Dynamic Secure Sharing of Cloud Audit Data Based on Blockchain Technology

Gangsong Dong[1], Xinyan Wang[1], Hanlei Cheng[2], Zhiyu Xiang[2], Dong Li[1], Boyu Liu[1]

[1]State Grid Information & Telecommunication Co., Ltd, Henan Province, China.

[2]YGSoft Inc, Zhuhai, Guangdong Province, China.

Keywords: blockchain; cloud audit; audit data; secure sharing; distributed storage; smart contract; privacy protection.

Abstract: Blockchain technology has become one of the most important emerging technologies in China's 13th Five-Year Plan period. Its characteristics of decentralization, non-tampering, traceability and high security can effectively solve the problems of traditional cloud audit data in central storage, vulnerability, tampering, incomplete transmission and unsafe data flow. The use of blockchain in cloud audit data can shorten compiling time and improve the quality of audit reports. In this model, a Consortium blockchain is built for different auditors; cloud auditing data can be shared only by users who have identity compliance through the node admission mechanism. Off-chain asynchronous secure storage is used for heterogeneous audit data with different ownership patterns and sensitivity degrees. Secure sharing of dynamic audit data is automatically performed through the consensus strategy and highly programmable smart contracts. Finally, based on blockchain technology, the goal of "simultaneous audit with economic activities" can be realized. The security and effectiveness of cloud audit data processing can be improved.

1. Development Situation of Cloud Audit

In cloud auditing, audit platforms are established based on cloud computing technology. The platforms collect scattered audit information from various industries. Then, through the storage and digitization of collected information, a central cloud database can be built. Thus, all kinds of audit resources (auditors, programs and related hardware devices) can work together through the cloud, [1] so as to better utilize the audit information, and provide auditors with a more efficient and scientific audit process.

Although cloud auditing brings some convenience to auditors, its problems in internal and external data security cannot be ignored. At present, the collection, storage, transmission, sharing and analysis of audit data are all under the centralized management of the "cloud audit platform". A single point of failure in the central cloud storage database can lead to data loss which requires long recovery time and high repair cost. [2] In the whole process of cloud audit, cloud audit software vendors have relatively strong control rights over background data. Information asymmetry makes it easy for software vendors to abuse, copy or even sell audit data without authorization. Compared with the traditional offline auditing, online synchronous auditing allows multiple auditors to access the "cloud audit platform" at the same time; it is difficult to realize the refined separation of duties, the effective data access and the storage privilege isolation control.

Therefore, a multi-node, synchronous backup and distributed storage system is needed to ensure the complete, safe and traceable dynamic sharing and circulation of audit data for different organizations, and ensure the high quality of audit.

2. Principles and Application Values of Blockchain Technology

2.1 Blockchain technology

The word of blockchain is proposed by Satoshi Nakamoto in the article, Bitcoin: A Peer-to-Peer

DOI: 10.25236/iccse.18.040

Electronic Cash System, which is a pioneering paper on the creation of Bitcoin. [3] It supports the stable and major-failure-free operation of the Bitcoin system for nearly nine years under the control of a non-central mechanism.

Blockchain is essentially a distributed data structure in which a block maintained by multiple parties is continuously growing and linking as a chain in chronological order. Blocks record packets of all transactions occur over a period of time and their hash values. When a transaction occurs, each node creates a candidate block; all nodes in the network collectively verify these candidate blocks. Once the majority of nodes (the amount of node data depends on different consensus mechanisms) confirm that block and broadcast to the whole network to accept the block, the candidate block becomes a new block and began to extend on the block chain. It provides permanent and non tampering transaction records. The use of programmable automated scripts (i.e. smart contracts) can support different business logics to achieve the value delivery of information.

