transaction verification, file upload, decryption and download.

(1) Access request initiation: Through the blockchain network, the access requester initiates access to the information data of the information owner.

(2) File encryption: When information owner B receives the user access request, it will be encrypted in advance of the access control of clear structure and information access control. At this point, the information owner B can choose the way of encryption; there are two ways, one is based on the attribute of the one-to-many encryption ciphertext, the other is for the user of A property broker heavy encryption ciphertext, after completing the process, The encrypted ciphertext is finally sent to the federation server.

(3) Consensus completion: After receiving the ciphertext of B, the union node group will further judge it to determine whether the ciphertext belongs to a one-to-one or one-to-many encryption ciphertext. Suppose the ciphertext is a one-to-one property proxy ciphertext. In that case, the accounting nodes generated by the transportation organisation federation server farm need to perform proxy encryption on the ciphertext and then broadcast the proxy ciphertext after a consensus is formed. If the ciphertext is a one-to-many attribute encryption ciphertext, the billing node broadcasts the ciphertext after a consensus is reached.

(4) Transaction verification: Alliance nodes verify transactions and data integrity.

(5) File upload: After verification, the proxy re-encrypts the ciphertext and stores it on the billing node.

(6) File decryption and download: When the blockchain network receives the broadcast transaction, the blockchain network will send feedback to the blockchain node to remind the user of the access request node. User A can access the ciphertext on the chain.

3. Attribute Encryption Mechanism

Nowadays, many fields have widely used an information-sharing system based on blockchain technology. To better realize fine-grained access to blockchain data, improve the security required in the access process, and solve the problems of privacy protection and data retrieval problems

in the traditional blockchain data sharing system, This paper designs an access control scheme of searchable proxy re-encryption based on attributes. This section will introduce the symbol description, primary structure, algorithm design, ideas and contract design of the attribute encryption access control mechanism based on the blockchain.

3.1. Symbolic Description

This scheme adopts the access control mechanism based on attributes, combines searchable encryption and proxy re-encryption, and realizes users' functions of data sharing, tracking and fast retrieval. The blockchain sharing scheme with searchable agent re-encryption can effectively solve data privacy leakage and quick query of traditional blockchain, and specifically adapt to the information resource sharing with a large amount of data and frequent interaction. Proxy re-encryption can implement the data owner and multiple data encryption technologies, the data sharing between the second through the searchable symmetric encryption to construct the inverted index structure, perform a binary search algorithm can use the keyword search keyword quick query token of the data, to improve the efficiency of data users access but also protect the plaintext data privacy [10-12]. All variable symbols designed in this scheme are shown in Table 1.

Table 1. *Symbolic description of access control mechanism.*

Symbol	Description
GP, PK, MSK	System public parameter, System public key, System master key
U, Sx	System total property set, User x property set
m, k	Original information plaintext, System security parameters
PKx, SKx	The public key of user x, The secret key of user x
(Mx, ρx)	Access shared architecture
CT	Metadata ciphertext
CTA, CTB	Original message ciphertext, Agent re-encrypt ciphertext
rkA->B	The agent re-encrypts key

3.2. Basic Structure

The primary participating entity is: the data owner，data users, external databases, and miners.

Data Owner: The data owner encrypts the data using the proxy re-encryption technology, extracts the keywords {w1, w2..., w3}, and generates a keyword index. Finally, the data owner forms the transaction and broadcasts it to the blockchain network. The union cluster nodes in the network verify that the transaction is correct and then add it to the block.

Data users: Data users in this model are all users who apply for access and use of information resources. The user has their own key, and when the user requests access to the data, they first initiate a transaction (Token with an additional search Token) to the blockchain. After the verification node verifies the Search Token and index match successfully, it sends the location of the file and the key re-encrypted by the agent to the user, who then requests the data ciphertext from the external database.

External database: Stores encrypted raw data.

Miners: Miners in this model refer to the union cluster nodes, which verify the transaction, verify whether the index matches the Search Token, and send the storage location of data and the key re-encrypted by the agent to the user after meeting the conditions.

