



# Application Architecture of Accounting Information and Auditing System Based on Blockchain Technology and a Private Data Sharing Technology

Beijia Zhong<sup>1</sup>, Minjia Du<sup>1</sup>, Sirui Huang<sup>1</sup>, and Jiawei Qian<sup>2</sup>(✉)

<sup>1</sup> School of International Nanchang, Jiangxi University of Finance and Economics, Nanchang, Jiangxi, China

<sup>2</sup> Shanghai Trusted Digital Technology Laboratory, East China Normal University, Shanghai, China

jwqian@stu.ecnu.edu.cn

**Abstract.** Under the background of informatization and intelligence of financial management, the accounting information and auditing system based on blockchain technology has improved the quality of financial information. It is possible to explore the use of the blockchain technology as a basis to solve the information traceability problem of information transmission in accounting information systems, and the distributed storage architecture of blockchain, lightweight digital signature algorithm, consistency Algorithms and other technologies are used to make up for accounting and auditing information security loopholes, thereby preventing information from being tampered with. Nevertheless, the authenticity, reliability and integrity of blockchain information transmission can also be solved by the EPC system network technology and Hash Encryption Algorithm. Aiming at safer and more efficient accounting information and auditing system, this paper proposes our computing scheme based on fully homomorphic encryption technology and semi-trusted mechanism in the context of applying financial robots, which improve the security of internal information under the premise of full disclosure.

**Keywords:** Blockchain · Homomorphic encryption · Accounting information system · Multi-party Secure Computing · Privacy Protection

## 1 Introduction

Blockchain technology is a new application mode of computer technology such as distributed data storage, encryption algorithm, point-to-point transmission, and consensus mechanism. The consensus mechanism refers to the algorithm for establishing trust relationships between different nodes in the blockchain system. As a distributed database system, blockchain is characterized by being difficult to tamper with, difficult to forge, and traceable. Once the data enters the blockchain, it will be recorded. This feature determines that it is inseparable from the application of the Internet. The richer the application scenarios, the faster the development of blockchain technology and industry. With the improvement of the blockchain technology framework and application scenarios, great

innovations have emerged in corporate accounting systems and internal controls. Under the application of blockchain, the corporate accounting presents the character of decentralization. Each blockchain participant completes the information record independently, compares and analyzes the accounting information and transmits it to each business activity participant for preservation, and the record can provide theoretical support for subsequent work. In the age of information, blockchain also has many inherent risks. Inherent risks include technical risks, data security risks and third-party vendor risks. Therefore, the inherent risks should be reasonably controlled and prevented, and the impact on information customers, the environment, and internal controls should be considered. For inherent risks, verifiable homomorphic encryption allows users to analyze and retrieve specific encrypted data under the condition of data encryption, effectively ensuring information security while verifying the accuracy of information. In recent years, homomorphic encryption has been increasingly used in the practical fields. Qian [1] propose a lightweight t-times homomorphic encryption scheme, which can reduce the computational cost of smart devices further and resist quantum attacks. Qian also [2] proposed an aggregate signature scheme based on new Batch RSA. After that, a data aggregation scheme is proposed based on this aggregate signature scheme and the qualified homomorphic cryptosystem. Lin [3] designs a more efficient and safer SaaS Cloud Accounting Platform based on the Multi-party Secure Computing technology and Lattice-based Homomorphic Encryption system, and the platform proposed by us further improves the accuracy of accounting information on this basis. In addition, Wei et al. [11] Also applied this technology to the Iov scene and proposed an anti quantum privacy protection scheme. In this paper, we will design a privacy protection platform based on this technology and CKKS [12] cryptographic algorithm.

Federated learning is a multi-layer collaborative data analysis model based on deep neural network and intermediate representation. In the process of using artificial intelligence, the quality of artificial intelligence analysis results depends on the quality of information, and information contains a lot of sensitive private information. In order to overcome these difficulties, the learning of federalism training without sharing sensitive local data was proposed by McMahan [4]. Federated learning defines a machine learning framework in which virtual models are designed to solve the problem of different data owners collaborating without exchanging data. Unlike traditional big data analysis and machine learning, federated learning does not require uploading large amounts of information owned by different subjects to the same server. Instead, it sends algorithms to subjects with data and trains shared models in coordination with a central server. Therefore, Ma J [5] proposed that FL has the advantage of preventing the leakage of sensitive private information because it does not require local data sharing.