Based on this, blockchain technology has characteristics of decentralization, non-tampering timing sequence, traceability, privacy protection, security and credibility; it is praised as "trust machine" by the Economists. [4]

2.2 Blockchain and audit

In foreign countries, all the Big Four auditors develop blockchain auditing. Ernst & Young launched a blockchain auditing analyzer. Through multiple blockchain sub-accounts, the overall transaction information can be obtained. Analysis and audit of the transactions of digital assets are carried out combined with data. Deloitte developed a blockchain platform Rubix, and designed Deloitte's Perma Rec blockchain application technologies. [5] By connecting various financial reporting systems, such as SAP and Oracle, Deloitte improved the transparency of purchasing and marketing processes, and realized the full automated auditing and strengthened audit supervision. Price Waterhouse Coopers can provide customers with an external review through blockchain technology, through with employees can monitor the company's blockchain transactions. [6] At the same time, KPMG joined the Wall Street Blockchain Alliance (WSBA) and provided its professional blockchain audit for BlockEx, an asset services platform.

In China, the blockchain was first written as a strategic frontier technology in the National "13th Five-Year" Informatization Plan. [7] In March 2018, the Ministry of Industry and Information Technology issued the Working Focus in Information Technology and Software Services Standardization of 2018 and proposed to establish a National Blockchain and Distributed Accounting Standardization Technology Committee. In June 2018, the National Audit Office put forward a number of proposals to strengthen and improve the audit of state-owned enterprises. The use of modern technology and methods, such as big data, cloud computing, blockchain and artificial intelligence, has brought revolutionary changes to the development of audit process. On April 24, 2018, the National Audit Office published a paper entitled Some Ideas for the Application of Blockchain Technology in Large Data Auditing. The paper envisages a decentralized storage system based on blockchain technology. The system does not have a centralized management institution; it treats local offices and certified auditors as independent peers. Data blocks in the system are maintained by nodes with maintenance functions in the whole system. [8]

2.3 Matching degree of blockchain and cloud audit data secure sharing

The data processing flow of cloud audit system includes data acquisition, data import, data exchange, data analysis and data display. The cloud audit data service model based on blockchain includes:

IaaS (Infrastructure as a Service) layer. Through standard data interface, offline upload and other means, massive data in ERP, SAP, financial control and other front-end business systems of audit units can be collected into the cloud for preliminary unified classification, filtering, storage and access control. [9]

PaaS (Platform as a Service) layer. It implements the fine management of audit data stored in the IaaS layer, and encapsulates various analysis and visualization components according to specific audit business requirements. It is helpful for audit institutions to construct different audit business processes independently and improve audit efficiency.

SaaS (Software as a Service) Layer. It encapsulates and stores the audit output of IaaS and PaaS. It not only displays the functions of collecting, analyzing and exchanging audit data in the cloud, but also stores existing audit methods, models, audit cases, auditor training programs and other resources to achieve more accurate value mining.

Blockchain cloud audit support module. It uses node access mechanism, distributed data storage, multi-node transaction consensus, asymmetric encryption, smart contract and other core technologies to effectively solve the security problem of data sharing in cloud audit.

