Privacy Preserving Model Based on Zero-Knowledge Proof for International Food Trade Blockchain Platform

Yue Li, Peiting Xu*, Yunfa Huang, Zengjin Liu

* Corresponding author: peitingx@163.com

School of Computer Science and Technology, Dong Hua University, No. 2999, Renmin North Road, Songjiang District, Shanghai, China 201620

Abstract: In recent years, the business demand of international cold chain food trade has been increasing, but the process is complex, time-consuming, and there are data trust issues. This paper proposes a blockchain-based international cold chain trade platform system, which uses the immutable and traceable features of the blockchain to solve the problem of unreliable information in traditional systems. Aiming at the financing difficulties of small and medium-sized enterprises in international cold chain trade, this paper proposes a privacy protection scheme based on zero-knowledge proof. Through the blockchain platform, quickly use historical order information to analyze the operating conditions of small and medium-sized enterprises, and evaluate the amount of financing that small and medium-sized enterprises can obtain. It can reduce the problem of many financing steps and long cycle for small and medium-sized enterprises in the traditional financing model. Through the analysis of simulation results, the privacy protection scheme proposed in this paper can be implemented within an effective time.

Keywords: zero-knowledge proof, blockchain, Pedersen commitment, homomorphic encryption

1. INTRODUCTION

With the further development of global food trade, the business demand for international cold chain food trade is also increasing. International trade involves the procedures of market supervision, customs, foreign exchange, taxation and other regulatory authorities. The international cold chain food trade platform builds a trade bridge for overseas suppliers and domestic small and medium-sized customers, and provides comprehensive services such as cross-border procurement, supply chain finance, and warehousing logistics. Cross-border cold chain trade often has many processes and takes a long time, which poses a major challenge to the capital turnover of small and medium-sized enterprises. Bank loans have high requirements on the financial status, development prospects and credit status of enterprises, and many medium-sized enterprises are already facing bankruptcy before obtaining financing.

The blockchain has the characteristics of decentralization, immutable data, and traceability[1], so that it can effectively solve data security-related problems in traditional supply chain systems. There have been many related studies on the application of blockchain technology in the field of trade at home and abroad. Alqaryouti et al. proposed a block chain international trade e-

MSEA 2023, May 26-28, Nanjing, People's Republic of China

DOI 10.4108/eai.26-5-2023.2334239

commerce platform framework to simplify the e-commerce transaction process[2], thereby easing the customs administrations duties. Chen et al. developed a blockchain-based international trade logistics platform to solve the problems of low efficiency and difficult responsibility attribution of document transfer and delivery of goods in traditional international trade processes[3]. When blockchain technology is applied to actual scenarios of international trade, a high level of transparency also increases the risk of information leakage such as business secrets and intellectual property rights. Therefore, privacy protection is an issue that cannot be ignored. Islam et al. proposed a blockchain-based supply chain management in the context of IIoT[4], discussing the trade-off between transparency and privacy. Al-Shaibani et al. provide a privacy protection framework for decentralized securities trading platforms[5], ensuring the anonymity and unlinkability of investor accounts and their trading activities.

The above research focuses on the application of blockchain technology in the trade process to simplify the process in actual scenarios and increase trust. Aiming at the financing difficulties of small and medium-sized enterprises in international cold chain trade, this paper proposes a data storage privacy protection scheme based on blockchain for international trade platforms. The solution solves the problem of credit evaluation of small and medium-sized customer enterprises on the platform through homomorphic encryption, zero-knowledge proof and other cryptography technologies. We apply blockchain technology to the international cold chain trade platform, use historical order information to quickly analyze the operating conditions of small and medium-sized enterprises, and then conduct credit ratings for small and medium-sized enterprises to evaluate the amount of financing that small and medium-sized enterprises can obtain. It can reduce the problem of many financing steps and long cycle for small and medium-sized enterprises in the traditional financing model.

2. METHODOLOGY

2.1 Zero-knowledge proof

Zero-knowledge proof [6] refers to the fact that the prover can convey to the verifier that the assertion about something is correct without revealing the thing itself. Since blockchains often have low storage requirements and the overhead of establishing network real-time communication is high, zero-knowledge proofs adapted to blockchains usually need to be simplicity and non-interactive. Among them, simplicity means that the communication complexity of the proof has a sub-linear relationship with the statement size, and non-interactive means that the prover only needs to send one round of messages to the verifier to complete the proof [7].