At present, countries around the world have carried out researches and applications of blockchain in the field of accounting information systems. Yermack [6] paints a scenario where, if a blockchain containing accounting transactions had access, anyone could aggregate those transactions into financial statements in real time without the need for auditors to guarantee the accuracy of the books. Ruckeshauser [7], on the other hand, highlighted the dangers of decentralized consensus in blockchain, enabling management to override internal controls in the enterprise blockchain. Blockchain accounting has been introduced to help professionals and track “block” orders in a secure way. With

blockchain, we can not only record cross-behavior, but also verify transactions without intervention or intermediaries, a technology based entirely on automated systems [8] (Walch, 2016). Blockchain technology has a beneficial positive effect on real-time accounting practices [9] (Byström, 2019). Blockchain provides transparency and certainty about asset ownership, history, and the existence of obligations. This will save accountants a lot of time and reduce the cost of maintaining and coordinating registers, which will greatly improve efficiency. In addition, as record keeping moves to blockchain, more resources will be available for planning and evaluation [10] (Bogdana, 2020).

In the process of accounting information collection, manual recording of original accounting documents is easy to make the accounting data recorded mixed with subjectivity. The manual cooperation mode of the original accounting information system will cause a variety of problems such as accounting information distortion, information asymmetry, information island and so on, which restricts the further development of accounting informatization. Blockchain technology not only lies in the transmission of information, but also completes the transmission of value, which puts forward new solutions to the realistic problems existing in the current accounting information system. At the same time, the combination of accounting information system and artificial intelligence is further developed. In the process of converting accounting data into accounting information through accounting algorithms, the deep learning of artificial intelligence makes the algorithm for complex conditions and logical discrimination further develop. Based on this, combined with the existing research results, this paper designed a set of accounting information system based on homomorphic encryption technology, encryption scheme. On the basis of human-machine cooperation, it provides a solution to prevent information leakage after the accounting information system is attacked, and also solves the problem of distortion caused by artificial tampering of accounting information.

## **2 Application Architecture Design of Encryption Platform of Accounting Information Systemase of Use**

Under the premise of artificial intelligence, while the economic business of enterprises is carried out, artificial intelligence can achieve accounting through smart contracts, improve the efficiency of accounting algorithms, and realize accounting processing on the blockchain. The accounting information system platform breaks the various drawbacks of the traditional model, not only has traditional financial information, but also contains more unstructured data. Through this comprehensive accounting information system platform, enterprise management can query production material information in real time, and these data are completely authentic and reliable on the blockchain. Finally, intelligent, full, real-time disclosure and personalized accounting reports are formed. In the application of blockchain technology, the authenticity, reliability and clarity of accounting information depends on the completeness and security of various dimensions of data and information systems such as suppliers, manufacturers, consumers, etc.

Encryption of accounting information system through cryptography and distributed storage technology, the input and storage of accounting information can be realized on the blockchain, and information users can realize the storage and circulation on the chain,

achieving technological innovation of full-process supervision, connecting enterprises, auditors, government and other stakeholders related to invoices, so that every link can be traced back, so that the data cannot be tampered with and non-repudiation. At the same time, the combination of multi-party secure computing technology enables the entrusting party to complete the calculation of financial data without submitting data in plain text, realizing “data availability is invisible”, and each node on the blockchain adopts an appropriate model to execute the accounting algorithm, and then, using the public key to encrypt the data of each node. After that, the platform can perform the homomorphic operation on the ciphertext to obtain the accounting information of the comprehensive multi-party data. Finally, use the private key for decryption to obtain the plaintext accounting information. In the meantime, the platform has a certain anti-interference ability, and can resist quantum computing attacks with small data sets, thereby preventing tampering by malicious attacks. In this process, the confidentiality of data information will always be guaranteed, and information inquirers and third-party platforms cannot obtain any other information except the information they should obtain, which avoids the problem of information leakage caused by traditional accounting information systems.