3.3. Algorithm Design Idea

In traditional blockchain technology, the global ledger that stores transaction information is open to any node that joins the blockchain system. Blockchain data privacy needs to strengthen further and perfect searchable encryption and proxy heavy encryption technology based on search agent under rich encrypted blockchain data privacy protection scheme, can reduce the storage load block chain, realize data sharing, one-to-many data privacy protection at the same time, improve the efficiency of search, These will be of great help to improve the quality of information resource sharing model with large data volume, frequent transactions and many information islands [13].

The searchable proxy re-encryption blockchain data sharing scheme based on attribute encryption uses the proxy re-encryption algorithm to encrypt the original data [14-16]. Only the data querier with the proxy re-encryption key can transform the data and then decrypt the plaintext data. This method protects the user's data privacy. The sharing scheme also adopts the keyword inverted index structure [17, 18]. The miner node can quickly query the storage location of ciphertext data by executing a binary search algorithm to locate the corresponding keyword index item. In the process of designing the algorithm, the ideas and techniques involved are as follows:

3.3.1. Attribute Encryption Based on Ciphertext Policy

The basic algorithm usually consists of the following four steps:

a. System initialization: select a security parameter λ to generate the public key PK (public key) and master key MK (master key) required by the system.
b. Cipher Text is generated with access policy A, public key PK and data to be encrypted as input.
c. Key generation: input Mk and a set of attributes to generate a private key SK (Secret Key).
d. Decryption: After obtaining the ciphertext, the user whose attribute set meets the access structure can decrypt the ciphertext.

3.3.2. Ciphertext Search Based on Searchable Encryption

Symmetric searchable encryption requires symmetric key interaction between data owners and consumers, but the computing performance is more efficient. The general symmetric searchable encryption algorithm includes the following four steps:

a. $(\mathrm{MK}, \mathrm{pp}) = \mathrm{KeyGen}(\lambda)$: Input security parameters, and form key Mk according to the security parameters.
b. $\mathrm{I_w} = \mathrm{Enc}(\mathrm{MK}, \mathrm{w}, \mathrm{pp})$: Using the generated key Mk and keyword w, generate keyword ciphertext index Iw.
c. $\mathrm{TK} = \mathrm{TokenGen}(\mathrm{MK}, \mathrm{w}, \mathrm{pp})$: Using the generated key MK and keyword w, generate the search token TK.
d. $\mathrm{B} = \mathrm{Test}(\mathrm{MK}, \mathrm{I_w}, \mathrm{pp}, \mathrm{TK})$: Match index and search token, return search result {0,1} if successful.

Public key searchable encryption is the earliest public-key searchable encryption mechanism that does not require key interaction. Which is described as follows:

a. Setup(λ): Input safety parameter λ and output global parameter PARAMS.
b. KeyGen(Params): Key generation algorithm, according to the global parameter Params, generates public key PK and private key SK.
c. PEKS(w, PL, I) : Data encryption and secure index generation algorithm, according to the extracted keyword W and using the receiver's public key PK to encrypt and index the data, and finally input the keyword ciphertext C and index I.
d. Trapdoor(w', SK) : Trapdoor (w',SK): Trapdoor generation algorithm. The query user meeting the conditions uses the keyword w' and the private key SK to generate the Trapdoor TW that cannot disclose the search keyword.
e. Test(PK, C, T_w, I): Search algorithm, which will match the keyword trap gate TW submitted by the data querier with the index I constructed by the data owner, input the public key PK and ciphertext C of the data querier, and compare the keyword W in the ciphertext with the keyword W 'in the search token. If the same output 1, otherwise, output 0.

3.3.3. Proxy Re-encryption

Proxy-re-encryption is a key conversion mechanism between ciphertexts. In proxy re-encryption, a semi-trusted agent converts the ciphertext encrypted with Alice's public key PA to one encrypted with Delegatee Bob's public key PB using the conversion key Rk generated by the delegator. During this process, The agent can not get the plaintext information of the data, thus reducing the risk of data leakage.