Bulletproofs[8] is a non-interactive zero-knowledge proof scheme that does not require trusted settings. It improves the inner product method in zero-knowledge range proofs based on the algorithm[9] proposed by Bootle and Groth et al. The proposed scheme is able to prove that committed values are in a range using only $2\ log\ (n) + 9$ group and field elements, where n is the bit length of the range, and proof generation and verification times are linear in n.

2.2 Pedersen commitment

Pedersen commitment[10] is a homomorphic commitment protocol that satisfies computational bindings that rely on the discrete logarithm assumption. The following is the Pedersen commitment formula based on elliptic curves:

$$Comm(v,r) = vG + rH \tag{1}$$

Among them, v is the privacy data to be committed, G and H are two base points on the elliptic curve, the random integer r is called the blinding factor, and $Comm(v,r)$ is called the committed value. The Pedersen commitment has additive homomorphism, and its formula is as follows:

$$\begin{aligned} Comm(v_1,r_1) + \mathrm{Comm}(v_2,r_2) &= (v_1\,\mathrm{G} + r_1\,\mathrm{H}) + (v_2\,\mathrm{G} + r_2\,\mathrm{H}) \\ &= (v_1+v_2)\times\,\mathrm{G} + (r_1+r_2)\times\,\mathrm{H} = \mathrm{Comm}(v_1+v_2, r_1+r_2) \end{aligned} \tag{2}$$

3. DESIGN OF BLOCKCHAIN-BASED FOOD TRADE PLATFORM

3.1 System model

This scheme is mainly for the following two closely connected application scenarios, and the system model is shown in Figure 1.

The first scenario is the daily transaction on the international cold chain food trade platform. Firstly, the enterprise submits the order, and after confirmation by the platform, the data related to the new order will be stored on the blockchain. Then the platform is responsible for the transaction process of negotiating with suppliers, freight forwarding companies, shipping companies, customs and other units, and updates relevant data on the blockchain at each process node to ensure that the process of ordering goods can be traced. When the company confirms the arrival of the goods and the platform receives the final payment, the order process ends. When the conditions for the end of the order process are met, the smart contract will automatically execute the relevant code, homomorphically encrypt the transaction amount of the order, and add it to the total amount of honest transactions of the enterprise on the platform. The transaction amount of a single order and the total transaction amount of an enterprise are always stored on the blockchain in the form of ciphertext.

The second scenario is that when a company needs a large amount of procurement and needs financing due to capital chain turnover problems, the company can generate a zero-knowledge proof. Without disclosing the specific amount of the total transaction amount on the platform, the generated proof can prove that the encrypted total transaction amount of the enterprise stored on the blockchain is indeed greater than a certain amount. Upload the proof to the blockchain, and the smart contract will verify the validity of the zero-knowledge proof and store the result. Financial institutions can check the verification results through the provided interface.

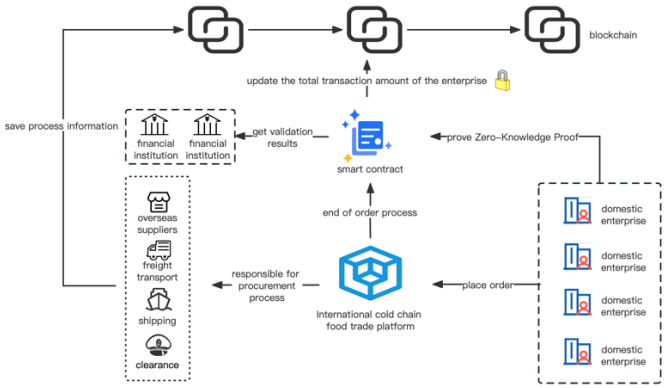

Figure 1. International cold chain food trade platform blockchain.

3.2 Privacy protection scheme

This paper focuses on the process of accumulating the total transaction amount of enterprises and proving the proof of transaction value, and proposes a privacy protection scheme based on Bulletproofs zero-knowledge proof. The scheme flow is shown in Figure 2.