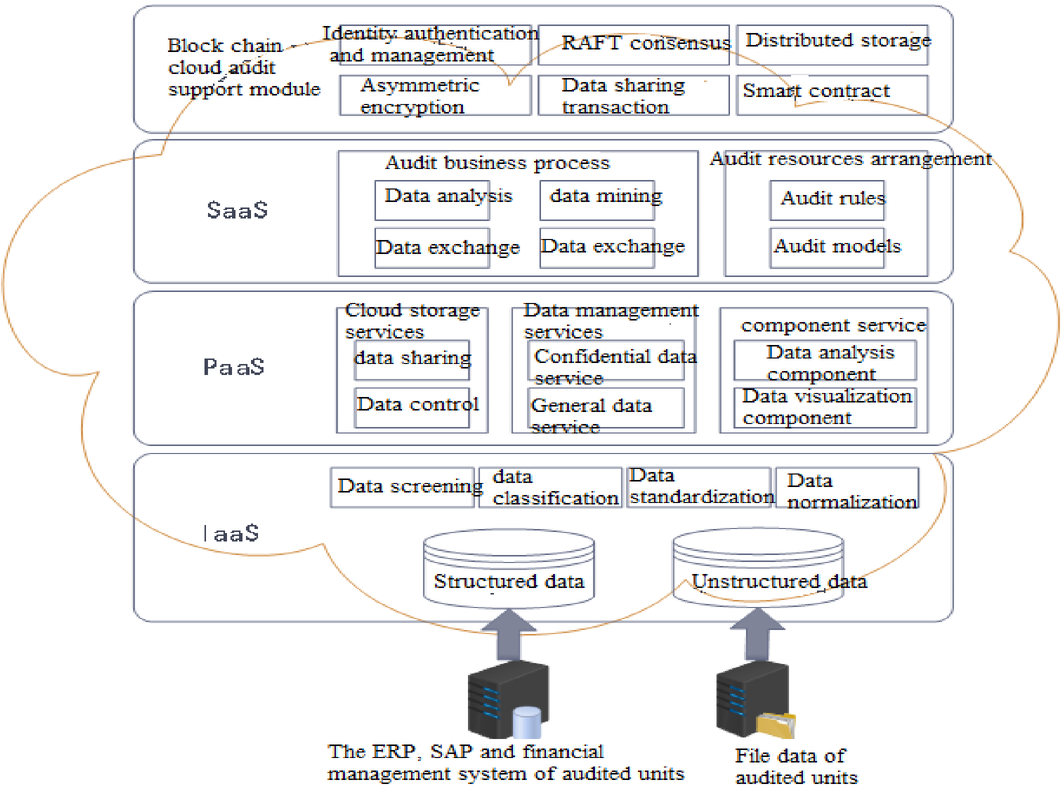


Figure 1. The service model of cloud auditing data based on blockchain

The matching degree of blockchain and cloud audit data security sharing is analyzed as following.

Audit data is encrypted asymmetrically by elliptic curve encryption algorithm and hash algorithm for a couple of times in the process of circulation. Only the private keys of authorized nodes can decrypt the data, which increases the difficulty of data decryption and strengthens the data security and credibility.

Key financial vouchers, documents and major contracts are stored as digital assets in the chain; different access rights are set according to auditors' responsibilities. The privacy of audit data is protected while the data can be shared across time and space; the shared log is traceable and cannot be tampered.

Using highly programmable scripts to code the audit model, [10] the system can automatically analyze relevant audit data and cross-check the authenticity of data according to specific audit objects and preset time periods, so as to eliminate auditors' subjective judgment on the validity of audit data, and make the whole audit process and audit results more fair, equitable, objective and reliable. [11]

In the distributed storage of blockchain cloud audit system, each node has a consistent data account, which not only solves the problems of high system load and slow running speed, but also increases the audit speed and reduces the maintenance cost of server by apportioning audit workload to different nodes.

Audit data on the chain is related to its producers; the auditor needs to formulate a programmable data access strategy. After data transaction is initiated, it is necessary to broadcast P2P in the whole network and get the approval of a certain number of nodes to get effective access permission, so as to ensure the utilization of audit data is compliance and security.

3. Cloud Audit Data Sharing Model Based on Blockchain Technology

3.1 Basic service model of cloud audit data based on blockchain

Consortium blockchain. In this model, the blockchain supporting platform is composed of accounting nodes of audit institutions, relevant auditors, audited units, local audit bureaus, institutes of certified public accountants and other authoritative organizations, and common nodes of stakeholders who use audit reports (including investors, tax bureaus, financial bureaus and banks). In the Consortium blockchain, all parties must participate in audit data maintenance and avoid unilateral tampering.

Basic structure of Consortium blockchain cloud audit. The cloud audit infrastructure model based on Consortium blockchain includes following parts.

1) Data Layer: it encapsulates asymmetric encryption, timestamp, hash operation and other technologies; the hash value of audit evidence received in a period of time is calculated through binary Merkle tree operation and then stored in the block. [10] When the cloud data is lost or damaged, data index can be used to synchronize data on the blockchain to ensure the fast and complete recovery of cloud data, and maintain the long-term stable operation of the cloud audit information system.

2) Network layer: it encapsulates the mechanism of data validation. Based on peer-to-peer network, it does not depend on any centralized nodes. Through the consensus mechanism, it asks nodes in the whole network to check the authenticity of data together, and adds trusted blocks to the longest main chain after authentication, in order to ensure the integrity of the entire audit resource chain.