In 2006, Green et al. proposed an improved proxy re-encryption scheme to protect distributed storage applications, which is described as follows:

a. Setup (λ): Input the safety parameter λ, and output the global parameter Params.
b. KeyGeneration(Params): Key generation algorithm, according to the global parameter Params, generate user A public key PKa=ga and private key SKa=a.
c. Re-Encryption Key Generation (RG): Re-encryption key generation, user A entrusts the key to B by issuing the re-encryption key rkA->B = gb/a.
d. First-LevelEncrypption (E1): In the first stage of encryption, the information m is encrypted with the public key PKa=ga, so that it can only be decrypted by the holder of SKa=a, and the output c=(Zak,mZk).
e. Second-LevelEncryption(E2): The second stage of encryption, m is encrypted with the public key PKa=ga, so that it can only be decrypted by the holder of SKa=a and its agent, and output c=(gak,mZk).
f. Re-Encryption(R): Re-encryption, anyone maliciously uses rkA->B=gb/a to change the second-level ciphertext of A to the first-level ciphertext of B. Starting from ca=(gak,mZk), calculate e(gak,gb/a)=Zbk, and then issue cb=(Zbk,mZk).
g. Decryption (D1, D2): Decrypt, decrypt the ciphertext ca=(α,β) and the key sk=a, calculate m=β/α1/a. Decrypt the second-level cipher text ca=(α,β) key sk=a, calculate β/e(a,g)1/a.

3.3.4. Inverted Index Structure

An inverted index structure is a data structure that stores content to map [21]. The purpose of this structure is to allow fast full-text searches. The inverted index structure is the most popular data structure used in document retrieval by large-scale search engines. Assume that there is a document D, set the document D={d1,d2... DN} is encrypted and stored in an external database. Each document di contains a set of keywords. Let w collection is the keyword in the document D collection, including |w| = n is the total number of keywords. Keyword and document sets are encrypted using different encryption algorithms ENC (Searchable Encryption Scheme) and E (Any Secure Encryption Scheme) and stored in an external database and on the blockchain, respectively. The keyword index set for the encrypted document is I. The corresponding data consumer can use a search token TK containing the document keyword. The miner node on the blockchain can conduct a binary search by calculating the inner product of the search token vector and the index vector to locate the matching index entries.

3.4. Algorithm Construction

In the scenario where the user A requests to access theinformation of a department B, the algorithm is constructed based on the re-encryption access control mechanism of searchable agents [22]. The specific plan includes the following 11 steps:

(1) Initialize:$(GP, PK, MSK) \leftarrow Setup(k, U)$

Given the security parameter k of the system and the set of all attributes U of the system, the public parameter GP, the public key PK of the system and the master key MSK of the system is generated.

(2) Key Generation: $((PK_A, SK_A), (PK_B, SK_B)) \leftarrow KeyGen(PK, MSK, S_A, S_B)$

Input the public key PK of the system, the master key MSK of the system, and the property sets of A and B,(SA, SB⊆U);output the public and private key pairs of A and B.

(3) Re-encryption Key Generation: $ReKey(SK_A, S_A), (M', p'), GP, PK_B) \leftrightarrow rk_{B\to A}$

Input B's private key SKB, attribute set SB, access sharing structure (M ',p '), system's public parameter GP and user A's public key PKA to generate the proxy re-encryption key.

(4) Cipher Encryption: $CT_B \leftarrow E(m, (M', p'), GP, PK_A)$

Enter the shared information plaintext, access sharing structure, system public parameter GP and proxy re-encryption key to generate the encrypted ciphertext. Also, extract the keywords of the shared information plaintext.

(5) Cipher Re-encryption:$CT_A \leftarrow RE(PK, GP, CT_B, rk_{B\to A})$

Enter the system public key PK, the system public parameter GP, the encrypted ciphertext CTB and the proxy re-encryption key. The proxy re-encryption ciphertext CTA is

generated on behalf of the node. After re-encryption is completed, the storage is sent to an external server, which sends the data storage location, LOCM, to the data owner B.

(6) Index Generation: $I \leftarrow E(PK, GP, w_i)$

Data owner B collects data with the keyword w={w1,w2...,wn}, input key PK, output encryption index I=(I1,I2... In). The data owner B creates a new transaction, appends the index I to the transaction and broadcasts the transaction to the blockchain system. The transaction with the index, just like the ordinary transaction in the blockchain, is verified and added to the block by the alliance cluster nodes.