(1) Generate Pedersen Commitment

m_1 is the plaintext of the transaction amount of a single order, which needs to be encrypted by the Pedersen algorithm. Upload the encrypted commitment value C_1 to the blockchain, and the encryption process is performed off-chain. The plaintext encryption steps are as follows:

a. Randomly generate blinding factor r_1

b. Calculate $C(m_1, r_1) = m_1 \times G + r_1 \times H$, where the public parameters G and H are points on the elliptic curve

Similarly, when initializing enterprise information, it is necessary to generate a blinding factor r_2 off-chain, and calculate the initial transaction total commitment value.

(2) Homomorphic operations on the blockchain

When the status of the order is changed to complete, the smart contract will automatically execute the code to add the transaction amount of this order to the current transaction amount of the enterprise. The execution steps are as follows:

a. Obtain the current total transaction commitment value C_2 of the enterprise on the blockchain

b. Calculate $C_{new} = C_1 + C_2$, The additive homomorphism of the Pedersen commitment is exploited here

c. Update the total transaction amount of the enterprise saved on the blockchain to C_{new}

(3) Generate zero-knowledge proof

When a company has financing needs, it can generate a zero-knowledge proof to prove that the current transaction total A is greater than a certain value limit. The steps are as follows:

a. The commitment value C_{limit} and blinding factor r_{limit} of limit are generated off-chain through the Pedersen algorithm, and r_{limit} is uploaded to the blockchain

b. Obtain the current transaction total commitment value C_A on the bloclchain, calculate C_R=$C_A - C_{limit}$, and save C_R. This step takes place on-chain

c. $\pi(prove,commitment) \leftarrow ProveAfterSubCommitment(A, limit, r_A, r_{limit}, C_A, C_{limit})$

Off-chain generated range proof π. π can prove $A - limit \geq 0$, upload π to the blockchain for verification.

(4) Verify zero-knowledge proof

After the enterprise submits the zero-knowledge proof π, the smart contract will call the verification method on the chain to verify the correctness of the $proof$ and $commitment$, and compare whether commitment is equal to the commitment value C_R previously deposited, and finally save the result to chain. When an enterprise applies for financing from a financial institution, it can provide $limit$ and r_{limit} to the financial institution, and the financial institution can verify off-chain whether it corresponds to the commitment value C_{limit} in the proof on the chain.

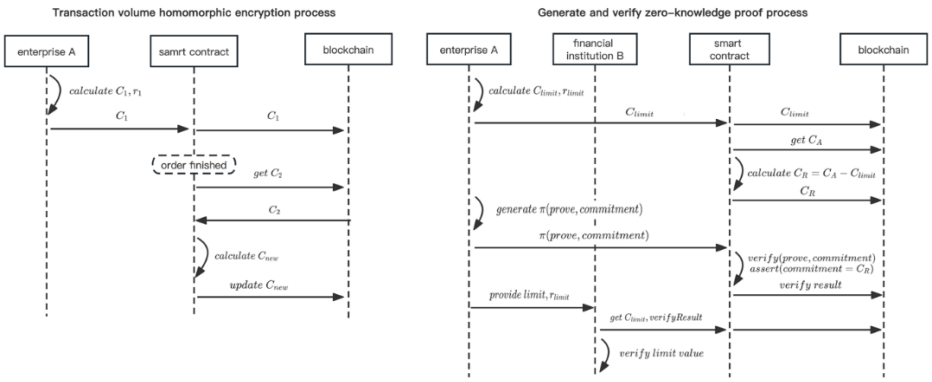

Figure 2. Zero-knowledge proof scheme process.

4. RESULTS

4.1 System feasibility

This article uses chainmaker to build a consortium blockchain network. The blockchain network built in this experiment is a single-machine 4-node cluster, using the PermissionedWithCert certificate mode, and the consensus algorithm is RAFT. Experiments run on 64-bit CentOS 7.6 operating system with 1.5 GHz 4-core Intel CPU and 4 GB RAM.