## **2.1 Selecting Framework Design of Encryption Platform for Accounting Information System from the Perspective of Blockchain**

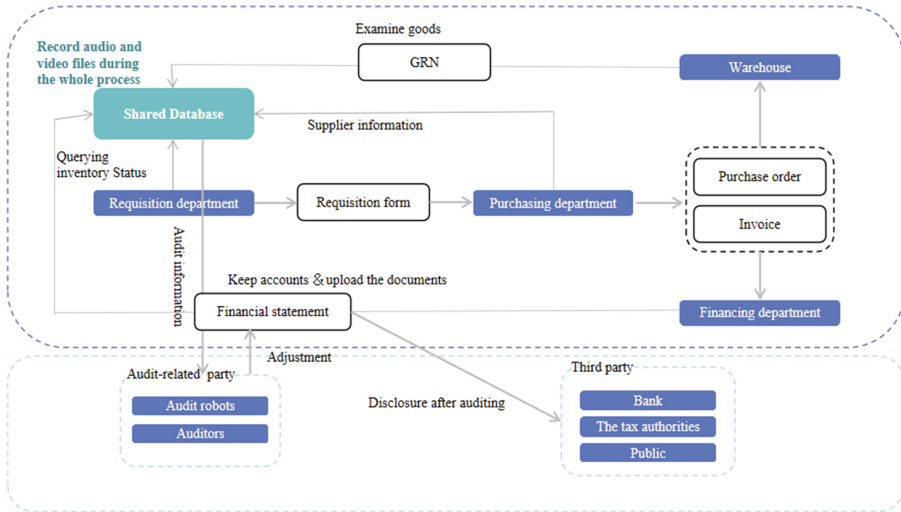
Accounting information stakeholders such as corporate financial staffs and auditors can register and log in their accounts at their network nodes, send data queries and other requests in the information transmission process, and back up and store the accounting information data entered each time.

Enterprises and other accounting information users hold different nodes, but have similar input and query functions, which can achieve a high degree of interoperability of accounting information. While the information is interoperable, the specific accounting information within the enterprise can be processed for this part through the MPC algorithm of the blockchain. Accounts and data are encrypted and backed up, which greatly ensures the security of information.

In order to ensure the data privacy of enterprise accounting information in the process of accounting information flow, the information input party of each node will access the data information to the multi-party secure computing platform for encrypted calculation (the data encryption platform performs ciphertext authorization), in order to ensure accurate calculation results. Error-free, the information transmission process is safe and reliable, and it also has security, that is, the computing party only returns the operation result, but does not know the initial data.

## **2.2 Application Structure of Encryption Platform of Accounting Information System**

The flow of accounting information passes through multiple nodes including enterprises, auditors, and governments, from the input of accounting information to the use of accounting information to produce financial statements or to strengthen internal control. When the accounting information stakeholders such as corporate financial personnel



**Fig. 1.** Accounting and Auditing Information System from the Perspective of Blockchain

connect the original data to the computing system, the data encryption platform will authorize the algorithm and data use, and then the computing party will perform various operations on the encrypted original data within the framework of the consensus rules. All kinds of calculations required, including accumulation, comparison and other operations, and then directly generate the results for dissemination across the network. The platform side does not need to know the calculation process, and the calculation side does not know the original calculation data. The entire operation can be supervised by supervisors. Safety and convenience are guaranteed.

In this framework, each node and encryption system perform their own functions. Homomorphic encryption enables certain authorizations to be given to data on the basis of privacy protection, and the decentralization of the blockchain makes it impossible for information to be tampered with at will (Fig. 1).

## 2.3 Case Study

### 2.3.1 Step1

By combining the sales information and inventory quantity in the shared database, the purchasing department finds the shortage of materials and fills the requisition form in the purchasing department;

### 2.3.2 Step2

The purchasing department decides whether to purchase after inquiring the inventory status and supplier information in the shared database;

### **2.3.3 Step3**

If purchasing is required, requisition department will fill out the purchase form and purchase invoice and submit them to the financial department after successful negotiation with the supplier, and then provide the specific purchase data and supplier information to database;

### **2.3.4 Step4**

Verify the supplier's materials with the purchasing information in the database after their arrival. If the verification is successful, the materials will be put into storage and the receipt will be filled out, and then the original voucher of the receipt will be uploaded to the shared database.