3) Consensus layer: it encapsulates the method of quickly reaching consensus in a topological network with highly decentralized decision-making power. RAFT consensus algorithm is used to ensure that the accounting can be carried out normally as long as the n/2+1 node are normal. The Leader node is responsible for ensuring the synchronization of other nodes and his log. When the Leader node is down, other nodes in the cluster will elect a new Leader to keep accounting. [12]

4) Contract layer: the audit data sharing policy is output in the form of coded script on the chain, [13] allowing the system to automatically perform data sharing on specific nodes. The chain mainly presets simple audit business logics. Most of these relatively complex audit business logics are deployed in the cloud audit platform.

5) Service layer: through the distributed server, it can effectively integrate and manage application-related functions, including: identity authentication services, encryption and decryption services, distributed account services, smart contract services and data management services.

6) Application layer: it clearly shows the specific functions of blockchain system. It is an important link in the storage and sharing of audit data. Its different functions can be divided into user management, permission control, audit resource directory management and audit business management.

7) Presentation Layer: the system functions are displayed through the portal website. It takes the role of interacting with users. Audit institutions, auditors and audited units can access the application layer and access information resources through various interfaces through mobile terminals of the system.

Identity authentication and management of audit subjects. Before the sharing of audit data, each node needs to generate a digital certificate to check the identity of audit subjects based on the PKI system in the blockchain, and uses MSP (Membership Service Provider) to authenticate user identities, generate signatures and authenticate user identities. [14]

After auditor's registration on the chain, the CA authority is responsible for providing digital certificates to users, including public and private keys. Private keys are kept in private by the producer of audit resources only; public keys can be saved and used by the owner. For example, the audited unit can use its private key to digitally sign the data of small files or the hash values of large files; the auditor can use its public key to verify the authenticity and security of sender's identity as an audit resource provider. [15]