This article uses the GO language version of contract-SDK to write smart contracts, and compiles and packages them on the chain through Docker VM. Use Go-SDK to simulate various business processes for testing, and bulletproofs related operations use the chainmaker.org/sdk-go/common/crypto/bulletproofs package. The zero-knowledge range proof algorithm used in this paper requires the value $x \in [0, 2^{64})$, so the values are taken on four orders of magnitude of 2^8, 2^{16}, 2^{32} and 2^{64} for experiments, and the result is 10,000 operations average time spent. The specific operation steps and their time consumption are shown in Table 1. It can be seen that in the zero-knowledge range proof operation involved in this paper, the time of each step is relatively stable for any value within the range of int64. And the relatively time-consuming step of generating proofs is performed off-chain.

Table 1. Blockchain deployment environment.

Step/ Time-consuming	**2^8**	**2^{16}**	**2^{32}**	**2^{64}**
Generating a Pedersen Commitment	0.20ms	0.21ms	0.21ms	0.25ms
Homomorphic computing commitment	20.05μs	22.24μs	23.03μs	26.55μs
Generate range proofs	71.01ms	70.10ms	68.47ms	69.60ms
Verify proof and commitment	3.65ms	3.66ms	3.62ms	3.64ms

4.2 System feature analysis

Privacy: It mainly considers the privacy protection of the single order amount and the total transaction amount of each enterprise. The total amount of business transactions is obtained through the homomorphic operation of the Pedersen algorithm in the ciphertext state, so the privacy of the amount is based on the privacy promised by Pedersen. The Pedersen commitment is based on the assumption of the discrete logarithm difficulty of the elliptic curve.

Zero-knowledge: The total transaction amount A of the enterprise is only held off-chain by the enterprise itself, and the verifier cannot directly or indirectly calculate the specific value of A. The Bulletproofs protocol guarantees the zero-knowledge nature of the entire process.

Self-statistical: The calculation rules for the total amount of enterprise transactions are deployed to the blockchain platform in the form of smart contracts and are automatically executed according to the predetermined rules. Due to the immutability and consensus mechanism of the blockchain, the invariance of the predetermined rules and the correctness of the rule execution are guaranteed.

5. CONCLUSIONS

This paper designs a blockchain system for international cold chain food trade, and proposes a privacy protection scheme based on zero-knowledge proof, which can automatically accumulate the total transaction amount of the enterprise while hiding the specific amount of the order. And without disclosing the specific value, it provides proof that the total transaction amount on the chain is indeed greater than a certain value. At the same time, this paper conducts a deployment test based on the chainmaker and go-sdk. The experimental results show that the scheme proposed in this paper can be implemented within an effective time.

REFERENCES

[1] Dai Chuangchuang, Luan Haijing, Yang Xueying,et al. A review of blockchain technology research[J].Computer Science,2021,48(S2) :500-508.

[2] Alqaryouti O, Shallan K. Trade Facilitation Framework for E-commerce Platforms using Blockchain[J]. International Journal of Business Information Systems, 2020, 1(1):1.

[3] Chen Y Y, Lai H C, Huang J L, et al. The Design and Implementation of a Blockchain-Based Logistics Platform for International Trade[C]//2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2021: 234-237.

[4] Islam M, Rehmani M H, Chen J. Transparency-privacy Trade-off in Blockchain-Based Supply Chain in Industrial Internet of Things[C]//2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys). IEEE, 2021: 1123-1130.

[5] Al-Shaibani H, Lasla N, Abdallah M, et al. Privacy-Preserving Framework for Blockchain-Based Stock Exchange Platform[J]. IEEE Access, 2021, 10: 1202-1215.

[6] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems[M]//Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. 2019: 203-225.

[7] LI W H, ZHANG Z Y, ZHOU Z B, DENG Y. An overview on succinct non-interactive zero-knowledge proofs[J]. Journal of Cryptologic Research, 2022, 9(3): 379–447.

[8] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more[C]//2018 IEEE symposium on security and privacy (SP). IEEE, 2018: 315-334.

[9] Bootle J, Cerulli A, Chaidos P, et al. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2016: 327-357.

[10] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Annual international cryptology conference. Springer, Berlin, Heidelberg, 1992: 129-140.