(7) Search token generation: $TK \leftarrow TokenGen(MK, GP, w_i)$, and user A builds the search token.

User A generates the transaction and appends the search token to the dealer to send to the surrounding miner node, the union cluster node, for validation.

(8) Test: $\{0,1\} \leftarrow Test(I, TK, GP)$

After receiving the search token Tk submitted by User A, the alliance group node now carries out index matching in its own stored blockchain copy.

(9) Ask $(TK, I, GP) \rightarrow E(LOC_m)$ or Terminate

Using search tokens for keywords and encrypted indexes, the blockchain's federation cluster node performs a binary search algorithm and returns the storage location of the encrypted file.

(10)Ciphertext Decryption: $m \leftarrow D(PK, CT_B, SK_B)$

Input the system public key PK, encrypted ciphertext CTB and data owner B private key SKB to generate the inscription information m.

(11)Re-encrypt Decryption: $M \leftarrow RD(CT_A, SK_A)$

Enter the agent re-encrypt ciphertext CTB and visitor A's private key SKA to generate the plaintext information m.

4. Function and Safety Analysis

Fine-grained access control: The access control mechanism based on CP-ABE (Ciphertext Policy Attribute-Based Encryption) proposed in this paper can achieve fine-grained access control of data. The data owner defines the access control policy by himself. At this time, the identity and attribute information of the accessing user node are not considered. The data access rights can be obtained as long as it meets the access control policy formulated by the data owner. Therefore, from the point of view of data ownership, this scheme to meet the targeted attribute information access control, is more in line with the needs of data access users to achieve their fine-grained access control of data [19, 20].

Support keyword search: this scheme uses blockchain technology and searchable encryption technology to realise the user can improve the efficiency of obtaining the required information through key retrieval when sharing information resources. In sharing data with a large amount of data and relatively vague classification, keyword searchable encryption technology can reduce the storage load of blockchain, realise one-to-many data sharing, protect data privacy, and improve search efficiency. These will greatly help the quality of the information resource sharing model with large data volume, frequent transactions, and many isolated information islands.

Protection of data privacy security: the data privacy security in this scheme is enhanced by the blockchain technology and the proxy re-encryption access control mechanism, which can ensure the privacy security of data resources. On the one hand, the blocks in the chain of information data are stored encrypted, providing the foundation for data privacy protection; at the time of data information is sensitive information, such as the user's real-time location address, personal privacy and information, etc., can achieve high security of heavy encryption based on the proxy access control scheme, achieving high secrecy of information sharing. On the other hand, the restriction of access control policy is a solid and effective guarantee to provide private data security. Therefore, even if malicious node attacks and obtains the ciphertext information of the data, the plaintext data cannot be accepted because the access control policy specified by the data owner cannot be satisfied, and the corresponding proxy re-decryption key cannot be obtained from the representative node, to ensure the security of the privacy data [21, 22].

5. Conclusion

This paper analyzes and designs the data resource access control mechanism based on blockchain technology in detail. Firstly, the basic system architecture of the access control mechanism is constructed, and the process of accessing the share is described. Secondly, the attribute encryption technology in access control is designed in detail. In the method, cp-ABE and searchable proxy re-encryption technology are mainly used to provide data sharing security guarantees. Finally, it comprehensively analyzes the blockchain-based access control mechanism involved in this paper in terms of function and security. It proves that the blockchain technology and the encryption technology proposed in this paper play an essential role in the sharing of traffic data resources, and can improve the security of the data sharing process and have feasibility.

In future research, keyword ranking and fuzzy searchable encryption are considered to develop a fine-grained ciphertext search scheme to conduct fine-grained search queries for ciphertext data and realize ciphertext search and access control at the same time. It is hoped that multiple keywords can be searched on blockchain in future research to protect data privacy better. In addition to data privacy protection, identity privacy protection will be strengthened. And if further research can realize smart contracts and blind signatures can be used to hide user identity and protect identity privacy effectively would be better.

Acknowledgements

I would like to thank the monographs of the scholars quoted in this paper. Without the inspiration and help of the research results of these scholars, I would not be able to complete the

final writing of this paper. At this point, I would also like to thank each one who gave me a lot of valuable materials in the process of writing the paper, and also offered warm help in the process of typesetting and writing the article.