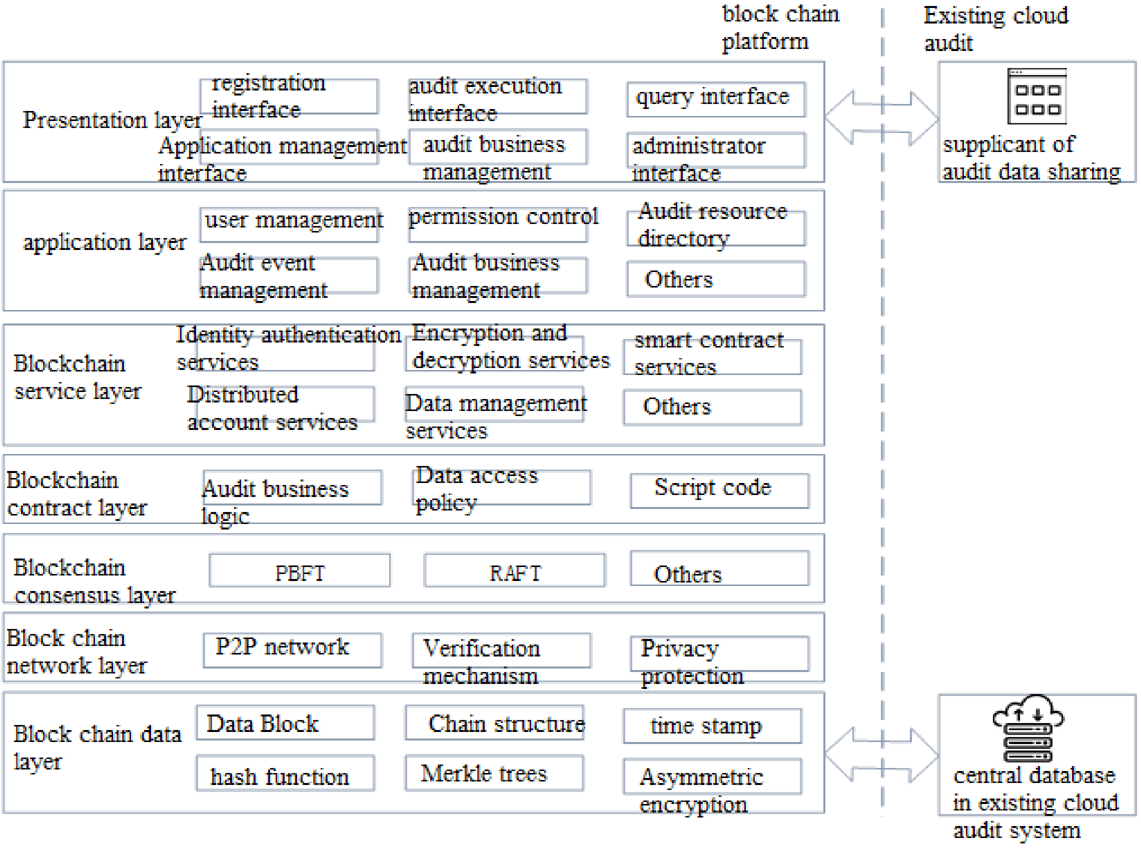


Figure 2. The infrastructure of cloud auditing model based on blockchain

3.2 The static secure storage of cloud audit data

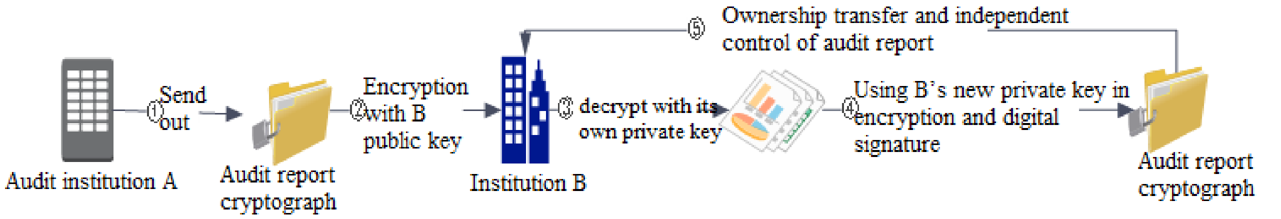
Audit data usually has large volumes and complex structures, including MySQL structured data, various kinds of accounting vouchers, financial statements, electronic contracts and other unstructured data. In order to improve the efficiency of audit data calling, the model applies the off-chain asynchronous storage mode in data secure storage.

Firstly, sensitive fields are set up in the cloud through content-aware encryption; key audit resources are screened out; asymmetric encryption is realized through RSA algorithm. For this kind of sensitive audit resources, structured data can be encrypted directly in the block-chain database through elliptic curve encryption algorithm. For unstructured data, after the hash operation, the unique hash value of the original data, namely the "digital fingerprint", can be generated. Then the file of hash fingerprint is signed by private key, and sent to the blockchain network to broadcast to all nodes. Then the data is verified through consensus. Finally, the effective records are synchronized to all nodes. The original data content cannot be deduced from the fingerprint; any changes in the original data will lead to the output of significantly different "digital fingerprint". [16] Therefore, once the chain is successfully linked, it cannot be falsified or forged.

3.3 The dynamic secure sharing of cloud audit data

Using public and private keys to decrypt data according to the ownership of audit data. Before the initiative of the audit business, audit resources produced by the audited units are stored in the block chain. Data access strategy is formulated through smart contract; only audit institutions and third parties with specific permissions can access and decrypt the file.

After the audit institution finishes the audit business, the audited unit can receive evaluation data which belongs to the audited unit. The data includes "audit reports, audit opinions and internal control evaluation reports". Then the audited unit needs to verify the signature of the audit institution, and decrypt the original cryptograph of audit evaluation with its own private key. [15] The newly generated private key is then used to digitally sign and encrypt the audit evaluation report again, so as to transfer the ownership of audit evaluation data from the audit institution to the audited unit. The audited unit can automatically authorize the sharing of audit results with the third party through the smart contract; it does not need to get the approval of the audit institution.