### **2.3.5 Step5**

The financial department backs up the warehousing receipt and purchase invoice in the shared database, selects the appropriate business type automatically in the shared database, and automatically produces the accounting vouchers to enter into the database while keeping accounts;

### **2.3.6 Step6 (Parallel with Step2–5)**

Verify the authenticity and fairness of the transaction and accounting by using electronic contract text, on-site audio and video files related to the transaction, and finally generate the audit domain information of the block when the business and accounting occur.

### **2.3.7 Step7 (Parallel with Step2–5)**

Audit robot audit publicly, check whether the transaction occurred in the bookkeeping process is correctly classified into the right subject. For example, if there exists a difference between inventory data and book data, we should perform audit difference adjustment. The inventory deficit is to be dealt with the property loss and overflow. After being approved by management, the company shall classify the inventory loss reasonably according to the causes: the inventory shortage caused by sending and receiving errors and poor management will be included in the management expenses; the inventory damage caused by natural disasters and other extraordinary reasons will be included in the non-operating expenses. If belongs to the error of accounting bookkeeping, the classification error between the inventory items can be directly adjusted the difference between the relevant categories. On this basis, if any significant anomaly is found, it will be submitted to the auditor for verification.

### 2.3.8 Step8

After auditing robot and auditor verifying, the purchase will affect the interactive electronic financial statement by affecting inventory, expense, cash flow, payable, etc.

### 2.3.9 Step9

Banks, tax authorities, the public and other nodes can judge and authenticate the statement information in combination with the public factual information.

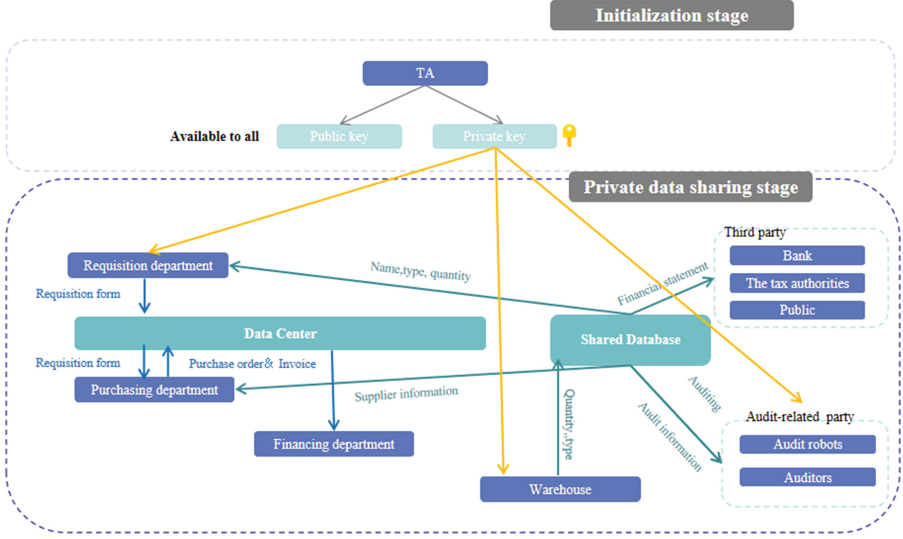
## 3 Key Cryptography Algorithms and Security Analysis

### 3.1 Homomorphic Encryption

In order to ensure that the four operations can be carried out normally on the supervision platform, we adopt a completely homomorphic ciphertext data analysis cryptographic scheme based on CKKS [12] real number field to encrypt the original data. CKKS is an approximate homomorphic cryptographic scheme based on the real number field. It is used for data analysis in ciphertext, and it is also a common scheme in outsourced machine learning computing. We adopt the famous CKKS17 scheme, which is described as follows:

$\text{Enc}_{\text{pk}}: m \mapsto (c, L, v, B_{\text{clean}})$  for some  $v \geq \|m\|_{\infty}^{\text{can}}$   
 $\text{Dec}_{\text{sk}}: (c, l, v, B) \mapsto ((c, sk) \pmod{q_l}, B)$   
 $\text{RS}_{l \rightarrow l'}: (c', l, v, B) \mapsto (c, l', p'^{l'-l} \cdot v, p'^{l'-l} \cdot B + B_{\text{scale}})$   
 $\text{Add}: ((c_1, l, v_1, B_1), (c_2, l, v_2, B_2)) \mapsto (c_{\text{add}}, l, v_1 + v_2, B_1 + B_2)$   
 $\text{Mult}_{\text{evk}}: ((c_1, l, v_1, B_1), (c_2, l, v_2, B_2)) \mapsto (c_{\text{mult}}, l, v_1 v_2, v_1 B_2 + v_2 B_1 + B_1 B_2 + B_{\text{mult}})$

- $\text{KeyGen}(1^\lambda)$ .
  - Given safety parameter  $\lambda$ , select second power  $M = M(\lambda, q_L)$ , the integer  $h = h(\lambda, q_L)$ , the integer  $P = P(\lambda, q_L)$  and the truth-value  $\sigma = \sigma(\lambda, q_L)$ .
  - Choose  $s \leftarrow \text{HWT}(h)$ ,  $a \leftarrow R_{q_L}$  and  $e \leftarrow \text{DG}(\sigma^2)$ . Set the evaluation key to  $\text{evk} \leftarrow (b', a') \in R_{P \cdot q_L}^2$ , when  $b' \leftarrow -a's + e' + Ps^2 \pmod{P \cdot q_L}$ .
- $\text{Ecd}(z; \Delta)$ .  
A vector of  $N/2$  dimensions for a Gaussian integer  $z = (z_j)_{j \in T} \in \mathbb{Z}[i]^{N/2}$ , calculate the vector  $[\Delta \cdot \pi^{-1}(z)]_{\sigma(R)}$ , and returns its inverse relative to the canonical embedding map.
- $\text{Dcd}(m; \Delta)$ . For input polynomial  $m(X) \in R$ , Compute the corresponding vector  $\pi \circ \sigma(m)$ . Returns the closest vector to a Gaussian integer after scaling.  $z = (z_j)_{j \in T} \in \mathbb{Z}[i]^{N/2}$ ,  $z_j = \left[ \Delta^{-1} \cdot m(\zeta_M^j) \right]$  for  $j \in T$ .
- $\text{Enc}_{\text{pk}}(m)$ .  
choose  $v \leftarrow \text{ZO}(0.5)$  and  $e_0, e_1 \leftarrow \text{DG}(\sigma^2)$ . And output  $v \cdot pk + (m + e_0, e_1) \pmod{q_L}$ .
- $\text{Dec}_{\text{sk}}(c)$ .  
For  $c = (b, a)$ , output  $b + a \cdot s \pmod{q_l}$ .



**Fig. 2.** Accounting and Auditing Information System based on private data sharing technology

- Add  $(c_1, c_2)$ . For  $c_1, c_2 \in R_{q_l}^2$ , output  $c_{add} \leftarrow c_1 + c_2 \pmod{q_l}$ .
- Mult $_{evk}(c_1, c_2)$ .  
For  $c_1 = (b_1, a_1), c_2 = (b_2, a_2) \in R_{q_l}^2$ , let  $(d_0, d_1, d_2) = (b_1b_2, a_1b_2 + a_2b_1, a_1a_2) \pmod{q_l}$ . Output  $c_{mult} \leftarrow (d_0, d_1) + [P^{-1} \cdot d_2 \cdot evk] \pmod{q_l}$ .
- RS $_{l \rightarrow l'}(c)$ . For  $c \in R_{q_l}^2$ , output  $c' \leftarrow \left[ \frac{q_{l'}}{q_l} c \right] \pmod{q_{l'}}$ .

Based on CKKS17 [12] and Qian et al.'s HLP [1] algorithm, we carried out 1000 different polynomial simulation experiments and verified that the error distance was small, and the results of four operations in plaintext could be 100% equivalent to the results of original data encryption and decryption. Therefore, this scheme is very suitable for our business scenarios (Fig. 2).