References

[1] Liu Bo, Wang Xinyan, Zhang Hongyan, Guo Jianxun, Qin Long, Zhang Jing, Chen Xin. A Data Access Control Method Based on Block Chain [P]. Henan Province: CN112257112A, 2021-01-22.

[2] Zhang Yuanyu, Nakanishi Ruka, Sasabe Masahiro, Kasahara Shoji. Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things † [J]. Sensors, 2021, 21 (15).

[3] Ding Yan, Huang Chenlin, Feng Chi, Tan Yusong, Dong Pan, Li Bao, Ren Yi, Tan Shuang, Zhang Jianfeng, Song Liantao. Access Control Method and System of alliance Data Sharing based on Blockchain [P]. Hunan Province: CN112364366A, 2021-02-12.

[4] Zhang Xiaohong, Sun Lanlan. Blockchain Ciphertext Cloud storage Sharing Method Based on property Broker Reencryption [P]. Jiangxi Province: CN109189727B, 2021-07-23.

[5] Raman R K, Vaculin R, Hind M, et al. Trusted multi-party computation and verifiable simulations: A scalable blockchain approach [J]. arXiv preprint arXiv: 1809.08438, 2018.

[6] Chen L, Lee W K, Chang C C, et al. Blockchain based searchable encryption for electronic health record sharing [J]. Future Generation Computer Systems, 2019, 95: 420-429.

[7] Zhang P, White J, Schmidt D C, et al. FHIRChain: applying blockchain to securely and scalably share clinical data [J]. Computational and structural biotechnology journal, 2018, 16: 267-278.

[8] Liang X, Zhao J, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications [C]. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017: 1-5.

[9] Xia Q, Sifah E B, Smahi A, et al. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments [J]. Information, 2017, 8 (2): 44.

[10] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain [J]. Journal of medical systems, 2018, 42 (8): 140.

[11] Boneh, D, Di Crescenzo, G, Ostrovsky, R, & Persiano, G. Public key encryption with keyword search [C]//In International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2004: 506-522.

[12] Ateniese G, Fu K, Green M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage [J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9 (1): 1-30.

[13] Zhang R, Xue R, Yu T, et al. Dynamic and Efficient Private Keyword Search over Inverted Index--Based Encrypted Data [J]. ACM Transactions on Internet Technology (TOIT), 2016, 16 (3): 21.

[14] Cai C, Yuan X, Wang C. Towards trustworthy and private keyword search in encrypted decentralized storage [C]. 2017 IEEE International Conference on Communications (ICC). IEEE, 2017: 1-7.

[15] Wang Z, Tian Y, Zhu J. Data Sharing and Tracing Scheme Based on Blockchain [C]. 2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS). IEEE, 2018: 1-6.

[16] Li H, Tian H, Zhang F, et al. Blockchain-based searchable symmetric encryption scheme [J] Computers & Electrical Engineering, vol. ED-73, 2019: 32-45.

[17] Meiklejohn, S, Pomarole, M, Jordan, G, Levchenko, K, McCoy, D, Voelker, G. M. A fistful of bitcoins: characterizing payments among men with no names [C]// In Proceedings of on Internet measurement conference. ACM, 2013: 127-140.

[18] Conti, Mauro. A survey on security and privacy issues of bitcoin [C]. IEEE Communications Surveys & Tutorials, Vol. 4, 2018: 3416-3452.

[19] Noether, S, Mackenzie, A. Ring confidential transactions [J], J. Ledger, 2016: 1-18.

[20] Jiang P, Guo F, Liang K, et al. Searchain: Blockchainbased private keyword search in decentralized storage [J]. Future Generation Computer Systems, 2020, 107: 781-792.

[21] Bouchaala Mariem, Ghazel Cherif, Saidane Leila Azzouz. TRAK-CPABE: A novel Traceable, Revocable and Accountable Ciphertext-Policy Attribute-Based Encryption scheme in cloud computing [J]. Journal of Information Security and Applications, 2021, 61.

[22] Zhang Y, Wang Y, Zhang Y, et al. A study on the data privacy access control and sharing mechanism of blockchain [J]. Lanzhou University of Technology, 2020.