⑤ Ownership transfer and independent control of audit report
Send ① out
Encryption ②with B public key
③ decrypt with its own private key
Using B's new private key in ④encryption and digital signature
Audit institution A
Audit report cryptograph
Institution B
Audit report cryptograph

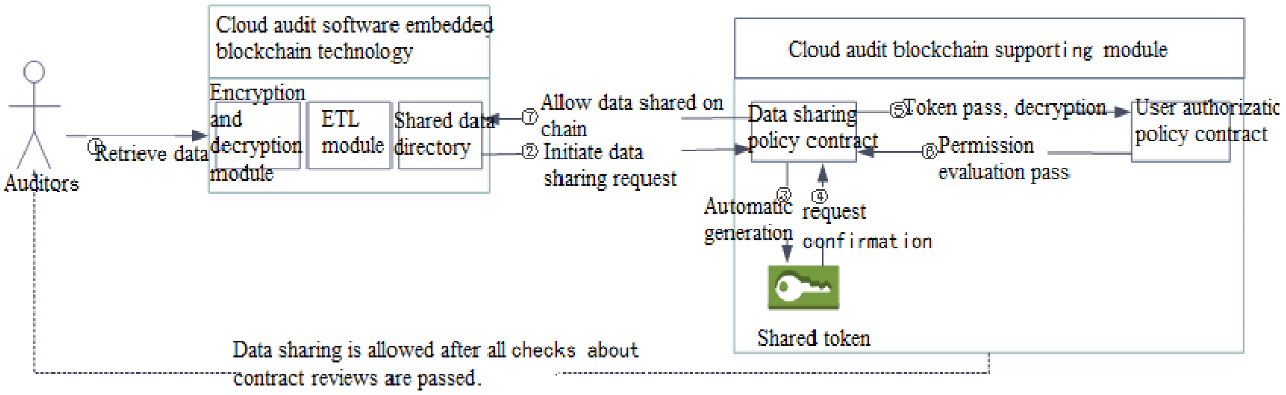
Figure 3. The mechanism of transferring the cloud auditing data ownership based on blockchain

Automate execution of data security sharing process through smart contracts.

(1) Auditors initiate audit data sharing requests. The auditor retrieves the shared data on the chain through the global shared data resource directory, creates a request for data sharing transaction, broadcasts it to the network, validates it and adds it to the blockchain for trusted records. [17] The auditor's own public key can be used in the request transaction.

(2) Smart contracts wait for the confirmation of audit data sharing request

Blockchain Membership Management Mechanism authenticates the identity of the auditor. If the auditor meets the criteria, the data sharing policy can be applied. At the same time, it sends the sharing request to the sharing policy contract and triggers the preset conditions. Each trigger automatically generates a shared token. The token is then sent back to the smart contract as a request transaction confirmation.



Cloud audit software embedded blockchain technology
Encryption and decryption module
ETL module
Shared data directory
Auditors
①Retrieve data
⑦ Allow data shared on chain
② Initiate data sharing request
Cloud audit blockchain supporting module
Data sharing policy contract
⑤Token pass, decryption
User authorization policy contract
⑥Permission evaluation pass
③ Automatic generation
④ request confirmation
Shared token
Data sharing is allowed after all checks about contract reviews are passed.

Figure 4. The secure sharing of cloud auditing data based on smart contract

(3) Audit data owners check auditors' shared tokens

The auditor receives the shared token and takes the token to visit the data owner. This node decrypts the shared token with the private key of audit data, obtains the public key of nonce and auditor, and then verifies the correctness of nonce and its signature. [18] After verification, the data owner decrypts the authorization policy according to the auditor's public key. The policy includes audit data operating authorization (includes the durations of data sharing, copy and download permission, could new contents be added or not, etc.)

(4) Sharing policy contracts wait for the results of evaluation on auditor's authority

Assessment is carried out based on the auditor's permission demands, requirements of the current audit business and current data environment. If all conditions are compliant and reasonable, the evaluation results will be returned to the shared strategy contract.

(5) Auditors are allowed to share data on the chain.

Sharing policy contract automatically releases or interrupts the auditor's API interface of sharing data according to evaluation results, and accomplishes the controlled and secure sharing of audit data.