### 3.2 Process Description of the Privacy Scheme

Initialization stage:

Perform the following initialization operations based on the permission requirements:

1) Step 1:

The third-party trusted authority TA releases the external public key and private key pair ( $PK_{HLP}$  and  $SK_{HLP}$ ) encapsulated by the key, and exposes the external public key and sends the private key to all participating parties respectively.

2) Step 2:

The third-party trusted organization TA promulgated the public and private key pairs of CKKS ( $PK_1, SK_1$ ), ( $PK_2, SK_2$ ), ( $PK_3, SK_3$ ) and HLP ( $PK_4, SK_4$ ) for the name, type, quantity and amount of the goods respectively. And all public keys are exposed,  $SK_1$ ,



$SK_2$ ,  $SK_3$  are given to warehouse personnel, and  $SK_2$ ,  $SK_3$ ,  $SK_4$  are given to audit robots and auditors.

Private data sharing (accounting informatization and auditing) stage:

*1) Step1:*

The purchasing department holds the private key to query the name, type and quantity of the inventory to be purchased in the shared database, fill in the purchase requisition, and transfer the name, type and quantity of the inventory to be purchased by uploading the original voucher chart of the purchase requisition to the data center. The purchasing department can download the purchase requisition through the data center. Purchase requisition format for the data field in the (hash (hash (ID) || T),  $PK_1$  (name), hash (name),  $PK_2$  (kind), hash (kind),  $PK_3$  (money), hash (money),  $PK_4$  (num), hash (num)).

*2) Step2:*

The purchase department queries the name, type and quantity of inventory in the purchase requisition in the data center through ciphertext, and queries the price in the supplier files in the shared database to decide the purchase plan;

*3) Step3:*

If the purchase department confirms the need to purchase, after successful negotiation with the supplier, it fills out the purchase order and purchase invoice as original documents and transmits them to the financial department through the data center. Only then can it use the private keys  $SK_1$ ,  $SK_2$  and  $SK_3$  for decryption, and then encrypt the amount, quantity and type of the purchased inventory with the corresponding public key and feed back to the shared database;

*4) Step4:*

Supplier after the goods shipped, warehouse personnel to enter the actual warehouse inventory quantity, type a Shared database, the dock receipt as China original vouchers input data, system in the condition of encrypted with the purchasing department input validation, the number of species do subtraction, proves successful, the material warehousing and fill the receipt as the original vouchers input data middle;

*5) Step5 (parallel with step4):*

The financial department records the previous purchase order and purchase invoice through the data center, performs the encrypted bookkeeping through the shared database, selects the appropriate business type from the shared database, and automatically produces accounting vouchers and inputs them into the shared database while automatically bookkeeping.

*6) Step6 (parallel with step2–5):*

When business and accounting occur, electronic contract text, on-site audio and video files, and other original credentials related to transactions are encrypted and stored in the shared database to form the encrypted audit domain information.

*7) Step7 (parallel to step2–5):*

Audit robot can hold about inventory in a Shared database type, quantity, amount to the private key, the number of inventory accounting after decryption encryption, kinds and amount of information, verify the deal in the process of charge to an account is correct categories in the right subjects, the auditor also hold type, quantity, amount of keys, In case of major abnormal events, the type, quantity and amount information of

audit classification can be viewed after decryption, and the audit process of the audit side composed of audit robot and auditor can be calculated by homomorphic addition and subtraction in ciphertext.

*8) Step8:*

After accounting by auditing robot and auditor on the shared database, the purchase transaction is verified and directly affects the amount under the account of the interactive electronic statement. The account and amount of the electronic statement are visible in plain text by other third parties.

*9) Step9:*

Banks, tax authorities, the public and other nodes can judge and authenticate the visible amount in the subject of public statements, in which the amount accounting process is not visible under ciphertext.