In above process, data sharing strategy and user authorization strategy are used to automatically complete the whole process of audit data secure sharing. In this process, the sender's digital signature is needed in every transaction submission. The smart contract can determine the digital identities of both parties and realize the permission control.

4. Summary and Prospect

This paper studies the application of blockchain technology in cloud audit data storage and sharing, and implements off-chain asynchronous secure storage according to the sensitivity and structural diversity of audit data. Based on core blockchain technologies, such as membership management mechanism, consensus mechanism and smart contracts, and according to the ownership of audit results and audit business requirements, multiple temporal and spatial access and operation control are set up for audit institutions and audit objects. A chain database access strategy is formulated to achieve the dynamic secure sharing of audit data; all audit data should circulate in a consistent and frictionless manner in every audit session. Through the blockchain technology, audit data cannot be tampered with; the high degree of privacy can be guaranteed. All transactions are traceable. A series of audit operations, including audit data confirmation and analysis, can be automatically carried out without relying on the third party. The goal of "simultaneous audit with economic activities" can be realized based on the objective technology. Blockchain can protect data security and standardize the audit procedure, and then improve the efficiency and quality of audit business.

In view of technical bottleneck of blockchain, in the future, we need to focus on improving the efficiency of consensus mechanism, shortening the time of data transaction confirmation, improving the capacity of sharing processing, and designing storage access and optimization modes to break the limitation on the capacity of original blockchain network. The well-conceived smart contracts can ensure the accurate correspondence between code logic and business logic. The exploration of blockchain in the field of cloud auditing has wide application. It cannot be limited in the real-time audit data storage and the whole network consensus of sharing behavior; it can also be used in business execution and post-audit tracking, which can help to achieve a sustainable and reliable audit model.

Acknowledgement

Fund Project: This project is supported by Foundation for Science and Technology Projects of State Grid Companies (Contract No.: SGHAXT00YJJS1800107).

References

[1] F. Wen, Cloud computing and cloud auditing - Reflection on the concept and framework of auditing in the future, J. The Chinese Certified Public Accountant. 2 (2011) 98-103.

[2] R.K. Duncan, M. Whittington, Creating an immutable database for secure cloud audit trail and system logging, Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 2017.

[3] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. J. Consulted, 2008.

[4]https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[5] J. Kokina, R. Mancha, D. Pachamanova, Blockchain: Emergent industry adoption and implications for accounting, J. Journal of Emerging Technologies in Accounting.14 (2017) 91-100.

[6] Wang Y, A. Kogan, Designing confidentiality-preserving Blockchain-based transaction processing systems, J. International Journal of Accounting Information. 2018.

[7] State Council, 13th Five-Year National Informatization Plan, 2016.

[8] http://www.audit.gov.cn/n6/n1558/c121809/content.html.

[9] M. Armbrust, A. Fox, R. Griffith, et al., A view of cloud computing, J. 53(2010) 50-58.

[10] A. Kosba, A. Miller, E. Shi, et al., Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, Security and Privacy (SP), IEEE Symposium, 2016.

[11] J. Dai, M. A. Vasarhelyi, toward blockchain-based accounting and assurance, J. Journal of Information Systems. 31(2017).

[12] D. Huang, X. Ma, S. Zhang, Performance Analysis of the Raft Consensus Algorithm for Private blockchains, J. 2018.

[13] http://www. ethereum. org/pdfs/EthereumWhitePaper. pdf, 2014.

[14] S. Tahir, M. Rajarajan, Privacy-Preserving Searchable Encryption Framework for Permissioned Blockchain Networks. J.

[15] G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops, 2015.

[16] X. Liang, S. Shetty, D. Tosh, et al., Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2017.

[17] D. Tapscott, B. Barry, Grown up digital: How the Net Generation is Changing Your World, McGraw-Hill New York, New York, 2009.

[18] M. Milutinovic, W. He, H. Wu, et al., Proof of luck: An efficient blockchain consensus protocol, Proceedings of the 1st Workshop on System Software for Trusted Execution, 2016.