### 3.3 Security Analysis

We analyze the proposed scheme from the privacy, integrity, forward security and confidentiality of the message. Homomorphic encryption technology ensures that the government, auditors and data encryption platform parties will not disclose to other participants except themselves and the plaintext size comparison in the case of third-party leakage of data privacy; and through identity-based fully homomorphic encryption to ensure that the information of the participants is not queried by other participants through ciphertext retrieval, these operations ensure the privacy of our scheme. What's more, we ensure the confidentiality of our scheme under the premise of high efficiency through fully homomorphic encryption with fewer operations; in addition, the public computing part of the multi-party secure computing platform ensures the integrity of the data involved in the operation. Finally, we guarantee the forward security of the scheme by randomly generating different identity-based fully homomorphic keys for the data queried by different users.

## 4 Conclusion

Due to the large accounting information system and the lengthy circulation chain, problems such as information leakage and information distortion are easy to occur in the process of information input and use. The application of the intelligent accounting system of financial robots improves the efficiency of information processing. Accounting information system can query financial information in real time. The performance problems of computing processing; and the multi-party secure computing technology has the characteristics of input privacy, computing correctness and decentralization, which can help solve these problems very well. On the one hand, it realizes the interconnection and cooperation between data holding points, and on the other hand, it ensures the privacy and security of computing. Aiming at the information security problem of accounting information system, this paper proposes our computing scheme based on fully homomorphic encryption technology and semi-trusted mechanism. From the query process and model proof, the data sharing system based on multi-party secure computing technology can

realize efficient and secure multi-party data sharing and collaboration. This application has great practical significance for the development of accounting information system.

At present, the application of blockchain in the accounting information system platform is in the exploratory stage, and there are defects such as high construction cost, limited storage space of the blockchain itself, and high computing cost; and the multi-party security computing model cannot perform high-order polynomial models. Fully homomorphic operation. We will continue to improve the computational efficiency of the scheme in future research.

**Acknowledgment.** This work was supported in part by School of Accounting of Jiangxi University of Finance and Economics for its reasonable suggestions for the accounting knowledge in this thesis, which really played an important role in the preparation of the original manuscript. Then, I will give my sincere gratitude to the MPC Technology Research Team of East China Normal University for the knowledge and technical support in the field of cryptography. It is of great help for me to finish this thesis successfully.

## References

1. Qian J, Cao Z, Dong X et al (2020) Two secure and efficient lightweight data aggregation schemes for smart grid. *IEEE Trans. Smart Grid* 12(3):2625–2637
2. Qian J, Cao Z, Lu M et al (2021) The secure lattice-based data aggregation scheme in residential networks for smart grid. *IEEE Internet Things J* 9(3):2153–2164
3. Lin J, Qian J (2021) A multi-party secure SaaS cloud accounting platform based on lattice-based homomorphic encryption system. In: 2021 international conference on public management and intelligent society (PMIS)
4. McMahan HB, Moore E, Ramage D, et al (2016) Communication-efficient learning of deep networks from decentralized data
5. Ma J, Naas SA, Sigg S, et al (2021) Privacy-preserving federated learning based on multi-key homomorphic encryption
6. Yermack D (2015) Corporate governance and blockchains. *Soc Sci Electron Publ* 21(1):7–31
7. Rückeshuser N (2017) Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls
8. Walch A (2015) The bitcoin blockchain as financial market infrastructure: a consideration of operational risk. *NYUJ Legis Public Policy*
9. Byström H (2019) Blockchains, real-time accounting, and the future of credit risk modeling
10. Bogdana PI, Adriana D (2020) Blockchain – the accounting perspective. In: Proceedings of the international conference on business excellence. Sciend
11. Wei C, Wu T, Liu X, Xiong S (2022) The latticed-based path privacy protection aggregation scheme for internet of vehicles. *IEEE Access* 10:19117–19123. <https://doi.org/10.1109/ACCESS.2022.3150839>
12. Cheon JH, Kim A, Kim M, Song Y (2017) Homomorphic encryption for arithmetic of approximate numbers. In: Takagi T, Peyrin T (eds) *ASIACRYPT 2017*, vol 10624. LNCS. Springer, Cham, pp 409–437. [https://doi.org/10.1007/978-3-319-70694-8\\_15](https://doi.org/10.1007/978-3-319-70694-8_15)

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

